



NORGES OFFENTLIGE UTREDNINGER

NOU 1997: 19

Et bedre personvern

- forslag til lov om behandling av personopplysninger

Utredning fra et utvalg oppnevnt ved kongelig resolusjon
6 oktober 1995.

Avgitt til
Justis- og politidepartementet 27 mai 1997

STATENS FORVALTNINGSTJENESTE
STATENS TRYKNING

OSLO 1997

Til Justis- og politidepartementet

Det Kgl Justis- og politidepartement nedsatte 6 oktober 1995 et utvalg for å utrede behovet for revisjon av lov 9 juni 1978 nr 48 om personregistre m m. Mandatet inneholder retningslinjer for utredningsarbeidet.

Personregisterlovutvalget legger med dette frem sin utredning med forslag til lov om behandling av personopplysninger. Utvalgets utredning er i hovedsak enstemmig, men for noen enkeltbestemmelser foreligger det avvikende forslag fra ulike mindretall.

Oslo 27 mai 1997

Arne Skauge leder

Georg Apenes

Mette Bredengen

Pål Gundersen

Arne Dag Hestnes

Jostein Håøy

Jens C Koch

Ewy Kristiansen

Tonje Meinich

Dag Wiese Schartum

Mari Bø Haugstad

Knut Erik Sæther

KAPITTEL 1

Sammendrag av personregisterlovutvalgets utredning**1.1 INNLEDNING**

Personregisterlovutvalget legger i denne utredningen frem forslag til en ny lov om behandling av personopplysninger. Loven skal erstatte lov 1978 nr 48 om personregistre m m. Bakgrunnen for utredningen fremgår av utvalgets mandat, se 2.1.

Utredningen består av tre deler. Del I er en i hovedsak deskriptiv oversikt over noen faktiske og rettslige utgangspunkter for utvalgets arbeid. Del II inneholder utvalgets vurderinger av en del utvalgte problemstillinger, som danner grunnlaget for del III; lovforslag med merknader til de enkelte bestemmelsene.

Lovforslaget atskiller seg på flere viktige punkter fra personregisterloven, se 1.2 nedenfor. Samlet sett er endringene så store at utvalget anser det som mest hensiktsmessig å foreslå en helt ny lov istedetfor å foreslå endringer i personregisterloven.

Utvalget mener at den nye reguleringen sett under ett ikke svekker, men *styrker* personvernet samtidig som forslaget ligger innenfor direktivets rammer.

Nedenfor presenteres først en punktvis oversikt av de viktigste endringene utvalget foreslår (se 1.2.1 – 1.2.7). Deretter følger et kronologisk sammendrag av de enkelte kapitlene.

1.2 HOVEDPUNKTER I UTREDNINGEN**1.2.1 Utvidet fokus: Ikke lenger bare «personregistre», men også «elektronisk behandling av personopplysninger»**

Personregisterloven regulerer opprettelse og bruk av personregistre. Utvalget foreslår at registerbegrepet ikke lenger skal gjelde som avgrenskningskriterium for elektronisk behandling av personopplysninger. Lovforslaget kommer til anvendelse på *elektronisk behandling* av personopplysninger mer generelt, og på *manuell behandling* av personopplysninger (dvs behandling uten bruk av elektroniske hjelpemidler) når personopplysningene *inngår i eller skal inngå i et personregister*. Dette medfører at den nye loven får et noe videre saklig virkeområde enn personregisterloven.

1.2.2 Større vekt på etterfølgende kontroll på grunnlag av meldinger til Datatilsynet

Personregisterloven bygger på en omfattende forhåndskontroll (konsesjonsplikt) ved opprettelse av personregistre. Utvalget foreslår at konsesjonsplikten innsnevres og at fokus i noen grad skiftes fra forhåndskontroll til etterfølgende kontroll med behandling av personopplysninger. Den etterfølgende kontrollen bygger på tre hovedelementer. For det første innføres en *plikt til å sende melding* til Datatilsynet om bestemte typer behandling av personopplysninger. Meldingene skal innføres i en offentlig tilgjengelig fortegnelse hos Datatilsynet, og vil gi Datatilsynet informasjon som bl a kan benyttes i kontrolløyemed. For det andre foreslås det at de som behandler personopplysninger skal *kvalitetssikre behandlingen og iverksette internkontroll*. For det tredje foreslås det at Datatilsynet gis kompetanse til å gi *pålegg om at lovstridig behandling av personopplysninger skal opphøre*, eller even-

tuelt stille vilkår som må oppfylles for at behandlingen skal være lovlig. Dersom pålegget ikke etterlevs, kan Datatilsynet ilegge en *tvangsmulkt* som løper inntil forholdet er rettet.

I lovforslaget ligger også at Datatilsynet skal gi mer *rettsinformasjon og veiledning* om personvern, blant annet ved å oppfordre til og delta i utarbeidelsen av bransjevisse atferdsnormer, dvs regler om personvern som ulike bransjer selv fastsetter.

Utvalget går inn for at det fortsatt skal være en konsesjonsplikt, men at området for konsesjon skal være atskillig mindre og fastsatt etter andre kriterier enn i dag. Avgrensningen av konsesjonsplikten etter lovforslaget er begrunnet i at personvern er særlig viktig når det benyttes sensitive personopplysninger til å treffe avgjørelser som er av stor betydning for den enkelte.

1.2.3 Flere regler i selve loven

Personregisterloven og forskriftene gitt i medhold av den inneholder få materielle regler, dvs regler som direkte sier noe om hvordan personopplysninger kan eller skal behandles. Mangelen på slike regler i loven har blitt avhjulpet av at Datatilsynet har satt generelle vilkår i sine konsesjoner. Utvalget foreslår at selve loven skal inneholde flere materielle regler, jf utredningen "*Regulering og kontroll*" i kapittel 12. Slike regler finnes bl a i kapitlene 2 og 4 i lovforslaget. Et konkret eksempel er begrenset adgang til å bruke personopplysninger til et annet formål enn de opprinnelig er innsamlet for.

1.2.4 Flere rettigheter til den som opplysningene gjelder (den registrerte)

Personregisterloven er basert på at den enkeltes personvernbehov dels varetas gjennom kollektive personverntiltak, som f eks Datatilsynets virksomhet, og dels ved at den enkelte selv er gitt rettigheter. Et eksempel på en individuell rettighet er retten til innsyn. Utvalget foreslår at den nye loven skal videreutvikle den registrertes individuelle rettigheter på tre områder.

For det første pålegges den som bestemmer formålet med behandlingen av personopplysningene (den behandlingsansvarlige) av *eget tiltak* å sørge for at den enkelte registrerte kan nyttiggjøre seg av rettighetene i loven. Et eksempel på dette er at den behandlingsansvarlige skal informere den registrerte når det innhentes opplysninger om vedkommende.

For det andre gis den registrerte noen *nye eller utvidete rettigheter* som man selv må ta initiativ for å benytte. Eksempler på dette er utvidet innsynsrett, rett til i visse tilfeller å kreve manuell behandling av personopplysninger, og rett til å kreve begrunnelse for beslutninger som bygger på slike behandlinger.

Endelig har utvalget lagt vekt på at lovfesting av rettigheter ikke alltid er nok – også *de faktiske forholdene må legges til rette* slik at det blir praktisk mulig for den registrerte å benytte seg av rettighetene. Dette skal oppnås bl a ved at Datatilsynet skal ha en offentlig tilgjengelig oversikt over behandling av personopplysninger.

1.2.5 Et mer uavhengig Datatilsyn

I henhold til personregisterloven er Datatilsynet et frittstående forvaltningsorgan. Utvalget foreslår bl a på bakgrunn av direktivet at Datatilsynet skal være faglig uavhengig av regjeringen og departementene, jf "*Tilsynsmyndigheten*" i kapittel 18. Regjeringens styringsredskaper vil være å gi forskrifter og å fremme forslag til lovendringer. Det foreslås at Justisdepartementet ikke lenger skal behandle klager over Datatilsynets avgjørelser. I forhold til uavhengigheten er poenget at departementet

ikke skal kunne legge føringer på Datatilsynets avgjørelser ved å avgi uttalelser i klagebehandlingen som også har rekkevidde utover den konkrete klagesaken.

1.2.6 Et nytt organ – Personvernemnda – skal behandle klager over Datatilsynets avgjørelser

Blant annet som følge av kravet om et uavhengig tilsyn foreslår utvalget at klager skal behandles av en nyopprettet klageinstans, Personvernemnda.

1.2.7 Strengere regler om overvåkning

En del overvåkning vil være elektronisk behandling av personopplysninger. Dette gjelder f.eks fjernsynsovervåkning med billedopptak som lagres digitalt. I så fall får loven anvendelse på vanlig måte. Men ikke all overvåkning vil være elektronisk behandling av personopplysninger i lovens forstand. Et eksempel på overvåkning som i utgangspunktet faller utenfor lovens saklige virkeområde, er fjernsynsovervåkning som lagres analogt uten effektive muligheter for gjenfinning av enkeltpersoner. Også for slik overvåkning er det etter utvalgets syn behov for strengere regler enn i dag, og utvalget foreslår at det også for denne type overvåkning bl a skal være meldeplikt og adgang for Datatilsynet til å gi pålegg. Dersom pålegget ikke respekteres, kan Datatilsynet gi tvangsmulkt.

1.3 SAMMENDRAG AV HVERT KAPITTEL

1.3.1 Utredningen del I

I *"Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte"* i kapittel 2 presenteres utvalgets bakgrunn, mandat, sammensetning og arbeidsmåte. Behovet for revisjon av personregisterloven skyldes dels en teknologisk utvikling som stadig åpner for nye muligheter til å innsamle, bearbeide og bruke personopplysninger, og dels Norges forpliktelse til å gjennomføre et EF-direktiv.

Begrepet «personvern» kan synes uklart og omfattende. Utvalget har derfor sett det som fornuftig å presisere hvilken betydning utvalget legger i begrepet, se *"Hva er personvern?"* i kapittel 3. På denne måten synliggjøres viktige referanserammer for utvalgets arbeid.

Som nevnt ovenfor begrunnes utvalgets mandat blant annet med teknologiske og samfunnsmessige utviklingstrekk som bør få betydning for reglene om personvern. I *"Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet"* i kapittel 4 utdypes enkelte av disse utviklingstrekkene, og det forklares hvorfor disse er av betydning for personvernet.

Når en lov skal revideres er loven selv et utgangspunkt for vurderingen. *"Personregisterloven med forskrifter"* i Kapittel 5 gir en oversikt over personregisterloven med forskrifter, mens *"Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern"* i kapittel 6 illustrerer at personvern også varetas av annen lovgivning, ulovfestede og avtalefestede regler.

Utvalget har sett det som viktig å orientere seg om internasjonale regler og om rettstilstanden i andre land. I *"Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse"* i kapittel 7 behandles Europarådets konvensjon om persondatabeskyttelse med tilhørende rekommandasjoner. I *"Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger"* i kapittel 8 gis en oversikt over EF-direktiv 95/46 om beskyttelse av fysiske personer i forbindelse med behandling av per-

sonopplysninger og om fri utveksling av slike opplysninger (senere også kalt «personverndirektivet» eller bare «direktivet»). I "*Oversikt over andre internasjonale reguleringer og andre lands rett*" i kapittel 9 redegjøres det kort for andre internasjonale reguleringer og for enkelte andre lands personregisterlovgivning. Enkelte grunnleggende likhetstrekk finnes, for eksempel kombinasjonen av lovregler med et tilsynsorgan som kontrollerer at loven etterleves. Utgangspunktet løser seg imidlertid opp i en rekke forskjellige reguleringsmåter fra land til land.

1.3.2 Utredningen del II

Personregisterloven gjelder for personregistre og bruk av personopplysninger i visse virksomheter. Utvalget foreslår at registerbegrepet opprettholdes som avgrensningskriterium for manuell behandling av personopplysninger, men at all elektronisk behandling av personopplysninger omfattes uavhengig av om opplysningene inngår i et personregister eller ikke. Dette er en utvidelse av det saklige virkeområde i forhold til personregisterloven. Utvidelsen blir imidlertid ikke så stor fordi det vil foreligge et «personregister» i personregisterlovens forstand dersom man relativt enkelt kan finne igjen personopplysninger om den enkelte som er lagret elektronisk.

Lovforslaget gjelder for behandling av opplysninger om *fysiske* personer. Opplysninger om juridiske personer vil også ofte ha et legitimt behov for vern. Dette behovet vil imidlertid i stor grad være begrunnet i andre hensyn enn personvern hensyn, som f.eks økonomiske interesser, og slike interesser bør varetas i annen lovgivning. Opplysninger om fysiske personer som knytter seg til juridiske personer (f.eks at en person er registrert som innehaver av en virksomhet) vil være en personopplysning som omfattes av loven. Opplysninger om døde personer omfattes i den grad opplysningene kan knyttes til gjenlevende enkeltpersoner.

Videre foreslås at loven gjelder for offentlig og privat virksomhet, men at behandling av personopplysninger for rent personlige formål – på samme måte som etter personregisterloven – ikke omfattes.

I "*Individuelle personverngarantier*" i kapittel 11 drøftes en rekke nye rettigheter som loven tildeler den enkelte. *Retten til innsyn* utvides i forhold til personregisterloven (11.2). Dette innebærer for det første en utvidet rett til generell informasjon om persondatabehandlinger og en utvidet rett til innsyn i registrerte opplysninger om en selv. For det andre pålegges den behandlingsansvarlige en informasjonsplikt (ved innsamling av personopplysninger fra den registrerte selv og ved innhenting av personopplysninger fra andre). For det tredje gis den enkelte et krav på begrunnelse for fullstendig automatiserte avgjørelser (krav til innsyn i «logikken» bak en automatisert avgjørelse, se 11.4).

Utvalget foreslår videre visse regler som gir den enkelte en rett til å motsette seg visse typer persondatabehandlinger (11.3). To rettigheter kan sies å tilhøre denne gruppen. Retten etter personregisterloven til å kreve sitt navn sperret mot bruk i direkte markedsføring foreslås videreført i den nye loven. Utvalget støtter Datatilsynets forslag om opprettelse av et sentralt reservasjonsregister for å gjøre det enklere for den enkelte å reservere seg. For det andre foreslås etablert en rett til å kreve manuell overprøving av enkelte fullstendig automatiserte avgjørelser.

Endelig foreslås visse regler om sletting av personopplysninger (11.5). Personregisterlovens bestemmelse om retting, sletting eller supplering av uriktige eller ufullstendige opplysninger eller opplysninger som det ikke er adgang til å registrere foreslås i all hovedsak videreført. I tillegg foreslås en generell regel om at personopplysninger skal slettes når det ikke lenger er saklig grunn for oppbevaring. Slike generelle slettingsregler fastsettes nå i Datatilsynets konsesjoner for opprettelse av personregistre. Nytt i forhold til dagens regulering er utvalgets forslag om at den

enkelte registrerte gis et utvidet rett til å kreve opplysninger om seg selv slettet eller sperret.

Avslutningsvis i "*Individuelle personverngarantier*" i kapittel 11 drøftes noen spørsmål tilknyttet tidsfrister for å etterkomme krav fra de registrerte og kostnader knyttet til de registrertes rettigheter (11.6).

Utvalget foreslår i "*Regulering og kontroll*" i kapittel 12 et bredt spekter av virkemidler for ivaretagelse av personvernet ved behandling av personopplysninger. Konesjonspliktordningen foreslås videreført, men blir langt mindre omfattende enn i dag og avløst av en rekke tiltak som bl a bygger på en meldeplikt i kombinasjon med mer tilsyn fra Datatilsynet. Utvalget foreslår dessuten at Datatilsynet skal gi råd til dem som planlegger å behandle eller allerede behandler personopplysninger, samt til å gjennomføre etterfølgende kontroller. Det foreslås flere regler enn i dagens lov, og det vil dessuten som i dag være behov for regulering i forskrift. Videre foreslås regler om internkontroll, og endelig har utvalget vurdert såkalte bransjevise atferdsnormer som er utarbeidet av de behandlingsansvarlige selv. Eksempler på nye regler i loven er bestemmelser om krav til uttrykkelig definert formål ved behandling av personopplysninger, bruk av personopplysninger til andre formål enn det opprinnelige, behandling av sensitive personopplysninger og bruk av fødselsnummer.

Personregisterloven regulerer bruk av personopplysninger i visse typer virksomheter (kredittopplysningsvirksomhet, databehandlingsvirksomhet, adresserings- og distribusjonsvirksomhet og opinions- og markedsundersøkelser) i loven kapittel 5-8. Utvalget foreslår ikke å videreføre slik særskilt regulering i den nye loven (se "*Særlige regler for visse virksomheter*" i kapittel 13). Utvalget foreslår i stedet en rekke nye regler som vil få anvendelse på alle typer elektronisk behandling (samt visse manuelle behandlinger). Flere generelle regler minsker behovet for særlige regler for visse utvalgte virksomheter. Det kan være aktuelt for den behandlingsansvarlige å benytte en databehandler som etter avtale behandler personopplysninger på vegne av den behandlingsansvarlige. Utvalget foreslår en bestemmelse som begrenser databehandlerens rådighet over personopplysningene. Dersom det viser seg ytterligere behov for særskilt regulering av visse virksomheter, foreslår utvalget at dette gjøres gjennom forskrift. Behandling av personopplysninger i kredittopplysningsvirksomhet bør etter utvalgets syn reguleres nærmere i forskrift.

Overvåking som innebærer elektronisk behandling av personopplysninger omfattes av lovforslaget, og enkelte bestemmelser i lovforslaget gjelder også for annen overvåking. I utredningen "*Fjernsynsovervåking og annen elektronisk overvåking*" i kapittel 14 foreslår utvalget at dagens regler om fjernsynsovervåking videreføres, samt suppleres på to punkter. For det første foreslår utvalget at fjernsynsovervåking som resulterer i billedopptak blir underlagt meldeplikt. For det andre foreslår utvalget at Datatilsynet gis kompetanse til å gripe inn og stoppe fjernsynsovervåking og billedopptak i forbindelse med slik overvåking når den blir igangsatt ulovlig, f eks fordi overvåkingen ikke kan sies å være saklig begrunnet. Endelig foreslås det at straffeloven § 390 b om varslingsplikt ved fjernsynsovervåking av offentlig sted og arbeidssted flyttes fra straffeloven til ny lov om behandling av personopplysninger.

I "*Sikring av personopplysninger*" i kapittel 15 behandles sikring av personopplysninger, dvs tiltak for å sørge for at personopplysninger blir behandlet i samsvar med loven. Mens rettsreglene stiller krav til hvordan personopplysninger skal og kan brukes, er sikringstiltak organisatoriske og tekniske krav som skal sikre at rettsreglene etterlevs. Utvalget redegjør for tidligere utredningsarbeider og initiativ på området, samt for gjeldende rett. I sine vurderinger legger utvalget til grunn at det er et stort behov for systematiske tiltak for å sikre at regelverket om behan-

dling av personopplysninger etterleves. Og slike tiltak er en nødvendig del av en fremtidig regulering på personvernområdet. Konkret foreslår utvalget at det lovfestes en plikt til å etablere og anvende metoder for informasjons- og datasikkerhet for visse typer persondatabehandlinger.

"Overføring av personopplysninger til utlandet" i Kapittel 16 omhandler overføring av personopplysninger til utlandet. Utvalget redegjør først for gjeldende rett og internasjonale reguleringer på området. I sine vurderinger legger utvalget til grunn at det skal bli lettere å overføre personopplysninger til stater som har gjennomført personverndirektivet. For overføring til stater som ikke har gjennomført EF-direktivet, blir det avgjørende om den aktuelle staten har et tilstrekkelig forsvarlig nivå på sin personvernregulering. Dersom mottakerstaten ikke oppfyller dette kravet, kan overføring kun finne sted dersom visse nærmere bestemte vilkår er oppfylt.

Regler om behandling av personopplysninger må ta hensyn til ytringsfriheten, se *"Forholdet til ytringsfriheten"* i kapittel 17. Utvalget foreslår at det gjøres et generelt unntak fra deler av lovforslaget der dette er nødvendig for å finne en rimelig balanse mellom ytringsfrihet og personvern. Med «ytringsfrihet» menes ikke bare en henvisning til overordnede regler som Grunnloven § 100 og Den europeiske menneskerettighetskonvensjon artikkel 8 og 10, men også ytringsfrihet som et reelt hensyn. Utvalget gir i kapittel en del eksempler på avveininger av ytringsfrihet mot personvern.

"Tilsynsmyndigheten" i Kapittel 18 omhandler tilsynsmyndighetens organisering, plassering og oppgaver.

Når det gjelder Datatilsynets oppgaver foreslås det at større vekt legges på rådgivning og kontroll av at loven etterleves. Behandling av konsesjonssøknader vil kreve mindre tid og ressurser enn i dag.

Et enstemmig utvalg går inn for at Datatilsynet skal være faglig uavhengig av regjeringen og departementene. Dette innebærer for det første at regjeringen og departementene ikke skal kunne instruere Datatilsynet om lovtolkning og skjønnsutøvelse verken generelt eller i enkeltsaker, og at Justisdepartementet ikke lenger skal behandle klager over Datatilsynets avgjørelser. Klager skal i henhold til forslaget behandles av et nyopprettet organ, «Personvernemnda». Også Personvernemnda skal være faglig uavhengig av Justisdepartementet. Forøvrig går utvalget inn for at både Datatilsynet og Personvernemnda administrativt skal høre under regjeringen og det departement Kongen fastsetter (i dag Justisdepartementet).

Utvalget er ikke enstemmig i alle problemstillingene knyttet til organiseringen og plasseringen av tilsynsmyndigheten. Utvalgets leder og medlemmene Apenes, Kristiansen, Meinich og Schartum går inn for at når det opprettes en bredt sammensatt og faglig kompetent klageinstans, vil det ikke lenger være behov for noe styre i Datatilsynet, mens medlemmene Bredengen, Gundersen, Hestnes, Håøy og Koch mener at dagens styreordning bør videreføres fordi opprettelse av nytt klageorgan etter disse medlemmenes syn ikke har betydning for spørsmålet om hvorledes Datatilsynet bør organiseres. Når det gjelder oppnevning av medlemmer til Personvernemnda går utvalgets flertall, medlemmene Bredengen, Gundersen, Hestnes, Håøy, Koch, Kristiansen og Meinich, inn for at klageinstansen bør ha fem medlemmer og at samtlige bør oppnevnes av Kongen. Et mindretall i utvalget, bestående av lederen og medlemmene Apenes og Schartum, mener at klageinstansen bør ha syv medlemmer og at to av disse bør oppnevnes av Stortinget mens resten bør oppnevnes av Kongen.

"Sanksjoner" i Kapittel 19 omhandler hvilke sanksjoner som kan benyttes dersom loven ikke etterleves. Straffansvaret videreføres med noen mindre endringer, bl a slik at overtredelsen av loven under særdeles skjerpene omstendigheter skal

kunne medføre fengsel inntil to år (i dag er maksimumsstraffen ett år). Straffansvar for foretak bør som i dag reguleres av straffelovens bestemmelser. Utvalget foreslår videre at det innføres et generelt erstatningsansvar for brudd på loven når dette fører til økonomisk tap og skadevolderen ikke kan godtgjøre at han eller hun ikke kan lastes for skaden. Utvalget går ikke inn for rett til erstatning for ikke-økonomisk tap (oppreisning), men foreslår istedet at skadevolderen pålegges en plikt til å sørge for at lovovertrедelsen får minst mulig konsekvenser for den registrerte (en plikt til gjenopprettelse). Utvalget foreslår videre at Datatilsynet skal kunne ilegge en tvangsmulkt dersom pålegg i medhold av loven ikke etterleveres.

I "*Økonomiske og administrative konsekvenser av utvalgets forslag*" i kapittel 20 gjøres rede for økonomiske og administrative konsekvenser av utvalgets forslag. For *Justisdepartementet* vil lovforslaget medføre at det ikke lenger må brukes ressurser på behandling av klager over Datatilsynets avgjørelser. Departementet må imidlertid sørge for at det opprettes en Personvernemnd og sette av midler til denne. For *Datatilsynet* vil lovforslaget føre til at ressurser kan flyttes fra behandling av konsesjonssøknader til rådgivning og etterfølgende kontroll. Datatilsynet vil i en overgangsperiode ha behov for vesentlig større ressurser enn i dag. For *den som behandler personopplysninger* (den behandlingsansvarlige) vil forslaget innebære noe kostnader, blant annet som følge av flere individuelle rettigheter og som følge av krav til sikringstiltak m.v. Nøyaktig hvor store kostnader det dreier seg om kan vanskelig fastslås på forhånd. Dette skyldes blant annet at kostnadene avhenger av hvor mange som benytter seg av de rettighetene loven gir.

Del I Utgangspunkter

KAPITTEL 2

Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte**2.1 UTVALGETS SAMMENSETNING OG MANDAT**

Som medlemmer av utvalget ble følgende personer oppnevnt:

1. Konserndirektør Arne Skauge, Den norske Bank, leder
2. Direktør Georg Apenes, Datatilsynet
3. Rådgiver, Birgitte Araldsen, Samferdselsdepartementet
4. Rådgiver Mette Bredengen, Statistisk sentralbyrå
5. Sekretær Pål Gundersen, Landsorganisasjonen i Norge
6. Advokat Arne Dag Hestnes, Næringslivets Hovedorganisasjon
7. Spesialrådgiver Jostein Håøy, Statskonsult (nå underdirektør i Planleggings- og samordningsdepartementet)
8. Utredningsleder (nå rådgiver) Ewy Kristiansen, Sosial- og helsedepartementet
9. Førstekonsulent i Justisdepartementet (nå dommerfullmektig) Tonje Meinich
10. Førsteamanuensis (nå professor) Dag Wiese Schartum, Universitetet i Oslo.

Utvalgets medlem Birgitte Araldsen gikk ut i permisjon fra sin stilling i Samferdselsdepartementet i juni 1996. I hennes sted har spesialrådgiver Jens C. Koch, Samferdselsdepartementet, gjort tjeneste.

Utvalgets sekretærer har vært rådgiver Mari Bø Haugstad og førstekonsulent Knut Erik Sæther. Utvalget har i innspurfasen hatt god hjelp av førstekonsulent i Datatilsynet, Åste Marie Bergseng.

Utvalget ble gitt følgende mandat:

Utvalget bør i utgangspunktet stå fritt til å ta opp alle sider ved personregisterloven og tilstøtende lovgivning som utvalget mener bør utredes og eventuelt endres. Utvalgets hovedoppgave bør være å forberede en generell oppdatering av personregisterlovgivningen i lys av den teknologiske, økonomiske og administrative utvikling på området. De forslag som legges fram må ligge innenfor Norges internasjonale forpliktelser. De administrative og økonomiske konsekvensene av utvalgets forslag må også utredes.

Utredningen skal bl a omfatte følgende punkter:

a. Personregisterlovens konsesjonsordning

Etter personregisterloven § 9 kreves det konsesjon fra Kongen for å opprette personregistre som skal gjøre bruk av elektroniske hjelpemidler. Videre kreves det konsesjon for å opprette andre personregistre dersom de skal inneholde følsomme opplysninger. Det er ved forskrift gjort en rekke unntak fra konsesjonsplikten. Myndigheten til å gi konsesjon er delegert til Datatilsynet.

Utvalget skal vurdere hvilken regulerings- og kontrollordning som kan/bør velges dersom EUs direktiv om beskyttelse av personopplysninger blir gjort til en del av EØS-avtalen, se også bokstav d nedenfor. I denne forbindelse skal utvalget vurdere alternative regulerings- og kontrollmåter, f eks regulering/kontroll gjennom meldeplikt og forholdsnormer.

b. Datatilsynets rolle

Datatilsynets oppgaver er nærmere angitt i personregisterloven kapittel 2. Etter § 3 skal Datatilsynet bli avgitt uttalelser, råd og rettleiing om bruk av personregistre og personopplysninger. Etter § 4 skal Datatilsynet føre fortegnelse over konsesjonspliktige personregistre. I § 5 har Datatilsynet hjemmel til å gjennomføre tilsyns- og kontrolloppgaver. Ved siden av disse lovfestede oppgavene har Datatilsynet fått delegert myndighet etter loven. Viktigste her er myndigheten til å gi konsesjon etter § 9.

Etter § 2 sammenholdt med kgl res 8 november 1979 er Datatilsynet et frittstående organ underordnet Kongen og Justisdepartementet.

Utvalget skal foreta en vurdering av hvilke oppgaver som bør ligge til Datatilsynet i framtiden. I denne forbindelse skal det vurderes hvilken stilling Datatilsynet bør ha i forhold til regjeringen og departementet, herunder regjeringens og departementets instruksjons- og kontrollmyndighet. *Utvalget* skal i denne forbindelse vurdere hvilke løsninger som kan/bør velges dersom EUs direktiv om beskyttelse av personopplysninger blir vedtatt og gjort til en del av EØS-avtalen, se også bokstav d nedenfor.

c. Varslingsplikt, innsynsrett

(1) Stortinget traff 21 april 1994 vedtak der det ble om at Regjeringen legger fram for Stortinget to konkrete forslag til endringer i personregisterloven. I vedtaket heter det:

«1. Stortinget ber Regjeringen legge fram forslag til endringer i lov om personregistre, slik at eieren av et personregister som hovedregel plikter å varsle personene som registreres eller er registrert, om registreringen, dens omfang og formålet med denne.

2. Stortinget ber Regjeringen legge fram forslag til endringer i lov om personregistre, slik at loven får en formålsparagraf som slår fast retten til vern mot utilbørlig inngripen i menneskers privatliv.»

Utvalget skal vurdere og legge fram forslag til lovbestemmelser i tråd med vedtaket. Forholdet til de relevante bestemmelsene i EUs direktiv om beskyttelse av personopplysninger om dette må også vurderes, se også bokstav d nedenfor.

(2) Etter personregisterloven § 7 er hovedregelen for edb-registre at «alle har rett til å få opplyst hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler». Unntak gjelder for opplysninger i registre som bare blir brukt til statistikk, forskning og generelle planleggingsformål. Videre er det gjort unntak for opplysninger «som det må anses utilrådelig at vedkommende får kjennskap til, av hensyn til deres helse eller forholdet til personer som står dem nær». I manuelle registre har den registrerte som hovedregel bare innsyn i personregistre i organ for stat eller kommune. Derimot har den registrerte i utgangspunktet ikke innsyn i det som er registrert om vedkommende i private registre. Med hjemmel i § 7 fjerde ledd er det ved forskrift fastsatt at det også skal være rett til innsyn i visse private registre.

Utvalget skal foreta en generell vurdering av bestemmelsene om innsynsrett i personregisterloven § 7. Det skal særlig vurdere om innsynsretten i forhold til private manuelle registre bør utvides. I forhold til offentlige registre skal *utvalget* vurdere om det er grunn til i større grad å harmonisere innsynsrettsbestemmelsene i personregisterloven § 7 med andre lovbestemmelser som gir innsynsrett i personopplysninger, f.eks. forvaltningsloven §§ 18 og 19. Forholdet til de relevante bestem-

melsene i EUs direktiv om beskyttelse av personopplysninger om dette må også vurderes, se også bokstav d nedenfor.

d. Internasjonale regler og utenlandsk rett

(1) EU-kommisjonen la i 1992 fram et revidert utkast til direktiv om beskyttelse av personopplysninger. Direktivet ble endelig vedtatt sommeren 1995.

Utvalget skal vurdere hvilke lovendringer EUs direktiv om beskyttelse av personopplysninger vil kreve i personregisterloven og annen lovgivning, samt foreslå eventuelle lovendringer. *Utvalget* kan også ta opp til vurdering andre sider av direktivet.

(2) Europarådets konvensjon 28 januar 1981 om persondatabeskyttelse setter krav til og rammer for medlemslandenes lovgivning. Norge ratifiserte konvensjonen uten forbehold 20 februar 1984. Personregisterloven antas å oppfylle konvensjonens krav. *Utvalgets* forslag til lovendringer skal ligge innenfor konvensjonens rammer og tilfredsstillende dens krav.

Europarådet har med utgangspunkt i konvensjonen vedtatt en rekke rekommandasjoner om persondatabeskyttelse. *Utvalget* skal ved sine vurderinger og eventuelle forslag ta særlig hensyn til rekommandasjonene.

(3) *Utvalget* skal i sitt utredningsarbeid også se hen til andre relevante internasjonale dokumenter.

(4) Norge var av de første land i Europa som fikk en generell lov om personregistre. De siste 15 år har en rekke land vedtatt regler om personregistre. Edb-teknologien reiser i stor grad de samme spørsmål, utfordringer og problemer i de ulike land. Hvordan andre land har valgt å regulere dette området vil derfor kunne være nyttig informasjon i forbindelse med arbeidet med ny norsk lovgivning. *Utvalget* bør derfor – så langt det finner det nødvendig – innhente opplysninger om andre lands rett.

e. Forholdet til forskriftsverket

Det er i medhold av personregisterloven gitt nærmere forskrifter. *Utvalget* skal ikke gjennomgå forskriftene ut over det *utvalget* måtte finne nødvendig for å oppfylle mandatets øvrige punkter. *Utvalget* skal derimot vurdere om gjeldende fullmaktsbestemmelser er tilfredsstillende og tilstrekkelige, og bes særskilt vurdere hjemmelen for å fastsette bestemmelser om datasikkerhet.

f. Lovtekniske spørsmål

Utvalget skal stå fritt med hensyn til om forslaget skal munne ut i et utkast til en helt ny lov om personregistre eller utkast til endringer i den eksisterende lov.

g. Andre spørsmål

Fra forskjellig hold har det i tiden etter forrige lovrevisjon blitt pekt på forhold ved personregisterloven som bør vurderes endret. Justisdepartementet ber *utvalget* særlig vurdere følgende:

- Spørsmål om utvidelse av ansvarsbestemmelsen i personregisterloven § 40 samt utvidelse av oppreisningsansvaret, se Innst S nr 80 for 1991-92 s 11.
- Spørsmål om personregisterloven bør gis anvendelse på virksomhet som driver salg, vedlikehold m v av edb-utstyr og gjennom denne virksomheten får tilgang til personopplysninger, samt informasjonsformidlingsvirksomhet, se Rapport om databehandlings-virksomhet 26 januar 1994 (Datatilsynet).

Utvalget konstaterer at mandatet er vidtfaende og utvalget har foretatt en generell gjennomgang av personregisterloven

2.2 BEHOVET FOR REVISJON AV PERSONVERNLOVGIVNINGEN

I St meld nr 23 (1994-95) Årsmelding for Datatilsynet 1993 uttalte Justisdepartementet følgende om behovet for revisjon av personregisterloven:

«Den teknologiske og økonomiske utvikling skaper hele tiden nye utfordringer for personvernet. I forhold til innsamling, lagring og bruk av personopplysninger bør regelverket holde tritt med utviklingen. Videre er det viktig at reglene er velegnede, betryggende og enklest mulig å praktisere.

Datatilsynet peker flere steder i sin årsmelding på at gjeldende regelverk ikke virker fullt ut tilfredsstillende (se årsmeldingen pkt 5.2, 7.1 og 7.3) Stortinget har selv tatt opp spørsmål om lovendringer; 21 april 1994 traff Stortinget vedtak der det ba om at Regjeringen legger fram for Stortinget konkrete forslag til endringer i personregisterloven, bl a om registeransvarliges plikt til å varsle personene som registreres eller er registrert, om registreringen, dens omfang og formålet med denne. Justisdepartementet har også merket seg andre områder innenfor personregisterloven (og forskriftene til denne) hvor det er behov for endringer.

Personregisterloven er fra 1978. I 1987 ble det på bakgrunn av en større utredning om revisjon av personregisterloven, foretatt en rekke endringer (lov 12 juni 1987 nr 55). Endringene var imidlertid ikke av grunnleggende karakter. Senere er det foretatt enkelte mindre endringer, f eks ved lov 11 juni 1993 nr 78 hvor det ble tatt inn et nytt "*Oversikt over andre internasjonale reguleringer og andre lands rett*" i kapittel 9a om fjernsyns- overvåkning.»

EUs direktiv om beskyttelse av personopplysninger ble vedtatt 24 juli 1995. Frist for implementering av direktivet i norsk rett er 18 oktober 1998.

Det gjøres forberedelser til vedtak i EØS-komiteen om å innlemme direktivet i EØS-avtalen. Etter at slikt vedtak er truffet vil regjeringen fremme en stortingsmelding hvor det anmodes om samtykke til at direktivet gjøres til en del av EØS-avtalen.

2.3 ANDRE RELEVANTE UTREDNINGER OG FORSLAG

I NOU 1993: 22 Pseudonyme helseregistre ble det lagt fram forslag til lov om helseregistre for forsknings- og helseadministrative formål. Et flertall i utvalget konkluderte med at det ikke burde opprettes et sentralt personidentifiserbart register, men at det i stedet burde gjøres forsøk med et nytt regionalt registersystem for institusjonshelsetjenesten basert på pseudonym i stedet for på navn og fødselsnummer. Utredningen inneholder bl a også en oversikt over grunnleggende interesser og verdier av betydning for personvernet, se utredningen punkt 5. Utredningen er nå til behandling i helse- og sosialdepartementet.

Enkelte andre relevante utredninger og forslag er det redegjort for senere i denne utredningen. Dette gjelder bl a tidligere utredningsarbeider og initiativ om sikring av personopplysninger, jf 16.2 og nedsettelsen av Ytringsfrihetskommisjonen, se "*Datatilsynets oppgaver i fremtiden*" i kapittel 18.2.

2.4 UTVALGETS ARBEIDSMÅTE

Utvalget startet sitt arbeid i desember 1995. I 1996 ble det avholdt 12 møter og i 1997 13 møter. Utvalget avsluttet sitt arbeid 5 mai 1997.

Utvalget har sett det som viktig å ha en bred kontaktflate utad både nasjonalt og internasjonalt. Den 13 og 14 august 1996 arrangerte utvalget et seminar på Viul Gård utenfor Hønefoss med deltakere fra de tilsvarende utvalgene i Danmark, Sverige, Finland og Island. Et sentralt tema på seminaret var gjennomføringen av personverndirektivet. Utvalget har vært i kontakt med en del organer og virksomheter som vil bli berørt av den nye loven. En rekke av disse har kommet med muntlige og skriftlige innspill som utvalget har tatt i betraktning i sitt arbeid.

Utvalget har på enkelte felter funnet det hensiktsmessig å benytte seg av ekstern spisskompetanse. Professor dr juris Eivind Smith har på oppdrag fra utvalget utredet enkelte konstitusjonelle spørsmål knyttet til organiseringen og plasseringen av tilsynsmyndigheten, se vedlegg 5. Stipendiat Lee Bygrave har bistått utvalget med å utarbeide en oversikt over internasjonale reguleringer av personvern og andre lands rett på personvernområdet, se "*Oversikt over andre internasjonale reguleringer og andre lands rett*" i kapittel 9. Stipendiat Kyrre Eggen har i uttrykt vedlegg 24 februar 1997 levert bakgrunnsmateriale av betydning for avveiningen mellom personvern og ytringsfrihet, jf "*Tilsynsmyndigheten*" i kapittel 18. Sekretariatsleder Dag Elgesem har på oppdrag fra utvalget kommet med et innspill som bl a belyser hvordan allmennmoralske normer har betydning for hvorledes samfunnet varetar personvern, se vedlegg 6. Jason Hoida har utarbeidet et sammendrag på engelsk, se vedlegg 1.

Utvalget har beklageligvis ikke hatt tilgang til en offisiell norsk versjon av direktivet. I den grad det har vært hensiktsmessig å sitere fra direktivet, er sitatene hentet fra den danske utgaven (vedlegg 3), som språklig sett ligger nærmest den kommende norske versjonen.

Flere personer har deltatt i skrivearbeidet, og det kan nok derfor være en viss forskjell i uttrykksmåte i de ulike delene av utredningen.

KAPITTEL 3

Hva er personvern?**3.1 OVERSIKT OVER FRAMSTILLINGEN**

Personvernbegrepet kan ofte synes omfattende og uklart. Utvalget anser det derfor som hensiktsmessig å gi en oversikt over den forståelse av personvernet som utvalget har lagt til grunn i sitt arbeid. Under 3.2 nedenfor skisseres personvernets historie, i 3.3 søkes personvernbegrepet klargjort ved at begrepet ses i fra ulike synsvinkler. Personvernet kan også beskrives som et knippe av ulike interesser, se nedenfor 3.4.

3.2 OM PERSONVERNETS HISTORISKE BAKGRUNN

Uttrykket «personvern» ble første gang brukt i to utredninger (NOU 1974: 22 og NOU 1975: 10) som dannet grunnlaget for personregisterloven.

Den moderne personverndebatten har imidlertid sitt utspring mer enn 100 år tilbake i tid. I en artikkel av de amerikanske juristene Samuel D. Warren og Louis D. Brandeis ble det argumentert for at det i amerikansk rett eksisterte en «right to privacy». Artikkelen var foranlediget av at pressen i økende grad hadde oppslag om kjente enkeltpersoners private forhold. Den teknologiske utviklingen og oppfinnelsen av rotasjonspressen (1863) gjorde det mulig å trykke flere aviser, noe som økte leserkretsen og spredningen av opplysningene. Med jernbane og dampbåt ble postgangen raskere og mer pålitelig. Disse endringene i samfunnet gjorde presseoppslagene mer krenkende for den som ble omtalt.

I 1890 utarbeidet Bernhard Getz et utkast til norsk straffelov der han også introduserte begrepet «privatlivets fred» (jf i dag strl § 390). Bestemmelsen setter straff for den «som krenker privatlivets fred ved å gi offentlig meddelelse om personlige eller huslige forhold». Bestemmelsen ble brukt i mange tilfeller som i dag faller naturlig inn under personregisterloven.

Andre land bruker uttrykk som gir litt andre assosiasjoner enn personvern, men «Datenschutz», «data protection», «privacy protection» og «skydd mot intrang i personlig integritet» dekker stort sett det samme. Tidligere ble også uttrykket *personlighetens rettsvern* brukt. Dette var en samlebetegnelse for rettsregler som beskyttet enkeltindividet mot krenkelse av immaterielle goder, som f.eks. injurielovgivningen, navnevernet, vernet mot fredskrenkelser etc. Dette «personlighetens rettsvern» dekket imidlertid ikke de problemene som oppstod i forbindelse med edb-basert behandling av personinformasjon.

Selv om «personvern» opprinnelig bare var ment å omfatte det området personregisterloven regulerer, har uttrykket i dag fått en videre betydning. I dagens språkbruk og i den offentlige debatt omfatter «personvern» gjerne alt som tidligere gikk inn under uttrykket «personlighetens rettsvern», herunder også det ulovfestede personvernet, dvs. personvernregler som følger av Høyesteretts avgjørelser.

3.3 ULIKE SYNSVINKLER PÅ DET MODERNE PERSONVERNET**3.3.1 Innledning**

På et helt generelt plan kan personvernet sies å gjelde krav til behandling av personopplysninger når kravene er begrunnet ut i fra visse *ideelle* (ikke-økonomiske)

interesser som en tillegger fysiske (og eventuelt juridiske) personer. Når det gjelder varetakelse av den enkeltes økonomiske interesser knyttet til behandling av personopplysninger, er det altså ikke personverntilnærmingen som er den mest aktuelle. I stedet vil vi da f eks snakke om forbrukervern. Personvernet er ikke den eneste relevante ideelle interesse når behandling av personopplysninger skal diskuteres. Hensynet til helse, sikkerhet, forskning og pressefrihet er noen stikkord som viser til andre viktige ideelle verdier.

I det følgende vil vi presentere tre ulike fokus på eller vektlegginger av personvernet. Inndelingen er primært et framstillingsmessig grep. Framstillingen må med andre ord ikke ses som en oppsplitting av personvernet i separate deler.

3.3.2 Det integritetsfokuserte personvernet

For det første kan personvernet betraktes med et fokus på *den personlige integriteten*. Dette kan ses som uttrykk for et grunnleggende ønske om å ha kontroll over opplysninger om en selv, særlig opplysninger som oppleves som personlige. Det integritetsfokuserte personvernet dekker imidlertid mer enn hensynet til at opplysninger om personlige og intime forhold ikke skal bringes videre uten samtykke fra de personer opplysningene gjelder. Også retten til å være i fred fra andre, uavhengig av om fredsforstyrrelsen innebærer at personlige opplysninger blir røpet eller ikke, kan sies å høre med. I NOU 1993: 22 «Pseudonyme helseregistre» er integritetsinteressen konkretisert på flere ulike måter (s 43 – 44).

Denne måten å se personvernet på kan illustreres ved at det trekkes en *sirkel av privatsfære* rundt enkeltpersonene slik at når en trår nær en person, må en enten eksplisitt eller implisitt ha en tillatelse, eller man må ha en god og legitim grunn for å nærme seg. Jo nærmere en trår uten tillatelse, jo sterkere må den legitime grunnen være. Det er trolig ikke mange som vil hevde at det eksisterer noen absolutt grense mot å krenke denne integritetssfæren. De fleste godtar at det eksisterer tilstrekkelig sterke og legitime grunner til selv den mest eklatante krenkelse av folks personlige integritet. Mange aksepterer f eks at tollere undersøker «kroppens hulrom» på jakt etter narkotika, og at enkelte psykisk utviklingshemmede blir gjenstand for vedvarende elektronisk tilsyn. Grensene mellom det akseptable og uakseptable er imidlertid ofte vanskelige å trekke. I hvilken grad bør f eks pressen eksponere folks privatliv; «offentlige personers» liv og levned, ofre for ulykker, forbrytere eller andre personer som det av en eller annen grunn har nyhetsverdi, underholdningsverdi eller «bare» økonomisk verdi å omtale eller avbilde?

Det integritetsfokuserte personvernbegrepet har mange «aner» fra tiden før vi tok personvernet i bruk, f eks bestemmelsene om ærekrenkelser og bestemmelser som verner om privatlivets fred ved å gjøre visse meddelelser om «personlige eller huslige forhold» straffbare (strl § 390). Straffeloven § 390 a som setter straff for den som «krenker en annens fred» ved skremmende eller plagsom eller annen hensynsløs opptreden, kan ses på samme måte. Også de mange bestemmelser om taushetsplikt for å verne fortrolige forhold mellom prest og sognebarn, lege og pasient, barnehagepersonale og foreldre, forvaltningstjenestemann og parter, kan ses som uttrykk for det integritetsfokuserte personvernet. Slike bestemmelser er med på å verne om den personlige sfære, også etter at personlige forhold er røpet til andre på grunn av et tillits- eller myndighetsforhold. En annen ting er at slike bestemmelser også kan ha andre motiver enn å sikre folks privatliv. F eks kan taushetsplikten for forvaltningstjenestemannen delvis ses som en forutsetning for å sikre en tilstrekkelig opplysning av en sak. Uten taushetsplikt kunne det f eks skje at sakens parter ble mindre åpne og meddelsomme.

3.3.3 Det maktfokuserte personvernet

Den andre typen fokus vi kan velge når personvernet skal forklares, kan sies å gjelde spørsmål om *makt og innflytelse* mellom ulike grupper og/eller personer i samfunnet. Hvis «kunnskap er makt» vil kanskje også kunnskap om andre mennesker gi makt, både i alminnelighet og spesielt over de mennesker kunnskapen gjelder. Ut i fra et slikt ståsted kan det for noen grupper av enkeltpersoner bli viktig å motvirke at andre grupper vesentlig styrker sin posisjon ved å ha tilgang til mye og betydningsfull personinformasjon. I den grad informasjonsteknologi kan anvendes for å skaffe tilgang til personinformasjon, kan det da også oppstå et ønske om å kontrollere teknologibruken.

Det kan f eks være at visse markedsaktører bruker informasjonsteknologi for å kartlegge våre forbruksmønstre og vaner for øvrig så godt at de blir i stand til å manipulere oss i vår rolle som kunder. En annen mulighet er at ulike forvaltningsorganer samvirker på måter som gjør at det enkelte organs informasjonstilfang om borgerne blir vesentlig utvidet. Dette kan bli å føre til at det offentligrettslige regimet inntar en ny, strammere og – for noen – uønsket karakter. En tredje mulighet er at arbeidsgivere oppnår vesentlig mer informasjon om sine arbeidstakere. F eks kan adgangskontrollsystemer, telefon- og elektroniske postsystemer og systemer som måler arbeidsprestasjoner, tenkes anvendt slik at det endrer forholdet mellom partene i arbeidslivet. I dette perspektivet kan personvernet ses som en grensegang mot det som av enkelte grupper i befolkningen oppleves som «overdreven» markedsrett, offentlig (og privat) myndighetsutøvelse og arbeidsgiverrett.

Spørsmålet om hva som er en akseptabel fordeling av makt og innflytelse i samfunnet, kan neppe avgjøres ut i fra kriterier som det er samstemmighet om i befolkningen. Det maktfokuserte personvernet kan derfor sies å være en utpreget politisk betont synsvinkel på spørsmål om behandling av personopplysninger. Den enkelte setter forskjellige grenser for hvilke maktmidler ulike grupper skal kunne disponere. Noen godtar f eks at forvaltningen gjennomfører inngående kontroll av borgernes disposisjoner ved å sammenholde store datamengder («registerkople»), andre motsetter seg intensiv kontroll under henvisning til «integritetskrenkelser» og «kontrollsamfunn». Det er også viktig å understreke at et maktfokus på personvernet ikke tilsier noen sementering av eksisterende maktforhold, men gir en foranledning til å registrere og diskutere endringer. En slik politisk ladet personvernsvurdering er ganske forskjellig fra den «det beslutningsfokuserte personvernet» normalt fører med seg (jf straks nedenfor). Når det gjelder det beslutningsfokuserte personvernet vil folk flest i stor grad kunne enes om hva som må kreves for at behandling av personopplysninger skal gi akseptable resultater.

3.3.4 Det beslutningsfokuserte personvernet

Personopplysninger brukes ofte som grunnlag for beslutninger av ulike slag. Listen over situasjoner der ulike beslutningsinstanser treffer avgjørelser om oss kan i vårt velferdssamfunn gjøres uendelig lang: Banken samler f eks inn personopplysninger for å vurdere lånesøknader, legen behandler opplysninger om pasienter for å treffe avgjørelse om et adekvat medisinsk behandlingsopplegg, ligningskontoret benytter opplysninger fra selvangivelse og oppgavepliktige tredjemenn for å fastsette skatt, og skolemyndighetene behandler opplysninger om karakterer for å avgjøre opptak til videregående skoler.

De nevnte eksemplene er likevel tilstrekkelig til å minne om at mange slike beslutninger kan være avgjørende for folks livssituasjon og velferd. Det er også grunn til å peke på at slike beslutninger både treffes innen offentlig og privat sektor, og at det neppe er mulig *generelt* å påstå at den ene sektoren er viktigere for et men-

neskes velferd enn en annen. Slik sett kan velferdssamfunnet sies å ha én offentlig og én privat dimensjon. Den offentlige dimensjonen dekker for det første bl a den myndighetsutøvelse som etablerer plikter for den enkelte, f eks til å betale skatter og avgifter. Dessuten dekker den tildeling av ulike typer rettigheter, f eks trygdeytelser, gunstige lån og støtteordninger, fordeling av tjenestegoder (helse- og sosialtjenester, utdanning mv). Den private dimensjonen av velferdssamfunnet kan eksemplifiseres ved samfunnsviktige institusjoner som arbeidsgivere, banker, forsikringsselskaper, fagforeninger og ulike interesseorganisasjoner. Slike private organisasjoner tilbyr funksjoner og tjenester som ofte kan anses å ha stor velferdsmessig verdi, og som sammen med den offentlige sektor uttrykker en «arbeidsdeling» mht varetakelse av velferd i samfunnet. Sosial sikkerhet er f eks ikke bare avhengig av folketrygdens ytelser, men kan (bl a) også være avhengig av private forsikringsordninger og tariffbaserte ordninger mellom arbeidsgiver og arbeidstakere.

Det faktiske grunnlaget som enkeltavgjørelsene i velferdssamfunnets beslutninger hviler på, har normalt avgjørende betydning for resultatet. Slike beslutningsgrunnlag vil for en stor bestå av personopplysninger, dvs opplysninger som direkte eller indirekte kan knyttes til identifiserbare enkeltpersoner. Derfor blir det viktig å sikre at behandling av slike personopplysninger skjer på måter som kan sies å være egnet til å sikre riktige og rettferdige avgjørelser.

Krav til beslutningsgrunnlag vil ofte stå i sentrum når vi tenker på personvern. Med det beslutningsfokuserete personvernet forutsetter vi at avgjørelser treffes på basis av et sett av personopplysninger, og stiller ut i fra dette krav til behandlingene av opplysningene. Det at en beslutning forutsettes eller forberedes, betyr ikke nødvendigvis at det er aktuelt å treffe beslutninger i umiddelbar framtid. Beslutningsfokuseringen er også aktuell fordi en forutsetter at opplysninger *kan* bli anvendt som beslutningsgrunnlag. Opplysninger om pensjonspoeng vil f eks normalt ikke anvendes med det første, men vil f eks bli beslutningsgrunnlag ved uførhet eller ved oppnådd pensjonsalder. Beslutningsfokuseringen blir selvsagt mindre hensiktsmessig jo større usikkerheten er mht om opplysningen noen gang vil inngå i et beslutningsgrunnlag. En kjenner f eks ikke til at opplysningen røyke- og drikkevaner vil bli brukt i avgjørelser som gjelder deg direkte. Likevel kan det tenkes framtidige situasjoner der muligheten for at slike opplysninger kan bli brukt som grunnlag for enkeltavgjørelser er tilstrekkelig stor til at vi på forhånd tar hensyn til denne muligheten. Man kan da velge å stille krav til bruken av disse personopplysningene *som om* det forelå en virkelig beslutningssituasjon.

På samme måte som det kan være stor forskjell på hvor sikkert det er at en beslutningssituasjon er aktuell, vil det kunne være store ulikheter med hensyn til hvor inngripende og viktige beslutningene er. Her er det et kontinuum fra de klart inngripende/betydningsfulle avgjørelsene (tvangsinnlegging på sykehus, søknad om boliglån), via de viktige avgjørelsene (beregning av forsikringsoppgjør, pris på hjemforsikring, avgjørelse om eksklusjon fra en idrettsklubb), til det som knapt kan kalles avgjørelser eller som bare har minimal interesse (fastlegging av hvem som skal motta informasjon om sykehjemmets orienteringsmøte, kåring av den fineste blomsterkassen i borettslaget). Det beslutningsfokuserete personvernet kan anlegges på alle situasjoner, fra det livsviktige til det latterlige, men er selvsagt primært aktuelt når det står vesentlige interesser på spill. Innenfor offentlig sektor er det således f eks «enkeltevedtakene» som i praksis primært settes i fokus på denne måten, (se forvaltningsloven første ledd § 2 bokstavene a og b), men denne tilnærmingen er likevel ikke avgrenset til slike vedtak.

Det at beslutninger skal være korrekte, er ikke noe en trenger personvernet for å begrunne. I rettssikkerhetstradisjonen ligger det nettopp et krav om at

avgjørelsene skal være riktige, og under et slikt krav må det nødvendigvis ligge et krav om riktig beslutningsgrunnlag. I et tradisjonelt rettssikkerhetsperspektiv har det imidlertid nesten utelukkende handlet om offentlig myndighetsutøvelse. Personverntilnærmingen er spesiell ved at den ikke skiller mellom offentlig og privat sektor (enkelte lands personregisterlovgivning skiller mellom offentlig og privat forvaltning. Danmark har en registerlov for hver sektor). Det kan derfor hevdes at det beslutningsfokuserte personvernet på mange måter representerer et utvidet rettssikkerhetsperspektiv.

I rettssikkerhetstradisjonen har en dessuten ikke lagt spesiell vekt på beslutningsgrunnlaget, herunder heller ikke på personopplysningene. Forvaltningsloven uttrykker f eks bare at saken skal være «så godt opplyst som mulig før vedtak treffes» (§ 17), men uten å angi noe nærmere kvalitetskrav. Ut i fra personvernet er det derimot nødvendig å stille opp detaljerte krav til personopplysninger. I dette forholdet ligger den andre viktige forskjellen mellom rettssikkerhetstenkning og det beslutningsfokuserte personvernet. For det tredje er særlig det beslutningsfokuserte personvernet knyttet til automatisering av avgjørelser, dvs til det å treffe beslutninger om enkeltpersoner ved hjelp av datamaskinsystemer. Derfor er det f eks mer nærliggende å se Husbankens fullstendig automatiserte sammenstillinger av personopplysninger som grunnlag for tildeling av bostøtte i lys av personvern enn f eks å vurdere den lokale sparebankens manuelle vurdering av søknad om lån fra en kjenning og sambygding på samme måte.

Det beslutningsfokuserte personvernet tar langt på vei utgangspunkt i en massesaksbehandling av personopplysninger i henhold til sterkt automatiserte behandlingsmåter. Avgjørelser i offentlig og privat «masseforvaltning» ses mer som resultater av en hensiktsmessig «produksjonsprosess» for å sikre effektivitet og likebehandling enn arbeidsmåter som er tilpasset det enkelte menneskets individuelle ønsker og behov. Slik sett kan disse aspektene ved personvernet sies å supplere og fornye den rettssikkerhetstradisjonen som har forutsatt individuell behandling av enkeltsaker.

3.3.5 Sammenhenger mellom de tre synsvinklene på personvern

Som nevnt i innledningen til dette kapitlet er ikke fokus på henholdsvis integritet, maktforhold og beslutninger uttrykk for «et personvern i tre deler», men representerer et framstillingsmessig grep for lettere å kunne formidle hva det sammensatte personvernbegrepet handler om. Etter at de tre ulike synsvinklene på personvern er presentert, kan det derfor være grunn til å sette dem sammen til ett bredt perspektiv. Eksemplene nedenfor er ment å illustrere noen sammenhenger.

Det er lett å tenke seg situasjoner der bare en av synsvinklene ovenfor trengs for å beskrive de personvernmessige problemstillinger knyttet til innholdet i en situasjon. Personvernaspektene ved at naboen tar bilde av en naken og blek herr Hansen på nudiststranden en vakker sommerdag, kan beskrives på tilstrekkelig måte ved å ta utgangspunkt i spørsmålet om krenkelse av Hansens personlige sfære og integritet. Dersom det i stedet er *fjernsynet* som gjør opptak og disse bildene ses av herr Hansens arbeidsgiver, vil vi i tillegg ha nytte av å se forholdet under synsvinkelen «det beslutningsfokuserte personvernet», f eks fordi arbeidsgiverens observasjon kan lede fram til en beslutning om å stille Hansen til ansvar for skofting. Dersom eksempelet varieres ved å la politiet stå bak kontinuerlig videoopptak på stranden, f eks for å dempe et for stort alkoholkonsum blant ungdom og derved hindre bråk og vold, kan situasjonen muligens best ses i et maktperspektiv: Hansen blir bare en av mange og verken naboen eller arbeidsgiveren får se opptaket. Overvåkning av offentlig sted ved hjelp av videoopptak vil imidlertid kunne diskuteres under syns-

vinkelen «Storebror-samfunnet», og som et spørsmål om «maktbalansen» mellom borger og offentlige myndigheter. Slik bruk av overvåkningsteknikker kan f.eks. få oss til å spørre hvilke virkemidler vi er villige til å godta for å nå gode mål (som de aller fleste er enige om, f.eks. å forebygge mot vold). Et vel utbygget system av videokameraer på badestrender og andre offentlige steder, kan f.eks. oppfattes som et *for* kraftig instrument for kontroll av borgerne. For noen kan frykten for en utvikling mot mer autoritære styresett da komme til å veie mere enn hensynet til å løse rus- og voldsproblemer *på akkurat denne måten*.

Det er også lett å tenke seg eksempler der alle tre måter å fokusere personvernet på blir nyttige på samme tid: Når f.eks. takstmannen fra forsikringsselskapet oppsøker din bolig for å bedømme omfanget av en vannskade og kommenterer hvorledes du har innrettet baderommet, vil dette lett kunne oppleves som en integritetskrenkelse av forsikringstakeren fordi ikke bare skadene, men også intime forhold åpenbares. Takstmannens observasjoner av skaden blir i sin tur grunnlag for avgjørelsen i skadeoppgjøret, og dermed avgjørende for forsikringstakerens økonomiske og velferdsmessige stilling. I tillegg vil omfanget av forsikringsselskapets kunnskap om personlige forhold kunne oppleves som utslag av et regime der selskapet har fått betydelig evne til makt og myndighetsutøvelse overfor «maktesløse» enkeltpersoner. Informasjonsteknologien kan synes å legge til rette for selskaper som «vet alt om deg» (og om alle andre), og som bruker denne kunnskapen for å fremme sine interesser. Selskapet vil av enkelte forsikringskunder da framstå som mektigere enn før teknologien tillot slik utstrakt bruk av personopplysninger, og som *for* mektig sett i forhold til enkelte kunders egen avmektighetsfølelse.

3.4 PERSONVERNINTERESSER

3.4.1 Innledning

Det er i norsk juridisk teori utviklet en modell som beskriver de antatte interessene hos dem som blir registrert, dvs. interessene bak personvernet. Denne modellen er kalt *interessemodellen* og den beskriver personvernet som et knippe ideelle «interesser» som en tillegger enkeltmennesker. Interessemodellen ble utviklet av Dag Ragnar Blekeli og Knut S. Selmer tidlig på 70-tallet (en tidlig framstilling er gitt av Blekeli og Selmer i *Data og personvern*, Universitetsforlaget 1977). De forskjellige interessene, og kanskje spesielt vektleggingen av dem, er gradvis utviklet i tråd med den teknologiske, kulturelle, sosiologiske og politiske utviklingen i samfunnet. Interessemodellen er relevant enten en velger et integritets-, makt- eller beslutningsfokus på personvernet, men *vektleggingen* av interessene vil variere noe avhengig av det fokuset en velger.

Norsk rett bygger på en avveiningsmodell der motstridende interesser må veies mot hverandre. Personregisterloven § 10 om konsesjon til etablering av edb-førte personregistre gir anvisning på en bred interesseavveining der personverninteresser må veies mot de interesser som taler for at opplysningene skal samles inn og behandles. Interessteorien har stor betydning for Datatilsynets avveininger i konsesjonsspørsmål. Nedenfor gis en kort redegjørelse for interessemodellen slik den i dag framstår ("*Interessteorien*" i pkt 3.4.2) og deretter sies det noe om personverninteressene i forhold til andre interesser – konflikt eller interessesammenfall.

3.4.2 Interessteorien

Etter interessemodellen kan personvernet beskrives ved hjelp av sju interesser. Disse har gjerne i teorien blitt delt inn i individuelle og kollektive interesser. De *individuelle* interessene gjelder den enkeltes rett til å ha kontroll med personopplys-

ninger som angår ham selv. De *kollektive* interessene beskriver de interessene folk har som en gruppe (f eks som samfunn) i å ha kontroll med opplysninger om gruppens medlemmer. Hvorvidt dette representerer personverninteresser eller om man her beveger seg over i andre beslektede interesser (f eks alminnelige rettssikkerhetsprinsipper) kan det være uenighet om. Fordi det er vanlig også å inkludere de kollektive interessene i interesseteorien, vil beskrivelsen i dette kapitlet også omfatte slike personverninteresser. Vi vil uansett i dette kapitlet gi en beskrivelse også av disse interessene da de tradisjonelt utgjør en del av interesseteorien.

De individuelle interessene kan angis ved stikkordene *diskresjon, fullstendighet, innsyn og privatlivets fred*. Interessen i diskresjon er sentral, og framstår ofte som personvernets overordnede interesse. Nærmere bestemt gjelder denne interessen muligheten for den enkelte til å kontrollere hvilke opplysninger om ham eller henne som samles inn, hvem som får tilgang til opplysningene, hva de brukes til osv. Det vil variere fra person til person hvor ille man synes det er at opplysninger kommer på avveie. Det vil også avhenge av hvor sensitive opplysningene oppfattes å være. De fleste vil ønske å begrense innsamling av opplysninger til de som er relevante og nødvendige for det formål de skal brukes til. Dette kan være med å forebygge at beslutninger treffes på usaklig grunnlag. Diskresjonsinteressen kan ivaretas både ved begrensninger i registreringsadgangen (jf personregisterloven § 6; nødvendige og relevante opplysninger) og ved begrensninger i utleveringsadgangen (f eks bestemmelser om taushetsplikt eller vilkår i konsesjonen om forbud mot utlevering). Taushetspliktbestemmelser er imidlertid fastsatt i forvaltningsloven og i særlovgivning, det vil si utenfor personregisterloven. I tillegg vil diverse regler om sikring av personopplysninger kunne hindre uautoriseres tilgang til opplysningene.

Med interessen i fullstendighet tenker man på individets ønske om at de avgjørelser som treffes på grunnlag av personopplysninger, blir truffet på et fullstendig og korrekt grunnlag. Ut fra denne interessen kan Datatilsynet komme til å nekte kobling av to registre fordi resultatet av samkjøringen vil gi for mange feil. Det kan imidlertid også være at Datatilsynet kan *kreve* samkjøring av registre dersom det er klare indikasjoner på at dette vil kunne gi riktigere eller mer fullstendige opplysninger. Regler om sletting/retting av uriktige opplysninger (personregisterloven § 8) er begrunnet i interessen i fullstendighet. Også bestemmelser utenfor personregisterloven stiller krav som understøtter fullstendighetsinteressen, f eks forvaltningsloven § 17 som stiller krav til forvaltningsorganers saksutredning.

Den enkelte antas videre å ha en interesse i å være *orientert* om den virksomhet og informasjonsbruk som kan få konsekvenser for ham eller henne. Retten til innsyn er en forutsetning for å kunne forfølge sin interesse i diskresjon og fullstendighet. Foruten ulike regler om innsyn (personregisterloven § 7 og forvaltningsloven § 18), er regler om meldeplikt til den registrerte, f eks ved kredittopplysningsvirksomhet (personregisterloven § 19), utledet fra denne interessen.

Privatlivets fred er angitt som stikkord for den siste «individuelle» personverninteressen. Den skiller seg fra de andre interessene ved at den i mindre grad er knyttet til registrering av personopplysninger. Interessen i privatlivets fred er interessen i å være i fred fra andre, uavhengig av om fredsforstyrrelsen innebærer at personlige opplysninger blir røpet eller ikke. Straffeloven § 390 kan for eksempel knyttes til denne interessen (selv om bestemmelsen gjelder offentlig meddelelse om personlige eller huslige forhold). I den moderne personverndebatten er denne interessen særlig aktuell i forbindelse med ulike former for markedsføringsvirksomhet, f eks telemarketing (markedsføring gjennom telefonoppringing og telefaksforsendelser).

De kollektive interessene kan angis ved stikkordene *en borgervennlig forvaltning, et robust samfunn og et begrenset overvåkningsnivå*.

Interessen i en borgervennlig forvaltning har også vært uttrykt som et ønske om at forvaltningen skal framstå med et menneskelig ansikt. Med en høy grad av automatisering kan det bli vanskelig for borgerne å forstå saksbehandlingen eller resultatet av en sak. Forutberegneligheten kan dermed svekkes. Automatisert behandling kan føles upersonlig og skape en avstand til forvaltningen hvis for mange avgjørelser tas av datamaskiner alene. Hvorvidt man skal kalle dette en personverninteresse eller et alminnelig rettssikkerhetsprinsipp kan være en smakssak. Personregisterloven har ikke regler som direkte ivaretar denne interessen, men reglene som gis ved konsesjon til å opprette personregistre kan inneholde relevante vilkår. Flere bestemmelser i flere andre lover som ikke direkte gjelder personvern kan imidlertid sies å ivareta denne interessen (f eks forvaltningsloven § 24 om begrunnelsesplikt og § 11 om veiledningsplikt. Bestemmelsene er imidlertid i liten grad gitt spesielt med tanke på en automatisert forvaltning).

Interessen i å ha et robust samfunn er også angitt som en annen kollektiv personverninteresse. Dette er samfunnets interesse i at viktige samfunnsfunksjoner ikke blir for sårbare. I informasjonssamfunnet er mange funksjoner avhengig av en pålitelig elektronisk informasjonsbehandling. Interessen i et robust samfunn innebærer et krav om å sikre samfunns viktig informasjonsbehandling. Sammenbrudd i pensjonsutbetalingene fra trygdeetaten er eksempel på en situasjon som kommer i konflikt med interessen i robusthet og fravær av sårbarhet. Den har sin begrunnelse i at en automatisert forvaltning blir sårbar på andre måter og i langt sterkere grad enn en forvaltning som bruker tradisjonelle arbeidsmåter. Samfunnet, og ikke minst forvaltningen, er avhengig av og må håndtere stadig større mengder informasjon. Moderne informasjonsteknologi gir betydelige muligheter for bedre og mer effektiv offentlig tjenesteyting. Det gis helt nye muligheter for utveksling av informasjon mellom saksbehandlere og mellom organisasjoner. På den annen side reiser det også nye problemstillinger om informasjonssikkerhet. En omfattende ødeleggelse av informasjon kan lamme hele grener av den offentlige forvaltning. Dersom man definerer informasjonssikkerhet som sikring av tilgjengelighet, konfidensialitet og kvalitet/integritet, er det tilgjengelighetsaspektet som først og fremst kan knyttes til interessen i et robust samfunn. Sikring av tilgjengelighet innebærer sikker tilgang til informasjon for dem som har lovlig tilgang til den. Personregisterloven har ingen bestemmelser om informasjonssikkerhet, men etter § 8b kan Datatilsynet gi pålegg om sikring av personopplysninger i form av enkeltvedtak.

Interessen i et begrenset overvåkningsnivå er den siste av de kollektive interessene. Det er kanskje en av de interessene det har vært fokusert mest på i personverndebatten. Den dreier seg særlig om behovet for vern mot maktmisbruk og urimeelig kontroll. I store, omfattende offentlige databaser ligger et betydelig makt- og kontrollpotensiale som det er ønskelig å holde under kontroll. Kobling av store, offentlige registre kan gi ytterligere informasjon om borgerne. På bakgrunn av opplysningene kan myndigheter danne seg et bilde av individene, som kan legges til grunn ved beslutninger rettet mot disse. Dette kan frata den enkelte en mulighet til å kunne holde tilbake opplysninger om sitt privatliv, en frihet til å kunne velge hvilken rolle han vil spille i forhold til ulike myndigheter og være premissleverandør til eventuelle avgjørelser som vil berøre ham. Ulike taushetspliktbestemmelser og legalitetsprinsippet kan sette skranker for etableringen av slike kontrollordninger. I tillegg kan Datatilsynet til en viss grad sette grenser for kontrolltiltak gjennom sin konsesjonsbehandling. Dette gjelder særlig ved kobling av registre slik at det oppstår et nytt konsesjonspliktig register. Avgjørelsene på dette området vil imidlertid ofte være politisk ladet, jf framstillingen av det maktfokuserte personvernet, "*Det integritetsfokuserte personvernet*" i avsnitt 3.3.2.

Personverninteressene gjenspeiles i noen grad i personregisterlovens materielle regler og dels også i andre regelsett. Det er imidlertid forutsatt i forarbeidene til loven en videre rettsutvikling av personvernet gjennom praksis. Dette har skjedd, og skjer fortsatt, først og fremst gjennom Datatilsynets avgjørelser i konsesjonsaker. Loven gir i seg selv lite veiledning mht hvordan skjønnsutøvelsen i personregisterloven § 10 skal skje. Interessemodellen benyttes imidlertid for å konkretisere noen generelt relevante skjønnsstema. Personverninteressene framstår derfor som et knippe av interesser som kan bidra til likeartede vurderinger og tiltak vedrørende behandlingen av personopplysninger. Modellen fungerer i første rekke som en «huskeliste» og angir intet helt bestemt og uttømmende innhold. «Interessen i innsyn» angir f eks at den enkelte skal være best mulig orientert om forhold som er knyttet til informasjonsbehandlingen. På hvilken måte interessen bør realiseres og hvorledes den i gitte situasjoner bør konkretiseres, vil imidlertid kunne variere. Kjernen i interessen i innsyn kan sies å være retten til å vite hvilke opplysninger om en selv som blir behandlet. I gitte situasjoner vil imidlertid også krav om f eks å kunne få kjennskap til den virksomhet som forestår behandlingen, eller et krav om å kjenne innholdet av vilkår som er knyttet til konsesjonen for behandlingen av personopplysninger, ses under synsvinkelen «interessen i innsyn». Hver av interessene kan således sies å ha en kjerne med et fast innhold som omgis med og suppleres av et mer situasjonsbestemt innhold. Heller ikke vektleggingen av interessene kan sies å være fast. Hensynet til diskresjon vil f eks typisk få større vekt, jo mer sensitive opplysninger vi har med å gjøre.

3.4.3 Personverninteresser og andre interesser – konflikt eller interessesammenfall?

Personverninteressene er ikke alltid i harmoni med seg selv. Interessene i «diskresjon» og «fullstendighet» innbyr f eks til motstrid og avveining mellom det å spre personopplysninger så lite som mulig og det å få et saksforhold tilstrekkelig opplyst. Selv om det kan være slik innbyrdes spenning mellom personverninteressene, vil den imidlertid kunne løses gjennom en avveining. Uten diskresjonsinteressen ville en kanskje samle inn personinformasjon «så en er på den sikre siden», med diskresjonsinteressen legges det til rette for en prøving av om den enkelte opplysningstype er nødvendig.

Det synes å være en forholdsvis utbredt oppfatning at personvernet ofte står i motstrid med interesser som ikke representerer personvern, spesielt i forhold til interessen i effektivitet (særlig kostnadseffektivitet), kommersielle interesser, interessen i en effektiv etterforskning i straffesaker, tilbud om et adekvat helsetilbud til befolkningen, forbrukerinteresser m v. Det er imidlertid grunn til å advare mot fastlåste oppfatninger om konflikter og sammenfall mellom personverninteresser og slike andre interesser. Riktignok eksisterer det ikke sjelden helt reelle motsetninger. Dersom en bedrift f eks ønsker å registrere opplysninger om sine ansattes helseforhold og dette nektes av Datatilsynet, kan det sies å være motstrid mellom personvernet (diskresjonsinteressen) og (f eks) bedriftens ønske om kontroll med sykefravær og en tilhørende økonomisk gevinst (ønsket om lavt sykefravær). Særlig diskresjonsinteressen vil lett komme i konflikt med andre interesser, fordi den bidrar til å hindre tilgang og bruk av informasjon. Når det gjelder andre aspekter ved personvernet, er det imidlertid ikke vanskelig å peke på tilfeller der det snarere er sammenfall enn konflikt med andre interesser som dominerer bildet. Et kredittopplysningsbyrå vil f eks være interessert i at de opplysningene de disponerer er korrekte og dekkende, noe personverninteressene i innsyn og fullstendighet også begrunner. En annen ting er at den som driver kredittopplysning kan ha en noe høy-

ere toleranse for feil enn den enkelte som det behandles opplysninger om. Når virksomheten vurderer opplysninger om mange personer som en helhet kan en feilprosent på 5 være et akseptabelt kvalitetsnivå. Samtidig kan dette være totalt uakseptabelt for de enkeltpersoner som rammes av feilforekomstene. Selv om styrken i kravene således kan være forskjellige avhengig om en f eks tar utgangspunkt i forretningsdrift eller personvern, er det ikke sjelden den samme type krav som stilles, og likeartede tiltak som er aktuelle uavhengig av utgangspunkt. Det kan imidlertid være et problem at den som forestår behandling av personopplysninger ikke alltid har innsett hvor viktig en høy informasjonskvalitet er for eksempel for å oppnå en tilfredsstillende forretningsdrift eller effektiv myndighetsutøvelse. I lys av den tilsynelatende økte vektlegging av «informasjonskvalitet» og «informasjonssikkerhet», kan det i framtiden være mulighet for et mildere møte ved at også interessenammenfall mellom personverninteresser og andre involverte interesser kan gis oppmerksomhet.

Det er viktig å understreke at det ikke er grunn til å gå ut i fra at personverninteressene står mot «alle andre» interesser. Der det kan påvises konflikt, er det ingen grunn til i utgangspunktet å regne med at denne er av en bastant karakter. Selv om personverninteressene fikk råde alene, er det heller ikke slik at disse alltid vil gi klare svar. Disse oppfatningene om forholdet mellom personvernet og dets «omgivelser» har bl a den konsekvens at en bør gå konkret til verks i avveiningene, uten fastlåste holdninger, men snarere med et åpent sinn for mulige «allianser» mellom personvern og kostnadseffektivisering, forbrukervern m v, enn med forventninger om motsetninger. En annen konsekvens kan være at det er flere myndighetsinstanser og aktører for øvrig som kan tenkes å støtte opp under personvernet: Når f eks Riksrevisjonen og Kredittilsynet stiller krav til informasjonskvaliteten i data-systemer innen henholdsvis statsforvaltning og finansinstitusjoner, vil dette også kunne fremme personvernet. Fordi «personopplysning» favner vidt (se 10.1.3), er det meget praktisk å tenke seg at slike instanser stiller krav til relevante systemer. Ikke minst vil forbrukermyndighetene kunne fremme personvern gjennom sitt virke for å ivareta kundeinteresser. Urimelig «markedsaktør» hos store aktører vil føre til krav fra Forbrukerrådet eller andre om å regulere informasjonsbehandlingen i tilknytning til kundeforhold. Et aktuelt eksempel kan være kritikk fra forbrukermyndigheter mot forsikringsselskapers omfattende krav til framlegging av helseopplysninger ved tegning av livsforsikring. Også en privat markedsaktør som selger adresseopplysninger m v og som vektlegger en høy kvalitet på «produktet» (personopplysningene), vil på lignende måte tjene sider ved personvernet, selv om det primært er forretningsdriften som motiverer kravet til kvalitet.

KAPITTEL 4

Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet

4.1 RAMMEVILKÅR OG FORVENTNINGER

Det norske velferdssamfunnet gjør det i stor grad nødvendig å gjøre omfattende og intensiv bruk av personopplysninger. I mange sammenhenger skjer anvendelsen av slike opplysninger med et omfang og på en måte som gjør det påkrevet med en intensiv bruk av informasjonsteknologi. På en rekke områder er det nødvendig at den enkelte gir opplysninger om seg selv før tjenester og goder kan ytes eller plikter oppfylles. Banken krever opplysninger om inntekts-, formues- og arbeidsforhold før de gir lån. Trygdeytelser gis først hvis bestemte vilkår er oppfylt, og stipend for utdanning er behovsprøvd.

Anvendelse av informasjonsteknologi har lenge vært et satsingsområde for både offentlig og privat sektor. I løpet av de senere årene har det framkommet flere signaler fra regjeringen om en bred satsing innen informasjonsteknologi. Satsing på informasjonsteknologi framheves som et vilkår for bl a en tilfredsstillende utvikling innen det økonomiske liv, for tilfredsstillende tjenesteyting til befolkningen og for nødvendig omstilling av offentlig sektor.

Realiseringen av informasjonssamfunnet innebærer ikke bare en satsing på teknologien (utvikling/produksjon og anvendelse av program- og maskinvare), men også satsing på informasjonen, informasjonstjenester og informasjonsbehandling som får økende betydning for økonomien. Det er således store forventninger til det økonomiske potensialet i informasjonsmarkedet, dvs i tilknytning til kjøp og salg av den informasjon som behandles av maskin- og programvaren, herunder handel med bearbeidet/videreforedlet informasjon. Tilsvarende gjelder i de fleste vestlige land, i EU og innenfor rammene av G7-samarbeidet. Spørsmål om hvordan man skal bygge globale informasjonsstrukturer og hvordan man skal vareta viktige hensyn i det globale informasjonssamfunnet står på dagsordenen.

Den økonomiske betydningen av informasjon, herunder personinformasjon, utgjør en viktig ramme for den regulering av personvernet som vil skje innenfor rammene av EFs direktiv om personvern. Felles personvernregulering skal både tjene personvernet og et fritt informasjonsmarked mellom landene. Det er grunn til å tro at satsingen på IT generelt og på informasjonsmarkedet spesielt, vil gjøre det mer utfordrende enn tidligere å ivareta personvernet. Selv om deler av informasjonen i framtidens informasjonsmarked vil være informasjon som er knyttet til aggregerte data, virksomhetsopplysninger m v, er det samtidig klart at meget av informasjonen vil være personinformasjon og således være gjenstand for personvernmessige vurderinger. Dette kan bidra til at økonomiske-/næringsmessige interesser vil bli knyttet til personopplysninger i større grad enn tidligere, og således skape grobunn for et høyere konfliktnivå. Når informasjonsmarkedet vokser, vil også antallet slike mulige konflikter øke, se "*Personverninteresser og andre interesser – konflikt eller interessesammenfall?*" i avsnitt 3.4.3 (foran). Spørsmål knyttet til personvern er derfor kanskje blant de mest krevende problemstillingene vi står overfor ved fremveksten av informasjonssamfunnet både globalt og nasjonalt.

4.2 ØKT INFORMASJONSTILGANG HAR KONSEKVENSER FOR PERSONVERNET

Man kan få inntrykk av at ny teknologi – vurdert ut i fra personvern hensyn – utelukkende er en trussel. Dette er ikke riktig. Som det framgår av Datatilsynets årsmelding fra 1995 s 26:

«Ny teknologi er i utgangspunktet verken positiv eller negativ for personvernet. Det er hvordan vi anvender teknologien og hvordan vi legger premisene for utviklingen av ny teknologi som bestemmer om teknologien skal styrke eller svekke personvernet.»

Med denne betraktningen i mente går vi over til å se på de ulike måtene ny teknologi gjør det mulig å samle inn mer informasjon på en raskere måte enn tidligere.

Tidligere ble personinformasjon samlet inn og registrert i datamaskinsystemene ved at noen mennesker leste utfylte skjemaer og tastet opplysningene inn i systemet. Det er fremdeles slik at personopplysninger i stor grad blir tilgjengelig for datamaskinbehandling på denne måten. Ny teknologi har imidlertid lagt til rette for at personopplysninger i større grad kan samles inn kun en gang og dessuten på andre og raskere måter og i større omfang enn tidligere. Nedenfor pekes det på noen slike utviklingstrekk som f eks scanning og opptak/måling av personers handlinger/tilstander. Det vises også at den enkelte borger selv bidrar til innsamlingen av data ved å etterlate seg såkalte «elektroniske spor». Til slutt gis det et par eksempler på hvilke konsekvenser bruken av ny informasjonsteknologi har for samfunnet.

For det første blir *scanning* av opplysninger som den enkelte oppgir på fastlagt blankett, i økende grad benyttet for en rask og billig informasjonsinnhenting. Således blir f eks bankgiroer, meldekort fra arbeidsledige og søknadsskjemaer fra elever ved opptak til videregående skoler, gjenstand for scanning. Scanningen innebærer bl a en digitalisering som gjør det mulig å behandle opplysningene videre ved hjelp av datamaskinsystemer. Scanningsteknologien kan både sies å legge til rette for en billigere og en økt innsamling av personinformasjon.

For det andre anvendes ulike typer utstyr for opptak og/eller måling av personers handlinger og tilstander på måter som innebærer digitalisering. Digitalisering gjør det mulig å gjenfinne og behandle den personinformasjonen som finnes i det innsamlede materialet ved hjelp av edb. Fjernsynsovervåkning og opptak fra ekspedisjonslokaler i banker og postkontorer kan være eksempel på slik informasjonssamling. Digitaliserte bilder og/eller lydopptak gjør det mulig å gjennomføre analyser for f eks identifisering av personer, av deres tale og opptreden m v. Med de identifiseringsmuligheter som digitaliseringen gir, vil et billed- eller lydopptak av en folkemengde kunne ses på som et «personregister» i henhold til gjeldende lovgivning. Organisk materiale fra mennesker vil på lignende måte legge til rette for analyser ved hjelp av utstyr som genererer analyseresultater i form av maskinlesbare personopplysninger. Selv om slike resultater i dag ofte ikke foreligger i digitalisert form, men må registreres manuelt etter at prøvene foreligger, er det grunn til å tro at resultatene i stigende grad vil bli direkte maskinlesbare.

Et viktig trekk ved den type teknologi som gjør opptak av menneskers handlinger/hendelser og som registrerer tilstander m v, er at slikt materiale kan gi store mengder personinformasjon. Med opplysninger som inngis på skjemaer er graden av formalisering så høy at registreringen gir få andre opplysninger enn de det direkte legges opp til å samle inn gjennom det formaliserte opplegget. Av verdien «ja» i feltet «forsørger barn over 18 år?», kan det således ikke utledes stort annen informasjon enn det som direkte sies. Annerledes er det dersom de data som foreligger ikke er undergitt noen sterk grad av formalisering, f eks slik som når det fore-

ligger opptak av lyd og bilde, eller en forekomst av et fysisk/biologisk materiale er gjort tilgjengelig. Moderne informasjonsteknologi gjør at vi får langt mer informasjon ut av ett datasett enn tidligere. Forekomsten av et hårstrå vil f eks uten bruk av ny teknologi kunne gi opplysning om det dreier seg om et menneskehår eller ikke, om hårfarge og antagelser om personens alder og kosthold. Med genteknologiske metoder og kunnskap om genetikk, vil en imidlertid på entydig måte kunne føre håret tilbake til en bestemt person, og en vil kunne slutte en rekke ting om denne personens helseforhold, arvelige disposisjoner m v. Fra enkelte informasjonsdatabærere kan vi m a o høste langt mer informasjon enn tidligere, og meget av denne informasjonen vil gå tett innpå de personer det gjelder. I tillegg vil vi ikke alltid egentlig vite hva slags opplysninger det innsamlede datamaterialet kan gi oss tilgang til, fordi det i framtiden kan utvikles nye analysemetoder som kan generere nye spørsmål og gi nye typer resultater i form av personopplysninger.

Opplysninger som er samlet inn og analysert er ikke bare svar personer har avgitt og derfor uttrykk for enkeltindividers subjektive meninger (som når vi fyller ut et skjema), men er opplysninger med naturvitenskapelig autoritet. Det kan oppstå særlige utfordringer for personvernet dersom slike opplysninger blir gjenstand for utveksling og anvendes utenfor det vitenskapelige miljøet som har kompetanse til å bedømme opplysningenes korrekthet m v.

Samfunnets informasjonsgrunnlag øker også i volum pga de registrertes *egne* bidrag til registreringen av personopplysninger. For det første innebærer bruk av ulike korttjenester ofte at det genereres personopplysninger, f eks ved kjøp ved en betalingsterminal eller ved uttak fra minibank. Det sterkt økende omfanget av korttjenester, slik som ved de mer enn 20.000 betalingsterminalene i Norge, gjør at persondata registreres kontinuerlig og i store mengder. Selv om hver enkelt slik registrering kan være banal og lite sensitiv, vil *summen* av slike data knyttet til en person kunne gi et intimt bilde av personens forbruks- og bevegelsesmønster m v. Den enkelte opplysning som vi rutinemessig etterlater som ledd i ulike gjøremål kalles ofte «elektroniske spor». Hver for seg er slike «spor» ofte uskyldige. En større samling av elektroniske spor i form av *personprofiler*, som er satt sammen for å danne et bilde av personers preferanser, holdninger, bevegelsesmønstre m v, vil imidlertid ofte oppfattes som sensitive opplysninger. På lignende måte vil det genereres store mengder «spor» gjennom logging av telefon- og elektroniske postsystemer, bruk av Internettjenester, elektroniske oppslagstavler m v. Spørsmål vedrørende elektroniske spor vil bli stadig viktigere, hvilket gjør det nødvendig med klare holdninger til hvilke formål det er akseptabelt å anvende slik informasjon.

Utvikling av ulike typer *overvåkingsteknologi* er en særlig iøynefallende del av de senere årenes teknologiske utvikling. Dette er teknologi som er utviklet med det formål å holde oppsikt med personers bevegelser og adferd. For det første gjelder dette fjernsynsovervåkning (med eller uten opptak) av gater, bygninger, arbeidsplasser m v. I tillegg til opptak er det eksempler på vid spredning av bilder fra offentlig sted via Internett, og muligheter for å fjernstyre opptaket. Fjernsynsovervåkning ble fra 1993 regulert i personregisterloven, og skal i henhold til straffeloven § 390 b varsles. Varslingen kan gjøre det mulig for folk å innrette seg etter overvåkingen, eventuelt ved å unngå å oppholde seg på overvåkete område.

Fjernsynsovervåkingen har etterhvert fått et omfang som i realiteten gjør det meget problematisk å unngå å bli overvåkete selv om overvåkingen varsles. Slik overvåking er i ferd med å endre karakter fra å være unntaket til å bli regelen. Dessuten har ny teknologi gjort at tradisjonell overvåking – hvor det har vært liten avstand mellom den som overvåkes og overvåkeren eller dennes utstyr – til dels er blitt erstattet med overvåkningsutstyr med mye lengre rekkevidde. Dette fører til at overvåkingen av den grunn både får større omfang og blir vanskeligere å oppdage

(enkelte fjernsynskameraer kan brukes på flere kilometers avstand). Til en viss grad kan det sies at den teknologiske utviklingen har gjort at tradisjonelle personverngarantier for den enkelte (f eks kravet om varsel) har blitt av mindre verdi enn tidligere.

Informasjonsteknologien ser også ut til å erstatte menneskelig observasjon av personers adferd m v. Dette er særlig aktuelt når adferden regnes som risikofylt for vedkommende person eller når den som på annen måte oppfattes som uønsket. Således er det utviklet teknologi med sensorer som f eks gjør det mulig å avgjøre om en aldersdement person ligger i sengen eller ikke, eventuelt som varsler dersom vedkommende nærmer seg utgangsdøren. Lignende teknologi har åpnet for «hjemmefengsel» ved at teknologien skaffer oversikt over en persons oppholdssted og adferd.

Med integritetsfokus på personvernet er disse og andre utviklingstrekk bekymringsfulle. I et integritetsperspektiv er det problematisk at vedvarende eller hyppig overvåkning av adferd reduserer deler av individenes «private rom» og usjenert personlig utfoldelse. Dette må både oppfattes som et problem for folk flest og kanskje særlig for de mennesker som i dag kun har en meget begrenset mulighet for å opprettholde et privatliv, fordi de må underlegges særlig omsorg eller er utsatt for samfunnets straff.

Økningen med tilgjengelighet til og anvendelse av overvåkningsteknologi reiser også noen grunnleggende spørsmål om endringer av personlige relasjoner i samfunnet. Bruk av ulike typer av overvåkningsteknologi kan f eks gjøre det mulig å effektivisere deler av helse- og hjelpeapparatet ved at helsearbeidere erstattes med fjernstyrt observasjon. «Privatlivets fred» tåler godt andres omsorg, men tåler dårligere vedvarende observasjon.

4.3 FRA REGISTRE TIL ANNEN ORGANISERING AV PERSONOPPLYSNINGER

Framstillingen ovenfor viser at ny teknologi har ført til at det tradisjonelle registerbegrepet i mange tilfelle ikke lenger er dekkende. Dette er noe av bakgrunnen for at utvalget senere i utredningen ("*Lovens saklige og geografiske virkeområde*" i kapittel 10) konkluderer med at den nye loven generelt bør fokusere på elektronisk *behandling* av personopplysninger, samt visse former for manuell *behandling*.

Den gjeldende norske loven har «personregistre» som et av sine sentrale begreper. Registerbegrepet gir assosiasjoner til *fysiske samlinger* av opplysninger slik vi er vant til fra papirarkiver der opplysningene f eks ligger i alfabetisk eller kronologisk orden. Lovens definisjon av «personregistre» forutsetter at opplysningene skal være «lagret systematisk» slik at opplysningene kan gjenfinnes.

Lenge ble datamaskiner anvendt slik at lagring og gjenfinning av opplysninger ikke var helt ulik framfinning av opplysninger i papirdokumenter, ved at ett sett av opplysninger lå fysisk samlet på et maskinlesbart lagringsmedium der opplysningene ble individualisert ved hjelp av en eller flere «nøkler», f eks personnummer/kundenummer og/eller personnavn. Ved samkjøring av to eller flere registre som genererte nye lister med personopplysninger (f eks ett register over sykehjemsbeboere og ett register over personer med formuesinntekt), ble denne nye kombinasjonen av opplysninger regnet som et nytt personregister i lovens forstand.

Det er flere forhold ved den tekniske- og organisatoriske utviklingen som gjør at registerperspektivet på behandling av personopplysninger ikke lenger er så enkel å opprettholde. For det første har den tekniske infrastrukturen gjort det vesentlig lettere å få tilgang til opplysninger som fysisk er plassert ett eller flere andre steder. Utbygging av infrastruktur for å muliggjøre kommunikasjon mellom tidligere «iso-

lerte» datamaskinsystemer har vært en målsetting for den norske og andre lands regjeringer. Etablering av nett for departementene, for hele den regionale offentlige statsforvaltning og for store landsdekkende statsetater er eksempler på at målsettingen kan realiseres. Under forutsetning av at det foreligger en teknologisk infrastruktur som nevnt, og at det finnes datamaskinprogrammer som knytter disse opplysningene sammen til en logisk enhet, kan det anses å foreligge et personregister selv når opplysninger om 100 personer finnes på 100 forskjellige steder.

Selv om mange personopplysninger også i dag ligger fysisk samlet, er det i stigende grad mulig å organisere og behandle opplysninger uavhengig av avstand. Med dagens muligheter for å få tilgang til opplysninger via moderne telekommunikasjon kan det dessuten lett oppstå ønsker om å benytte flere eller andre opplysninger enn tidligere. Tilgjengeligheten kan også gjøre bruksmønsteret mer komplisert og mindre stabilt enn tidligere. For en gruppe mennesker (f eks utenlandske statsborgere) kan det tenkes at opplysninger om bosted hentes fra en annen kilde enn opplysninger om arbeidsforhold, selv om bostedsopplysningen også finnes sammen med opplysninger om arbeidsforholdet. Årsaken kan f eks være at den alternative kilden anses å ha høyere kvalitet på sine bostedsopplysninger når det gjelder denne persongruppen. Samtidig er det en rekke lovbestemte begrensninger knyttet til den som kan anvende eller få tilgang til informasjon. Dette reguleres bl a av taushetspliktbestemmelser og ikke minst gjennom de krav personvernet stiller.

Kommunikasjonsteknologi gjør det også lettere enn tidligere å la opplysninger krysse landegrensener (se nærmere "*Forholdet til ytringsfriheten*" i kapittel 17 nedenfor). For det første pågår det en internasjonalisering av viktige deler av politikken, noe som bl a resulterer i felles forvaltnings- og rapporteringsordninger innen EU/EØS. For det andre utvikler store deler av informasjonsmarkedet seg i en internasjonal retning. For det tredje har det skjedd en økende grad av internasjonalisering av næringsvirksomhet generelt, noe som igjen kan sies å skape et press mot friere bevegelse av den informasjon som inngår i ulike deler av virksomhetene. For det fjerde er det gjennom lang tid bygget opp systemer som er basert på rutinemessig og nødvendig persondatatrafikk over landegrensener (f eks innen betalingsformidling og ulike Internett-tjenester).

Flere av de utviklingstrekk som her er nevnt legger til rette for at persondata i framtiden vil utveksles friere enn tidligere. De samme faktorene peker i retning av et større volum av opplysninger og en høyere omløpshastighet. Dersom disse framtidsutsiktene realiseres, vil det særlig bli vanskeligere enn tidligere å ivareta personverninteressen i diskresjon, fordi det kan bli mer begrensede muligheter til å forby og/eller innskrenke utveksling av de fleste typer personopplysninger. På den annen side vil en slik utvikling styrke begrunnelsen for å ivareta ulike kvalitetskrav til informasjonsbehandlingen. Det forhold at opplysninger som er fysisk spredt benyttes som om de inngår i en felles informasjonssamling gjør at det blir nødvendig å enes om felles definisjoner av de opplysningstyper som skal utveksles, dvs å ha samsvarende forståelse av hvordan persondata skal fortolkes. Hvis det f eks skal utveksles opplysning om et «hushold» er det av avgjørende betydning at det finnes en felles definisjon av denne opplysningstypen og at det følges felles retningslinjer ved fortolkning og avgjørelse av tvilstilfelle. Dette blir ytterligere komplisert dersom det gjelder et samarbeid over landegrensener og mellom ulike språk.

Uavhengigheten av fysisk plassering skaper også utfordringer med hensyn til den enkeltes mulighet til å få overblikk over den aktuelle informasjonsbehandlingen. Når datamaskinprogrammer styrer trafikk av personopplysninger mellom flere behandlingsinstanser, vil denne behandlingen lett bli så innfløkt og omfattende at det kan bli vanskelig å skaffe seg kunnskap om den. Et kompliserende element er at

en kan trenge kunnskap om *mange* aktørers forhold, i stedet for bare én «registreiers» rutiner og systemer.

4.4 PERSONOPPLYSNINGER UTENFOR ELEKTRONISKE MEDIER

I det foregående er det i første rekke fokusert på personopplysninger i maskinlesbar form. Det er imidlertid grunn til å minne om at personvern i høy grad også er aktuelt *utenfor* de maskinelle rutinene. Særlig er det grunn til å peke på sammenhengen mellom manuell og maskinell behandling av personopplysninger. For det første er det grunn til å tro at økt tilgjengelighet til personopplysninger i datamaskinsystemer vil gi større mengde personopplysninger på papir fordi det tas utskrift fra datamaskinsystemene. Slike utskrifter skaper store utfordringer m h t varetakelse av diskresjonsinteressen, og det kan bli også være et problem å verifisere at papirdokumenter inneholder troverdig og oppdatert papirinformasjon. Økende spredning av personopplysninger i datamaskinsystemer og på papir, vil dessuten generelt kunne skape større kunnskap om folks personlige forhold. Fordi opplysningene ofte er undergitt en sterk grad av formalisering, vil opplysningene imidlertid kunne framstå som fragmenterte og ute av sin sammenheng. Lettere tilgang til maskinlesbar personinformasjon, f eks via søkemaskiner på Internett, vil også kunne stimulere massemedia (ukeblader, aviser, radio- og tv-kanaler m v) til å gjøre journalistisk arbeid som i sterkere grad enn tidligere er knyttet til folks personlige forhold. Muligheten for kritisk journalistikk vil ikke i seg selv være sikret gjennom eksistensen av Internett-nettverkstjenester, men er i stor grad avhengig av det innhold slike tjenester kan tilby. En videre vektlegging av underholdning og «lettere stoff» på World Wide Web, vil f eks kunne danne grunnlag for en økende personfokusering i massemedia og ellers.

KAPITTEL 5

Personregisterloven med forskrifter

Personregisterloven ble vedtatt 9 juni 1978 og er senere endret flere ganger. Til grunn for loven lå to utredninger. I NOU 1974: 22 Persondata og personvern la et utvalg ledet av Tore Sandvik fram forslag til lov om innsamling, registrering, bruk og meddelelse av personopplysninger i privat virksomhet. I NOU 1975: 10 Offentlige persondatasystem og personvern la et utvalg ledet av Helge Seip fram forslag til lov om persondatasystem som opprettes av organ for stat eller kommune. Sammen dannet disse utredningene grunnlag for Ot prp nr 2 (1977-78) om lov om personregistre mm, jf også Innstilling O nr 47 (1977-78).

I 1987 (lovvedtak 12 juni 1987 nr 55) ble loven endret på en rekke punkter. Det ble blant annet lovfestet en plikt for registreiere til å bistå Datatilsynet ved kontroller mv (personregisterloven § 5), og det ble lovfestet en rett for den enkelte til å få sperret sitt navn i forbindelse med utsending av reklame som skjer med bakgrunn i personregistre (personregisterloven § 8 a). Forarbeidene til endringsloven er Ot prp nr 34 (1986-87) og Innst O nr 64 for 1986-87. Til grunn for disse endringene lå en utredning av tidligere kontorsjef i Datatilsynet Arve Føyen (utredningen er trykt i Complex 1/83 og som vedlegg nr 6 til St meld nr 14 (1983-84), og betegnes heretter som Føyenutredningen. Sidehenvisninger gjelder Complex-utgaven).

I 1993 (lovvedtak 11 juni 1993 nr 78) ble loven endret på nytt, ved at det ble tilføyd et nytt "*Oversikt over andre internasjonale reguleringer og andre lands rett*" i kapittel 9 a om fjernsynsovervåkning, jf Ot prp nr 56 (1992-93) og Innst O nr 91 (1992-93).

Personregisterloven gir generelle regler om registrering og informasjonsbehandling i organ for stat eller kommune og for privat næringsvirksomhet, foreninger eller stiftelser. Loven omfatter ikke bare opprettelse av personregistre (manuelle kartotek/arkiver såvel som elektroniske registre), men også annen bruk av personopplysninger i visse typer virksomheter. Personregisterlovens anvendelsesområde er nærmere beskrevet i "*Lovens saklige virkeområde*" i kapittel 10.1 nedenfor.

Kapittel 2 i loven inneholder reglene om kontrollorganet Datatilsynet, som ble etablert 1 januar 1980. Datatilsynet avgjør om det skal tildeles konsesjon i henhold til personregisterloven § 9, og foretar for øvrig kontroll i tillegg til å drive generell opplysningsvirksomhet innenfor sitt myndighetsområde. En nærmere redegjørelse for Datatilsynet finnes i "*Sanksjoner*" i kapittel 19 nedenfor.

"*Hva er personvern?*" i Kapitlene 3 og "*Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet*" i 4 gir materielle regler om opprettelse og bruk av personregistre. Mens "*Hva er personvern?*" i kapittel 3 inneholder alminnelige regler om personregistre, f eks saklighetskrav til registrering, innsynsrett og rette-/sletteplikt, etablerer "*Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet*" i kapittel 4 konsesjonsplikt for et stort antall registre. Nærmere omtale av disse reglene gis nedenfor i "*Regulering og kontroll*" i kapittel 12 og "*Særlige regler for visse virksomheter*" i 13.

"*Personregisterloven med forskrifter*" i Kapitlene 5- "*Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger*" i 8 regulerer bruk av personopplysninger i visse typer virksomheter: Kreditt- og personopplysningsvirksomhet ("*Personregisterloven med forskrifter*" i kapittel 5), databehandlingsforetak ("*Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern*" i kapittel 6), adresserings- og distribusjonsvirksomhet

(*"Europarådets konvensjon og rekommandasjoner om persondataskyttelse"* i kapittel 7) og opinions- og markedsundersøkelser (*"Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger"* i kapittel 8). Reglene for særlige virksomheter behandles i *"Særlige regler for visse virksomheter"* i kapittel 13 nedenfor.

Lovens *"Oversikt over andre internasjonale reguleringer og andre lands rett"* i kapittel 9 regulerer overføring av personopplysninger og personregistre til utlandet, se nærmere *"Tilsynsmyndigheten"* i kapittel 18 nedenfor.

"Oversikt over andre internasjonale reguleringer og andre lands rett" i Kapittel 9a som omhandler fjernsynsovervåkning, ble tatt inn i loven ved lov 11 juni 1993 nr 78, og trådte i kraft 1 januar 1994. Bestemmelsene regulerer fjernsynsovervåkning og billedopptak i de tilfeller billedopptaket ikke utgjør et personregister i lovens forstand. Regler for fjernsynsovervåkning behandles i *"Fjernsynsovervåkning og annen elektronisk overvåkning"* i kapittel 14.

"Lovens saklige og geografiske virkeområde" i Kapittel 10 inneholder bestemmelser om straff og erstatning (se (nytt) *"Økonomiske og administrative konsekvenser av utvalgets forslag"* i kapittel 20 nedenfor), mens regler om ikraftsetting finnes i loven kapittel 12. Justisdepartementet har i medhold av personregisterloven gitt fire forskrifter; 21 desember 1979 (sist endret 2 desember 1996) heretter personregisterforskriften, 12 desember 1988 (om årsavgift for foretak som er konsesjonspliktige etter loven), 1 juli 1994 (om fjernsynsovervåkning) og 23 mars 1995 (om fritak fra konsesjonsplikt for finansinstitusjoner – hvitvasking av penger). Ved kgl res 21 desember 1979 er dessuten flere typer personregistre unntatt fra personregisterlovens anvendelsesområde.

Forskrift 21 desember 1979 er personregisterlovens hovedforskrift. Forskriften *"Sammendrag av personregisterlovutvalgets utredning"* i kapittel 1 har nærmere bestemmelser om innsynsretten etter personregisterloven § 7. *"Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte"* i Kapittel 2 gjør en rekke unntak fra konsesjonsplikten etter personregisterloven § 9. Det er knyttet en rekke vilkår til disse konsesjonsfritakene; bestemmelser om registrenes innhold, bruk mv (*"Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte"* i kapittel 2 og *"Hva er personvern?"* i 3). I *"Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet"* i kapittel 4 – 7 er det gitt bestemmelser om de forskjellige virksomhetene som i henhold til personregisterloven er underlagt konsesjonsplikt, og *"Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger"* i kapittel 8 fritar fra konsesjonsplikten etter personregisterloven § 36 (overføring av personopplysninger til utlandet) og etablerer en meldepliktsordning i stedet. *"Oversikt over andre internasjonale reguleringer og andre lands rett"* i Kapittel 9 inneholder en bestemmelse om straff.

En nærmere framstilling og vurdering av forholdet mellom lov og forskrift gis i kapittel 21.2. De enkelte reglene i personregisterloven er nærmere kommentert i del II som bakgrunn og utgangspunkt for utvalgets vurderinger.

KAPITTEL 6

Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern**6.1 ANNEN LOVGIVNING OM BEHANDLING AV PERSONOPPLYSNINGER****6.1.1 Innledning**

Personvern generelt og behandling av personopplysninger spesielt varetas ikke bare av personregisterloven, men også av en rekke andre lover og lovbestemmelser. Nedenfor gis en oversikt over noen av de viktigste av disse, for på den måten å plassere personregisterloven i en større rettslig sammenheng. For å få et helhetssyn på normer om personvern må perspektivet gjøres enda videre; avtalefestet personvern omtales under 6.3, mens ulovfestede regler om personvern – både rettslige og sosiale/etiske regler – behandles under 6.4.

6.1.2 Straffelovens regler om ærekrenkelser

Hovedbestemmelsene i straffeloven kapittel 23 om ærekrenkelser er §§ 246 og 247, som angir rammen for hva som er ærekrenkelse. Mens § 246 verner den enkeltes æresfølelse, verner § 247 omdømmet. Bestemmelsene rammer først og fremst usanne ærekrenkelser. Sanne ærekrenkelser er i utgangspunktet ikke rettsstridige, medmindre fremsettelsen av dem er utilbørlig, jf straffeloven § 249 nr 2. Heller ikke usanne ærekrenkelser er alltid straffbare, jf straffeloven § 249 nr 3. Rettsstridige ærekrenkelser kan ikke bare medføre straffansvar, men også mortifikasjon (jf straffeloven § 253 nr 1) og erstatningsansvar.

6.1.3 Vern av privatlivets fred

Straffeloven § 390 hjemler straff for «den som krenker privatlivets fred ved å gi offentlig meddelelse om personlige eller huslige forhold». Denne regelen om vern av «privatlivets fred» var den viktigste lovfestede regelen om vern av personligheten inntil vi fikk personregisterloven i 1978. Tidligere ble denne regelen brukt om forhold som i dag naturlig omfattes av personregisterloven.

6.1.4 Telefonavlytting og annen telefonkontroll

Straffeloven § 145 a forbyr hemmelig avlytting av samtaler mellom andre. Doms-tolene kan imidlertid gi politiet tillatelse til slik avlytting i to typer saker; forbrytelser mot rikets sikkerhet og – mer praktisk – i narkotikasaker (jf straffeprosessloven kapittel 16 a). I narkotikasaker kan opplysninger fra telefonavlytting m m kun brukes til hjelp under etterforskningen, og ikke benyttes som bevis i en eventuell retts sak (straffeprosessloven § 216 tredje ledd). Informasjon som ikke er av betydning for straffbare forhold, skal snarest tilintetgjøres (straffeprosessloven § 216 g).

6.1.5 Gjengivelse eller visning av personbilde

Åndsverkloven § 45c forbyr i utgangspunktet gjengivelse eller offentlig visning av et fotografi som avbilder en person uten samtykke fra vedkommende. Det er visse unntak fra bestemmelsen, blant annet dersom avbildingen har aktuell og allmenn interesse, eller avbildingen av personen er mindre viktig enn hovedinnholdet i bildet. Vernet gjelder i den avbildedes levetid og 15 år etter utløpet av hans dødsår.

6.1.6 Lovbestemt taushetsplikt om personopplysninger

Den alminnelige lovregel om taushetsplikt for ansatte i offentlige organer (alle organer for stat eller kommune) framgår av *forvaltningsloven § 13 første ledd*. Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det tjenestemannen i forbindelse med tjenesten eller arbeidet får vite om noens personlige forhold. Som personlige forhold i forvaltningslovens forstand regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige (jf § 13 annet ledd). Begrepet «personlig forhold» i forvaltningslovens forstand er med andre ord forskjellig (både mht innhold og funksjon) fra begrepet «personopplysning» slik dette nyttes i personregisterloven og i lovforslaget her, se personregisterloven § 1 annet ledd og 11.1 nedenfor.

Den generelle taushetspliktregelen i forvaltningsloven er supplert med en rekke taushetspliktregler i *særlovgivningen*, som i en del tilfeller oppstiller strengere taushetspliktregler, se for eksempel lov 16 januar 1970 nr 1 om folkeregistrering § 13. Også ansatte i visse former for *private virksomheter* er undergitt lovbestemt taushetsplikt, se for eksempel lov 24 mai 1961 nr 2 om forretningsbanker § 18 som pålegger tillits- og tjenestemenn og revisorer i en forretningsbank taushetsplikt om det de i stillingens medfør får kjennskap til om bankens eller bankkundens eller en annen banks forhold. Et eksempel på lovbestemt taushetsplikt som omfatter både private virksomheter og offentlige organer, finnes i lov 23 juni 1995 nr 39 om telekommunikasjon § 9-3, som pålegger bl a teletjenesteleverandør og telemyndigheten å bevare taushet om bl a innholdet av telekommunikasjonen.

Videreformidling av taushetsbelagte opplysninger uten samtykke fra den opplysningene gjelder krever hjemmel i lov eller i medhold av lov. Dette gjelder selv om mottagerne er en avgrenset krets av offentlige tjenestemenn. Et generelt eksempel på adgang til å videreformidle slike opplysninger finnes i forvaltningsloven § 13 b nr 6, som bl a gjør det mulig for offentlig ansatte å gi taushetsbelagte opplysninger til påtalemyndigheten dersom det finnes ønskelig av allmenne grunner. Et eksempel på plikt til av eget tiltak å videresende taushetsbelagte opplysninger (meldeplikt), framgår av lov 13 desember 1991 nr 81 om lov om sosiale tjenester m v § 8-8 a (opplysningsplikt til barneverntjenesten bl a dersom det er grunn til å tro at det foreligger alvorlige former for omsorgssvikt).

6.1.7 Lovregler om innsyn i forvaltningens saksdokumenter

Personregisterlovens regler om innsynsrett supplerer de mer generelle bestemmelsene i forvaltningsloven og offentlighetsloven, se nærmere 11.2 nedenfor. Hovedregelen i *offentlighetsloven* er at forvaltningens saksdokumenter (herunder registre) er offentlige, jf § 2 første ledd. Enhver kan som utgangspunkt kreve innsyn i dokumentene i en bestemt sak («allmennoffentlighet»). Unntak fra offentlighet krever særskilt hjemmel i eller i medhold av lov. I henhold til offentlighetsloven § 5 a er opplysninger som er undergitt taushetsplikt i lov eller i medhold av lov (noen

eksempler er gjengitt ovenfor) unntatt offentlighet. Også andre bestemmelser i offentlighetsloven gir adgang til å unnta personopplysninger fra offentlighet, se for eksempel § 6 nr 4 (dokument i sak om ansettelse eller forfremmelse i offentlig tjeneste) og § 6 nr 8 (personbilde inntatt i et personregister). Offentlighetsloven gir ikke innsynsrett i private registre, og gjelder heller ikke for domstolene eller Stortinget m v.

Forvaltningsloven § 18 første ledd gir partene i en sak (se loven § 2) rett til å gjøre seg kjent med sakens dokumenter («partsoffentlighet»). Innsynsretten er ikke til hinder for at sakens parter får innsyn i opplysninger som er taushetsbelagt i lov eller i medhold av lov (jf *forvaltningsloven* § 13 b). Enkelte unntak fra partsoffentligheten følger av *forvaltningsloven* § 18 andre ledd flg samt § 19. Den sistnevnte bestemmelsen gir bl a adgang til å nekte en part å gjøre seg kjent med opplysninger som det av hensyn til hans helse eller hans forhold til andre personer ikke er tilrådelig at han får kjennskap til (første ledd bokstav c) og – medmindre det er av vesentlig betydning for parten – opplysninger om en annen persons helseforhold (annet ledd bokstav a).

I forskriftene til personregisterloven § 2-1 og i Datatilsynets konsesjoner er det oppstilt tildels strenge begrensninger i adgangen til å utlevere personopplysninger. Disse reglene må vike for krav om innsyn i medhold av *forvaltningsloven* og *offentlighetsloven*.

Ny teknologi gjør at personopplysninger i offentlige dokumenter kan bli vesentlig lettere tilgjengelig, f eks ved at journaler og offentlige dokumenter legges ut på Internett. Ut fra personvern hensyn kan det stilles spørsmål ved om slik dramatisk forbedret tilgjengelighet bør ha betydning for gjennomføringen av offentlighetsprinsippet. Utvalget har imidlertid ikke hatt anledning til å prioritere denne problemstillingen, og nøyer seg med å peke på spørsmålet.

6.1.8 EDB-systemer som planleggings- og styringsredskap i arbeidsforhold

Arbeidsmiljøloven § 12 fastsetter at teknologi og arbeidsorganisasjonen skal legges opp slik at arbeidstakerne ikke utsettes for uheldige psykiske belastninger. Arbeidsmiljøloven § 12 nr 3 pålegger arbeidsgiverne å holde arbeidstakerne og deres tillitsvalgte orientert om systemer og planlagte endringer i systemer, som nyttes ved planlegging og gjennomføring av arbeidet. De mest typiske eksemplene er datamaskinbaserte systemer for produksjonsplanlegging. Bakgrunnen for bestemmelsen er dels at slike systemer kan redusere den enkelte arbeiders mulighet til selvbestemmelse og faglig utvikling/ansvar, og dels at systemene kan være vanskelige å forstå, slik at det blir større avstand mellom de som styrer og de som styres.

Utplassering av overvåkningsutstyr på arbeidsplassen vil utløse plikt for arbeidsgiver til å orientere arbeidstakerne og deres tillitsvalgte. Det kan også være nødvendig å innhente Arbeidstilsynets tillatelse før slikt utstyr blir utplassert, jf arbeidsmiljøloven § 19 som blant annet krever Arbeidstilsynets godkjenning av vesentlige endringer av betydning for arbeidsmiljøet, jf Ot prp nr 50 (1993-94) s 66 høyre spalte.

Arbeidsmiljøloven § 12 må ses i sammenheng med hensynet til bedriftsdemokrati, og med avtaler mellom partene i arbeidslivet (se som eksempel rammeavtalen mellom LO og NHO om datamaskinbaserte systemer (nedenfor 6.3)).

6.1.9 Arkivlovgivning

Som det framgår av "*Personverninteresser og andre interesser – konflikt eller interessesammenfall?*" i pkt 3.4.3, kan arkivhensyn komme i konflikt med personvern-

hensyn. Dagens regulering av arkiv er spredt rundt i en rekke ulike regelverk som dels er fastsatt ved kongelig resolusjon, og dels av Riksarkivaren etter fullmakt i kongelig resolusjon. Stortinget har vedtatt lov 4 desember 1992 nr 126 om arkiv, men loven er ennå ikke satt i kraft. Formålet med loven er å sikre arkiv som har betydelig kulturell eller forskningsmessig verdi, eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon, slik at disse blir tatt vare på og gjort tilgjengelige for ettertiden (§ 1). I tillegg til dette bevaringsaspektet skal arkivloven vareta funksjonshensyn og offentlighetshensyn i forvaltningen. Arkivreglene om kassasjon reiser ulike spørsmål om forholdet til personregisterlovens bestemmelser om sletting og retting, se arkivloven § 9 og nedenfor 11.5.

6.1.10 Statistikklovgivning

Opplysninger til bruk i offisiell statistikk er nærmere regulert i lov 16 juni 1989 nr 54 om offisiell statistikk og Statistisk Sentralbyrå. Loven varetar personvernens hensyn på tre måter. For det første gjelder plikten til å gi opplysninger til bruk i offisiell statistikk bare så langt lovbestemt taushetsplikt ikke er til hinder for dette, jf loven § 2-2. For det andre er de som behandler innhentede opplysninger undergitt spesielle regler om taushetsplikt, jf § 2-4. Endelig er det strenge begrensninger mht hvordan de innhentede opplysningene kan benyttes, se § 2-5 som fastslår at opplysningene kun kan benyttes i forbindelse med offisiell statistikk (medmindre Datatilsynet spesielt godkjenner annen bruk). Offentliggjorte opplysninger skal ikke kunne føres tilbake til oppgavegiver eller til annen identifiserbar enkeltperson til skade for denne, jf loven § 2-6.

6.2 ANNEN REGISTERLOVGIVNING

Det er ikke bare personopplysninger som registreres. I medhold av særskilte lover er det bl a opprettet registre over *realobjekter* (alt fra skip og kjøretøyer til kraftledninger og kulturminner), *rettigheter* (f eks tinglysning av heftelser i fast eiendom i grunnboken, og registrering av immaterielle rettigheter som patenter og mønstre) og *hendelser* (som f eks atomulykker). I det følgende er det imidlertid særlovgivning om registrering av personopplysninger som skal behandles.

I tillegg til personregisterloven (med forskrifter) som gir en generell regulering av personregistre, er en rekke personregistre i organ for stat eller kommune opprettet i medhold av særskilte lover. I slike tilfeller er det ikke nødvendig med konsesjon fra Datatilsynet. Hvorvidt de øvrige reglene i personregisterloven kommer til anvendelse på særlovregisteret, beror på en tolkning av den enkelte loven. Utgangspunktet er at personregisterlovens regler får anvendelse med mindre det er holdepunkter for noe annet, se personregisterloven § 41 in fine.

Nedenfor gis en kortfattet omtale av noen av de praktisk viktigste særlovsregistrene; folkeregisteret, enhetsregisteret, strafferegisteret samt foretaksregisteret.

Lov 16 januar 1970 nr 1 om folkeregistrering bestemmer at hver kommune skal føre et folkeregister over enhver fysisk person som er bosatt i kommunen (§ 1). Den som er bosatt i kommunen plikter i en rekke tilfeller å melde fra til folkeregisteret slik at registeret kan holdes oppdatert (§ 6 – § 10). Brudd på melde- og opplysningsplikten er straffbart (§ 16).

Lov 3 juni 1994 nr 15 hjemler opprettelsen av Enhetsregisteret, som er et landsdekkende register hvis formål er å samordne offentlige opplysninger om juridiske personer, enkeltmannsforetak samt andre registreringsenheter. På sett og vis kan enhetsregisteret sies å være et motstykke til folkeregisteret. Fysiske personer skal ikke registreres i registeret, men enkelte av opplysningene om den juridiske per-

sonen vil inneholde informasjon om fysiske personer, se f.eks. loven § 5 annet ledd bokstav f), som pålegger den juridiske personen å melde fra om hvem som skal være kontaktperson for virksomheten. (De registerpliktige er pålagt en tildels omfattende melde- og opplysningsplikt.)

Lov 11 juni 1971 nr 52 hjemler opprettelsen av tre registre som inneholder personopplysninger. For det første bestemmer loven at det skal finnes et Strafferegister som skal inneholde opplysninger om dommer, vedtatte forelegg og andre avgjørelser om straff (§ 1). For det andre bestemmes det at det enkelte politikammer skal føre et bøtere register (§ 3). Endelig skal den sentrale politimyndighet føre et register med personopplysninger som kan være av betydning for politiets arbeid med etterforskning og oppklaring av lovbrudd (§ 4). Loven er supplert med forskrifter. Forholdet mellom straffelovregistrene og lovforslaget her er kommentert nærmere i merknadene til § 3.

Foretaksregisteret er opprettet ved lov 21 juni 1985 nr 78 om registrering av foretak. Registeret inneholder en rekke forskjellige opplysninger om juridiske personer, se loven kapittel III. Foretakene har meldingsplikt (kapittel IV), mens registeret har plikt til å kontrollere opplysningene som kommer inn, samt plikt til å rette oppdagede feil (kapittel V og VII).

6.3 AVTALEMESSIG REGULERING AV PERSONVERNSPØRSMÅL I ARBEIDSFORHOLD

I arbeidsforhold vil avtaler mellom arbeidsgiver og arbeidstaker i visse tilfeller være hjemmel for ulike behandlinger av personopplysninger mht administrasjon, styring, kontrolltiltak mv i en virksomhet. Disse avtalene må i alle tilfeller være innenfor de prinsipper som er nedfelt i arbeidsmiljøloven og andre lovfestede og ulovfestede regler for regulering av forholdet mellom arbeidsgiver og arbeidstaker i norsk rett.

Det finnes en rekke kollektive avtaler mellom ulike organisasjoner på arbeidsgiver og arbeidstakersiden. Utvalget har valgt å trekke fram hovedavtalen mellom Landsorganisasjonen i Norge (LO) og Næringslivets Hovedorganisasjon (NHO) som eksempel i det etterfølgende.

Hovedavtalen mellom LO og NHO regulerer partenes rettigheter og plikter og trekker opp de overordnede retningslinjene for hvordan ulike spørsmål skal løses mellom partene. Avtalens kapittel IX inneholder generelle bestemmelser om informasjon, samarbeid og medbestemmelse. Grunntonen er nødvendigheten av et godt og tillitsfullt samarbeid i alle sammenhenger.

"Oversikt over andre internasjonale reguleringer og andre lands rett" i Kapittel 9, § 9-13 inneholder særskilte bestemmelser om personalarkiv og kontrolltiltak. Her tariffestet en plikt for bedriften til å drøfte behandling av personopplysninger med de tillitsvalgte. Hovedorganisasjonene råder i den sammenheng partene på den enkelte bedrift til å utarbeide en lokalt tilpasset persondatainstruks. Videre fastslås bedriftens tariffplikt til å drøfte behovet for og utforming og innføring av eventuelle interne kontrolltiltak. Nærmere bestemmelser om dette er gitt i Hovedavtalen del C, Tilleggsavtale II – Rammeavtale om teknologisk utvikling og datamaskinbaserte systemer, og Tilleggsavtale V – avtale om kontrolltiltak i bedriften.

Tilleggsavtale II bygger på Hovedavtalen kapittel IX og er en rammeavtale som skal legges til grunn ved utforming, innføring og bruk av datamaskinbaserte systemer. Avtalen omfatter teknologi og systemer for produksjon, styring og administrasjon, samt behandling av persondata i bedriften. Avtalen har særlige bestemmelser om lagring og bruk av persondata. Dersom en av partene ber om det, skal det søkes opprettet en særavtale etter de retningslinjer som trekkes opp i rammeavtalen.

Tilleggsavtale V fastsetter en del prinsipper som skal gjelde ved klarlegging av behov og innføring av eller vesentlig endring, av eksisterende kontrollordninger i bedriften. Drøfting mellom partene er også her en forutsetning. Kontrolltiltak må ha grunnlag i tekniske og økonomiske sikkerhets- eller helsemessige eller sosiale og organisatoriske forhold i bedriften, og skal alltid ligge innenfor rammen av personregisterloven med forskrifter. Alle ansatte skal stilles likt i forhold til de kontrolltiltak som gjennomføres, og i forkant ha mottatt informasjon om tiltakenes formål og praktiske konsekvenser. Informasjonsansvaret er tillagt både ledelse og tillitsvalgte. Avtalen åpner for at kontroll skal kunne utføres av andre enn bedriftens egne ansatte (vaktelskap). Dersom en av partene ber om det skal denne avtalen legges til grunn for utformingen av lokale avtaler.

Lokale avtaler som opprettes etter de retningslinjer som trekkes opp i tilleggssavtalene II og V vil nødvendigvis måtte bli forskjellige da de i mange tilfeller også tar opp i seg lokale særegenheter og behov.

6.4 ULOVFESTET PERSONVERN

I tillegg til de lovfestede reglene om personvern – som f.eks. personregisterloven – har vi i norsk rett også et ulovfestet personvern. Det ulovfestede personvernet er domstolsskapt, og relaterer seg til relativt ulike forhold.

Grunnstenen ble lagt allerede med Rt 1896 s 503 (Aars-dommen), som på ulovfestet grunnlag statuerte vern for visse typer slektsnavn. Det virkelige gjennombruddet kom likevel med dommen i Rt 1952 s 1217, som under henvisning til «et alminnelig rettsvern for personligheten» (konkret en straffedømts mulighet for rehabilitering)) forbød visning av en film som bygget på et faktisk hendelsesforløp (drapene på to lensmenn) fordi det var fare for at gjerningsmannen kunne bli gjenkjent. Høyesterett avgjorde saken ut fra en konkret tilbørlighetsvurdering. Det ulovfestede personvernet er utviklet videre i nyere avgjørelser. I Rt 1977 s 1035 ble rett til innsyn i en legejournal bl.a. begrunnet med det ulovfestede personvern. En annen side ved det ulovfestede personvern kommer fram i avgjørelsen i Rt 1991 s 616, som gjaldt avvisning av ulovlig videopptak som bevis i en straffesak. Høyesterett la avgjørende vekt på at den ulovlige overvåkingen medførte et så sterkt inngrep i den personlige integritet at den «ut fra alminnelige personvern hensyn» burde anses som uakseptabel. Avgjørelsen i RG 1993 s 77 viser at det ulovfestede personvernet også kan ha betydning på arbeidsrettens område; her ble en avskjed av en arbeidstaker funnet urettmessig fordi arbeidsgiveren uten samtykke hadde gått inn på arbeidstakerens personlige datafiler.

Avgjørelsen i Rt 1990 s 1008 illustrerer at personvern hensyn ikke alltid slår igjennom overfor andre hensyn. Det ble i denne avgjørelsen lagt til grunn at såkalt overskuddsinformasjon som følge av trafikkovervåking kunne brukes som bevis også i forhold til heleri og brukstyveri.

Som det fremgår ovenfor favner det ulovfestede personvernet over en rekke ulike rettsområder. I en videre forstand omfatter det ulovfestede personvernet ikke bare rettsregler som skapes og håndheves av domstolene, men også mellommenneskelige regler for sosial atferd og moralregler. Etterlevelsen av slike regler – man søker f.eks. å unnlate å overhøre to personers fortrolige samtale om intime forhold – skyldes ikke frykt for rettslige sanksjoner dersom normen overtres, men istedet en intuitiv følelse av at det ikke er «riktig» eller sosialt akseptabelt å handle uoverensstemmende med den. Det er grunn til å tro at betydningen og etterlevelsen av slike normer er vekslende for ulike samfunnsgrupper med ulike verdigrunnlag. Likeledes kan sanksjonen over oppdagede brudd på denne type normer være av høyst ulik karakter – alt fra kommunikasjon av sterk misbilligelse gjennom kritiske utsagn, til en

mer likegyldig konstatering av at normen er overtrådt. Ujevn gjennomslagskraft til tross er det ikke grunn til å undervurdere betydningen av ikke-rettslige adferdsnormer. Blant annet illustrerer de at mange personvernspørsmål ikke er rettsliggjort – og at de kanskje heller ikke er egnet til å rettsliggjøres. Under enhver omstendighet vil slike normer supplere rettslig bindende regler som håndheves av domstolene, og hører naturlig med i en oversikt over regler som er av betydning for personvernet.

KAPITTEL 7

Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse

7.1 OVERSIKT

Det finnes flere internasjonale regelsett som er av betydning for utformingen av norske regler om behandling av personopplysninger. Grovt sett kan de internasjonale reglene deles i to grupper. Den første gruppen er konvensjoner m v som er folkerettslig bindende for Norge. Et eksempel på dette er EF-direktivet. Den andre gruppen er regler – anbefalinger – som ikke er rettslig forpliktende, men som likevel bør tas i betraktning, se oversikten i "*Oversikt over andre internasjonale reguleringer og andre lands rett*" i kapittel 9.

I dette kapitlet presenteres Europarådets konvensjon 28 januar 1981 nr 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger (*the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*) med senere rekommandasjoner. Direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger m m omtales i "*Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger*" i kapittel 8 nedenfor. I "*Oversikt over andre internasjonale reguleringer og andre lands rett*" i kapittel 9 behandles andre internasjonale reguleringer i tillegg til at det gis en oversikt over andre lands rett.

Felles for "*Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse*" i kapitlene 7, 8 og 9 er at framstillingen er begrenset til en orientering om hovedpunkter. Formålet med framstillingen her er blant annet å gjøre det lettere å forstå henvisningene og de mer detaljerte redegjørelsene i del II.

7.2 KONVENSJONEN

Konvensjonen ble ratifisert av Norge 20 februar 1984 uten forbehold, og tok til å gjelde 1 oktober 1985. Konvensjonen gjelder i utgangspunktet for all lagring og håndtering av personopplysninger som blir foretatt ved hjelp av EDB. Formålet med konvensjonen er å sikre respekten for frihet og andre grunnleggende rettigheter, og særlig sikre personlig integritet når personopplysninger bli behandlet ved hjelp av EDB.

Konvensjonen dannet et viktig grunnlag for utarbeidelsen av EF-direktivet. Fordi konvensjonen allerede er gjennomført i norsk rett blir arbeidet med å implementere EF-direktivet mindre omfattende enn det ellers ville vært.

Konvensjonen inneholder minimumsregler. Dette betyr at de som opplysningene gjelder kan gis flere og mer omfattende rettigheter enn det som følger av konvensjonen.

7.3 REKOMMANDASJONENE

Konvensjonen er senere fulgt opp med en rekke rekommandasjoner som tar for seg mer avgrensede områder og gir mer detaljerte regler enn konvensjonen. Rekommandasjonene har en annen rettslig status enn konvensjonen i det de bare er anbefalinger, og ikke folkerettslig bindende. Rekommandasjonene er imidlertid politisk bindende, og det fremgår av utvalgets mandat at det skal tas hensyn til disse (se 2.1).

Pr 1 mars 1997 foreligger det 10 ulike rekommandasjoner. Mange av rekommandasjonene er best egnet til å følges opp på annen måte enn i en generell lov om behandling av personopplysninger, for eksempel i særlovgivning og gjennom myndighetens praktisering av regelverket (slik Datatilsynet gjør i dag).

KAPITTEL 8

Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger**8.1 DIREKTIVETS BAKGRUNN OG SIKTEMÅL**

Kommisjonen la i juli 1990 fram et forslag til et direktiv med det formål å sikre et høyt beskyttelsesnivå for personer i forbindelse med behandling av personopplysninger. Bakgrunnen for Kommisjonens initiativ var at flere medlemsland ikke hadde personvernlovgivning, mens andre land hadde lover med et høyt beskyttelsesnivå. Flere land hadde heller ikke tiltrådt Europarådskonvensjonen om personvern. Kommisjonen fryktet at disse ulikhetene ville vanskeliggjøre den frie flyt av persondata mellom medlemslandene, og dermed skape problemer for det økonomiske samkvetmet landene i mellom.

Etter å ha behandlet forslaget i 1992, kom Europaparlamentet med en rekke endringsforslag, og Kommisjonen la i oktober 1992 fram et revidert utkast. Dette har senere vært til behandling i en arbeidsgruppe under Rådet. Norge deltok på denne gruppens møter fra 1 juli 1994 fram til folkeavstemningen 28 november 1994.

Rådet kom 20 februar 1995 fram til et felles forslag, som ble ferdigbehandlet av Europaparlamentet 15 juni 1995 og endelig vedtatt i Rådet 24 juli 1995. Direktivet omtales i utredningen som «personverndirektivet», «EF-direktivet» eller bare «direktivet».

Personverndirektivets siktemål er å etablere felles reguleringsprinsipper og et ensartet vern i hele EU-området. Innen denne målsettingen er det åpnet for at det enkelte land kan fastsette høyere standarder for personvern enn det som følger av direktivet (se fortalen avsnitt 9). I hvilken grad det er adgang til å supplere med strengere nasjonale regler må vurderes i forhold til den enkelte artikkel i direktivet. Direktivet inneholder forbud mot å innføre personvernbeskyttelse som forbyr eller innskrenker fri utveksling av personopplysninger mellom medlemslandene, se artikkel 1 annet avsnitt, jf EF-traktatens artikkel 7 bokstav A om de fire friheter.

Direktivet kan anses å ha tre begrunnelser. De *markedsmessige* overveielsene må sies å dominere, idet uniforme regler for personvern ses som en forutsetning for å få et fritt marked til å fungere. I tillegg kommer en *forvaltningsmessig* begrunnelse, idet personopplysninger må kunne flyte uhindret for at felles forvaltningsordninger skal kunne etableres. For det tredje har også direktivet en *idealistisk* begrunnelse, idet personvern ses som en grunnleggende rettighet.

8.2 DIREKTIVETS FORHOLD TIL NORSK RETT

Personverndirektivet bygger i utgangspunktet på prinsippene i Europarådets konvensjon om beskyttelse av personopplysninger. I og med at norsk lovgivning på området, i første rekke personregisterloven, tilfredsstiller de krav som Europarådets konvensjon fastsetter, inngår allerede en rekke av de prinsipper som fastsettes i direktivet i norsk lovgivning. Enkelte endringer er imidlertid nødvendig for gjennomføring av direktivet i norsk rett. Disse kommer vi nærmere tilbake til nedenfor i del II.

8.3 TOLKNING AV PERSONVERNDIREKTIVET

Det finnes ikke vanlige forarbeider til direktivtekstene. Ordlyden blir derfor den viktigste rettskilden for tolkning av direktivet. Det er imidlertid knyttet enkelte usikkerhetsmomenter til den. Direktivene utferdiges for eksempel i en rekke offisielle språk og ordlyden i de forskjellige språkene kan ha forskjellige nyanser. Personverndirektivets bestemmelser inneholder dessuten forholdsvis mange vage og skjønnsmessige uttrykk, noe som kan gjøre ordlydsfortolkning vanskelig. Ordlyden i fortalen er i enda større grad vag og skjønnsmessig, men denne har heller ikke i seg selv særlig rettskildemessig vekt. EU-domstolen har ennå ikke tolket direktivet.

8.4 OVERSIKT OVER INNHOLDET I PERSONVERNDIREKTIVET

Personverndirektivet skal sikre fysiske personers grunnleggende rettigheter og frihetsrettigheter, spesielt retten til privatlivets fred, i forbindelse med behandling av personopplysninger, og dessuten sikre fri utveksling av personopplysninger mellom medlemsstatene.

Direktivets bestemmelser gjelder generelt ved behandling av personopplysninger når dette skjer helt eller delvis ved hjelp av edb, samt ved manuell behandling av personopplysninger når opplysningene inngår eller skal inngå i et personregister. Ren privat behandling av opplysninger omfattes ikke av direktivet, heller ikke behandling av personopplysninger innenfor de samfunnsområder som ikke er omfattet av fellekskapsretten.

Medlemsstatene skal utpeke en eller flere tilsynsmyndigheter som skal påse at bestemmelsene overholdes. Tilsynsmyndigheten skal utøve sine oppgaver i fullstendig uavhengighet, og skal bl a ha myndighet til å iverksette undersøkelser, gi konsesjoner, stoppe ulovlige behandlinger mm. Alle behandlinger av personopplysninger skal være offentlig tilgjengelige, og registermyndigheten plikter å føre et register over de behandlingene som skjer (i alle fall de meldepliktige behandlingene).

Direktivet gir en uttømmende oppregning av hvilke situasjoner som tillater behandling av personopplysninger. Oppregningen åpner imidlertid for en vid grad av skjønn; for eksempel kan slik behandling skje dersom behandlingen er nødvendig av hensyn til en oppgave i samfunnets interesse eller behandlingen hører inn under offentlig myndighetsutøvelse.

I utgangspunktet er behandling av enkelte sensitive opplysninger forbudt, men også for slik behandling åpner direktivet for å gjøre unntak i en rekke tilfeller. For eksempel kan sensitive opplysninger behandles dersom den opplysningene angår samtykker, eller medlemsstatene kan på visse vilkår gjøre unntak fra dette utgangspunktet dersom dette kan begrunnes i viktige samfunnsmessige interesser. Direktivets angivelse av hva som er å anse som sensitive opplysninger er stort sett sammenfallende med oppregningen i personregisterloven § 6 annet ledd. Nytt i forhold til norsk rett er at opplysning om fagforeningstilhørighet etter direktivet er å anse som en sensitiv opplysning (dvs underlagt strengere regulering).

Direktivet innfører en aktiv opplysningsplikt for den behandlingsansvarlige ved innsamling av personopplysninger overfor den opplysningene gjelder. Denne plikten kommer i tillegg til den retten den registrerte har til innsyn i opplysninger om seg selv. Dette er ikke noe helt nytt i forhold til norsk rett i dag, jf f eks personregisterloven § 19 (når det gis kredittopplysning om noen som ikke er næringsdrivende skal kredittopplysningsforetaket sende melding til den det innsamles opplysninger om), men direktivet krever en betydelig utbygging av dagens ordning.

Direktivet etablerer videre en meldeplikt for den behandlingsansvarlige til tilsynsmyndigheten forut for en behandling av personopplysninger, når behandlingen helt eller delvis gjør bruk av elektroniske hjelpemidler. Det kan gjøres unntak fra

meldeplikten, både slik at enkelte behandlinger underlegges mildere regulering (forenklet meldeplikt eller fritakelse for meldeplikt) og slik at enkelte behandlinger underlegges en strengere regulering (konesjonsplikt). Ordningen skiller seg imidlertid fra personregisterlovens system i dag ved at det er meldeplikt som er hovedregelen og ikke konsesjonsplikt.

Det innføres nye rettigheter i tilknytning til visse automatiserte avgjørelser og avgjørelsesprosedyrer. For det første kan enhver kreve å få vite hvilken logikk som ligger bak en slik automatisert behandling av opplysninger om en selv. I dette ligger et krav på begrunnelse for den avgjørelsen som er truffet automatisert, dvs en rede-gjørelse for hvilke behandlingsregler som er lagt inn i programmet; et krav på dokumentasjon av programmet. For det andre har alle rett til å kreve manuell overprøving av helautomatisert behandling av visse avgjørelser.

8.5 ANDRE EF-DIREKTIV SOM ANGÅR PERSONVERNET

8.5.1 Direktiv om beskyttelse av personopplysninger og kommunikasjonshemmeligheter i forbindelse med offentlige digitale telenett

Europakommisjonen fremmet i 1994 et forslag til direktiv om behandling av personopplysninger og beskyttelse av privatlivet i forbindelse med offentlige telenett, særlig ISDN (Integrated Service Digital Network). Direktivutkastet forventes vedtatt i løpet av våren 1997 etter pågående sluttbehandling i henhold til den fastlagte prosedyren for enighet mellom Rådet og Parlamentet (Conciliation procedure). Direktivets formål er å detaljere og supplere det alminnelige personverndirektiv (direktiv 95/46/EF).

Direktivet inneholder en rekke konkrete og detaljerte bestemmelser om bl a plikt for leverandører til å informere kunder om fare for brudd på nettsikkerheten og om plikt til å sikre konfidensialitet, hindre avlytting, lagring og overvåking av kommunikasjonen med mindre dette har hjemmel i lov. Videre inneholder direktivet bestemmelser om lagring av trafikkdata, visning av oppringerens nummer (A-nummer), rett for mottager til å avvise innkommende samtaler hvor A-nummer ikke vises og rett til å hindre uautorisert viderekopling til eget apparat. Direktivet inneholder også regler knyttet til oppføring i telefonkatalog.

Direktivet anses for EØS-relevant, og vil bli vurdert inntatt i EØS-avtalen når det er vedtatt.

8.5.2 Direktiv 97/7/EF om forbrukervern ved fjernsalg

Fjernsalgdirektivet ble vedtatt 23 januar 1997, men er foreløpig ikke publisert i EF-tidende.

Fjernsalgsdirektivet regulerer forhold omkring avtaler om varer eller tjenester som inngås mellom en forbruker og en selger ved *fjernsalg*, dvs at partene i forbindelse med avtaleinngåelsen bare har kontakt gjennom såkalte fjernkommunikasjonsmidler. Typiske former for fjernsalg er postordresalg, telefonsalg, salg gjennom skriftlig/telefonisk bestilling på grunnlag av annonsering i kataloger, radio, TV etc. Salg via Internett er en fjernsalgsform som forventes å få en dramatisk vekst i de kommende år. Direktivet har ulike bestemmelser som skal vareta forbrukeren ved inngåelse av avtaler om fjernsalg, herunder en reservasjonsrett for forbrukeren ved direkte markedsføring, og for enkelte salgsformer et krav til forhåndssamtykke.

Direktivet anses for EØS-relevant, og vil bli vurdert inntatt i EØS-avtalen.

KAPITTEL 9

Oversikt over andre internasjonale reguleringer og andre lands rett**9.1 OVERSIKT**

Først i kapitlet omtales noen internasjonale regelsett som kommer i tillegg til Euro-parådskonvensjonen ("*Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse*" i kapittel 7) og EF-direktivet ("*Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger*" i kapittel 8). Deretter gis en redegjørelse for rettstilstanden i endel ulike land.

9.2 OECDs RETNINGSLINJER

Organisasjonen for økonomisk samarbeid og utvikling (OECD) utviklet i 1980 retningslinjer for beskyttelse av og utveksling av persondata over landegrensene («Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data»). Retningslinjene er ikke rettslig bindende, men har hatt stor betydning, særlig for land som ikke omfattes av reguleringene i regi av Europarådet eller EU/EØS.

9.3 EUROPARÅDETS MENNESKERETTIGHETSKONVENSJON 4 NOVEMBER 1950

Konvensjonen er en generell konvensjon om menneskerettigheter og beskytter rettigheter på en rekke felt.

Konvensjonen håndheves i første rekke gjennom individuelle klagesaker. Etter dagens system behandles klagesakene først av Kommisjonen som avgir en rapport. Denne er ikke bindende for statene. Hvis saken ikke klages inn for Domstolen avgjøres saken med bindende virkning av Ministerkomiteen. Ministerkomiteen bygger i praksis nærmest alltid sin avgjørelse på kommisjonens rapport. Hvis saken blir klaget inn for Domstolen avsier denne en bindende dom. Systemet er nå vedtatt endret slik at individuelle klager bare skal behandles av Domstolen. Endringen er imidlertid ikke trådt i kraft.

Særlig aktuelt for personvernet er artikkel 8 som lyder:

«1. Enhver har rett til respekt for sitt privat- og familieliv, sitt hjem og sin korrespondanse.

2. Offentlig myndighet skal ikke gjøre noe inngrep i utøvelsen av denne rett medmindre dette inngrep er i samsvar med loven og i et demokratisk samfunn er en nødvendig forholdsregel for den nasjonale eller offentlige sikkerhet, for landets økonomiske velstand, for å forebygge uorden eller forbrytelser, beskytte helse eller moral eller beskytte andres rett og friheter.»

Kommisjonen og Domstolen i Strasbourg har gjennom sin praksis vist at de tolker reglene på en dynamisk måte, dvs at rettsreglene utvikler seg etterhvert. Dette gjelder også artikkel 8 som bl a har vært ansett for å sikre enkeltpersoners innsyn i opplysninger om en selv (se f eks Leandersaken Serie A no 116 hvor klageren riktignok ikke fikk medhold pga at det var antatt at politiregistre kunne unntas i hen-

hold til artikkel 8 andre ledd, og Gaskin-saken Serie A no 160, hvor klageren fikk medhold i at artikkel 8 ga ham innsynsrett i et offentlig register).

Utvalget finner det klart at artikkel 8 kan få anvendelse på områder som omfattes av den nye loven om behandling om personopplysninger. Utvalget er imidlertid av den oppfatning at sålenge loven implementerer reglene fra Europarådskonvensjonen om persondatabeskyttelse og EF-direktivet, vil kravene i Den europeiske menneskerettighetskonvensjon artikkel 8 også være oppfylt.

Den europeiske menneskerettighetskonvensjonen artikkel 10 verner ytringsfriheten, jf "*Forholdet til ytringsfriheten*" i kapittel 17.

9.4 ANDRE INTERNASJONALE RETTSINSTRUMENTER

9.4.1 Verdenserklæringen om menneskerettighetene og senere FN-konvensjoner og retningslinjer

Verdenserklæringen fra 1948 er ikke folkerettslig bindende, men har stor moralsk og politisk autoritet. Flere av erklæringens tretti artikler oppstiller prinsipper som er av betydning for personvernet i vid forstand, jf særlig artiklene 3, 18, 19 og 20. Den artikkelen som mest direkte berører behandling av personopplysninger er artikkel 12:

«Ingen må utsettes for vilkårlig innblanding i privatliv, hjem eller korrespondanse, eller for angrep på ære og anseelse. Enhver har rett til lovens beskyttelse mot slik innblanding eller slike inngrep.»

Som det fremgår verner artikkelen om flere typer rettigheter. Viktigst i vår sammenheng er retten til vern om den enkeltes «privatliv».

Verdenserklæringens artikler av betydning for personvernet er senere fulgt opp i regi av FN, blant annet gjennom *konvensjonen om sivile og politiske rettigheter av 1966* (ikraft 23 mars 1976). Konvensjonen har fått global oppslutning, og er ratifisert av omlag to tredjedeler av verdens stater. Overtredelser kan innklages til FNs Menneskerettighetskomite. Komiteens avgjørelser er ikke rettslig bindende, men følges allikevel stort sett av statene. Fra et personvernssynspunkt er særlig konvensjonen artikkel 17 interessant:

«1. Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige angrep på ære eller omdømme.

2. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.»

Bestemmelsen bygger i hovedsak på verdenserklæringen artikkel 12. Det er viktig å merke seg at bestemmelsen ikke bare sikrer beskyttelse i lov mot vilkårlige inngrep i privatlivet fra offentlige myndigheter, men også fra private rettssubjekter. Den nærmere rekkevidden av bestemmelsen, herunder forståelsen av begrepene «vilkårlige» og «privatliv» er omdiskutert og usikker. Utvalget legger til grunn at såvel gjeldende norsk personregisterlov og EF-direktivet går lenger i å beskytte enkeltindividers rettigheter ved behandling av personopplysninger enn det som kan utledes av FN-konvensjonen om sivile og politiske rettigheter artikkel 17.

Generalforsamlingen i FN vedtok 14 desember 1990 resolusjon 45/95 «*Guidelines Concerning Computerized Personal Data Files*». Retningslinjene inneholder en rekke minstekrav til behandlingen av personlige opplysninger.

9.4.2 Organisasjonen av amerikanske stater (OAS)

Det er ikke bare land i Europa som har tatt initiativ til regionale reguleringer av personvernspørsmål. Organisasjonen av amerikanske stater (OAS) vedtok en egen menneskerettighetserklæring i 1948 («American Declaration of the Rights and Duties of Man»), hvor det i artikkel V heter at enhver har rett til beskyttelse i lov mot «abusive attacks upon ... his private ... life».

I likhet med FNs menneskerettighetserklæring er ikke erklæringen rettslig bindende for medlemsstatene. OAS har imidlertid senere fulgt opp erklæringen med en rettslig bindende konvensjon («American Convention on Human Rights», i kraft fra 18 juli 1978). I artikkel 11 heter det blant annet at ingen må utsettes for «arbitrary or abusive interference with his private life», og at enhver har rett til lovbestemt beskyttelse mot dette.

9.5 ANDRE LANDS PERSONREGISTERLOVGIVNING

9.5.1 Innledning

Nedenfor gis en oversikt over personvernlovgivningen i en del land. Utvalget er basert på flere kriterier; blant annet har det vært et ønske å hente erfaringer fra personregisterlovgivningen og tilsynsmyndighetens praksis i land som samfunnsmessig er sammenlignbare med Norge.

Ettersom mange europeiske land i likhet med Norge er forpliktet til å oppfylle EF-direktivet (jf "[Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger](#)" i kapittel 8), og det av den grunn er naturlig å forvente endringer i disse landenes lovgivning, er omtalen av den nåværende reguleringen på enkelte punkter nokså kortfattet.

9.5.2 Sverige

Lovgivningen

Sverige var blant de første land i verden til å vedta personregisterlovgivning. Datalagen (1973:289) ble vedtatt 11 mai 1973 (i kraft 1 juli 1974). Sverige var også først ute med å gi allmenn rett til innsyn i offentlige dokumenter (jf Tryckfrihetsförordningen fra 1766), en rett som senere er nedfelt i den svenske grunnloven. Også andre konstitusjonelle regler varetar personvernet, jf Regeringsformen (1974:152) 2 §:

«Den offentliga makten skall utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet. [...] Det allmänna skall tillförsäkra män ock kvinnor lika rättigheter samt värna den enskildes privatliv och familjeliv.»

13 § i Regeringsformen fastslår at retten til ytringsfrihet kan begrenses ut i fra hensynet til «privatlivets helgd». 3 § i Regeringsformen må formentlig forstås slik at den oppmuntrer til at det gis lovgivning som varetar hensynet til den personlige integritet i forbindelse med elektronisk behandling av personopplysninger:

«Varje medborgare skall i den utsträckning som närmare anges i lag skyddas mot at hans personliga integritet kränkes gjennom at uppgifter om honom registreres med hjälp av automatisk databehandling.»

Den samme bestemmelsen forbyr at en persons politiske oppfatning blir registrert uten at vedkommende samtykker i registreringen.

Datalagen regulerer etablering og bruk av personregistre i både offentlig og privat sektor, og omfatter opplysninger om fysiske personer. Manuelle registre omfattes ikke av datalagen, og ei heller opplysninger om juridiske personer. Datalagen inneholder flere bestemmelser som vektlegger det såkalte «formålsbestemthetsprinsippet». Et eksempel på dette er 7 §, hvor det blant annet heter at personregistre skal innrettes slik at «inte otilbørlig intrång i registrerads personliga integritet uppkommer». I motsetning til personregisterloven inneholder datalagen for øvrig en egen straffebestemmelse om «hacking» eller «dataintrång».

Datalagen er for tiden under revisjon. Datalagskommittén la frem sitt forslag til persondatalag i SOU 1997:39 «Integritet – Offentlighet – Informationsteknik».

Forsåvidt gjelder regelverket ellers, varetas personvernet av flere andre lover enn datalagen. Eksempler på slike lover er kredittopplysningslagen (1973:1173), inkassolagen (1974:182), sekretesslagen (1980:100) og sekretessförordningen (1980:657), samt förvaltningslagen (1986:223) som tilsvarende den norske forvaltningsloven. Flere av disse lovene beskytter opplysninger om juridiske personer.

Tilsynsmyndigheten

Datainspektionen er satt til å føre tilsyn med at loven overholdes. Datainspektionen er ledet av en direktør som er tilsatt av regjeringen (justitiedepartementet) på åremål (seksårsperioder). I likhet med Datatilsynet har Datainspektionen en administrasjon og et styre. Direktøren er leder av administrasjonen og også styremedlem. Styret består for øvrig av 10 personer, som representerer bl a forvaltningen, fagforeninger og forskningsmiljøer. Styremedlemmene oppnevnes av regjeringen for fire år av gangen. Justitiedepartementet har administrativt- og budsjettansvar for Datainspektionen, men har ikke instruksjonsmyndighet.

Klager over Datainspektionens avgjørelser kan etter en lovendring i 1995 bringes inn for den almänna förvaltningsdomstolen. Dersom den registeransvarlige er et forvaltningsorgan, behandles klagen av regjeringen (justitiedepartementet).

I utgangspunktet kan ikke et personregister opprettes før den registeransvarlige «har anmeldt sig hos Datainspektionen och fått bevis om detta av inspektionen (licens)», jf datalagen 2 § første ledd.

- Enkelte personregistre krever «tilstånd» fra Datainspektionen. Dette gjelder
- særlig sensitive opplysninger som angitt i 4 § (f eks om helsetilstand)
 - opplysninger som utgjør «omdömme eller annan värderande upplysning om den registrerade» (jf 6 § annet ledd)
 - opplysninger om personer som ikke er tilknyttet den registeransvarlige som følge av medlemsskap, ansettelse, kundeforhold eller lignende (jf 2 § annet ledd nr 3)
 - opplysninger innhentet fra et annet personregister, med mindre opplysningene er registrert eller utlevert etter lov, Datainspektionens vedtak eller datasubjektets samtykke (jf 2 § annet ledd nr 4).

Hovedregelen er at Datainspektionen skal tillate etablering av personregistre «om det saknas anledning antaga at, med iakttagande av de föreskrifter som meddelas enligt 5 och 6 §§, otilbørlig intrång i registrerads personliga integritet skall uppkomma» (jf 3 § første ledd, 7 § første ledd og 15 § første ledd). Det er ikke nødvendig å innhente tillatelse fra Datainspektionen for å føre personregistre som etableres etter beslutning av Regjeringen eller Riksdagen, eller som skal oversendes en «arkivmyndighet» til oppbevaring, eller som etableres «i enlighet med» forskrifter gitt av Datainspektionen i medhold av datalagen 19 §. Hittil har Datainspektionen

gitt slike forskrifter for bruk av personregistre i forbindelse med blant annet kommunale myndigheters og forsikringsselskapers virksomhet.

9.5.3 Danmark

Lovgivningen

Den danske grunnloven inneholder ikke noen alminnelig bestemmelse om privatlivets fred. Til forskjell fra en del andre land har man i Danmark regulert personregistre i offentlig og privat sektor i hver sin lov, jf Lov nr 293 af 8 juni 1978 om private registre m v, og Lov nr 294 af 8 juni 1978 om offentlige myndigheters registre. I tillegg finnes det en rekke bestemmelser rundt om i lovverket av betydning for personvernet.

Loven om private registre får anvendelse på opplysninger om juridiske personer i tillegg til fysiske personer. Registrering av data er tillatt i den grad det er et «naturligt led i den normale drift» av organisasjonen (jf § 3 første ledd). For sensitive opplysninger – som f eks opplysninger om rase, religion, politiske, straffbare eller seksuelle forhold – gjelder enda strengere regler. I slike tilfeller kan registrering kun finne sted dersom dette er «nødvendig» ut i fra interessene til den som foretar registreringen, og registreringen enten er tillatt i medhold av annen lovgivning, den registrerte gir fra seg informasjonen, eller at den registrerte samtykker i at det samles inn opplysninger fra andre kilder enn ham selv.

Registertilsynet kan gi tillatelse selv om de ovennevnte vilkårene ikke er oppfylt. I Danmark benytter man seg for øvrig av meldeplikt (notifikasjon til tilsynet om registrering) ved visse former for registrering.

For offentlige registeransvarlige er reglene i noen grad annerledes. Lov om offentlige registre omfatter for det første bare elektroniske registre. Et register som benyttes av et statlig organ kan bare opprettes etter tillatelse av statsråden med ansvaret for den aktuelle virksomheten (jf § 4 første ledd). Før et register som inneholder «fortrolige» opplysninger skal tas i bruk, skal det utarbeides forskrifter for bruk av registeret. Det samme gjelder bl a for samkjøring av registre «der er oparbejdet med henblik på varetagelse af forskellige opgaver» (med mindre samkjøringen utelukkende foretas i statistisk eller vitenskapelig øyemed), og for opprettelse av interkommunale registre. Før reguleringen blir godkjent, må Registertilsynet få anledning til å kommentere forskriftene. Selv om Registertilsynets uttalelser ikke er rettslig bindende (se nærmere nedenfor om tilsynsmyndigheten), blir de nesten alltid fulgt.

Oversikt over registre som ikke krever forskrifter må bli sendt til tilsynsmyndigheten med jevne mellomrom (jf § 8 a tredje ledd og § 8 b femte ledd). Registertilsynet kan «under hensyn til et registers formål, personkreds, dataindhold, størrelse og anvendelsesområde» kreve at det gis forskrifter selv om registeret ikke er av en slik art at loven krever dette.

Felles for registre med og uten forskrifter er at det kun kan registreres opplysninger som klart er av betydning for varetagelsen av vedkommende myndighets oppgaver. Opplysninger om politiske forhold som ikke er offentlig tilgjengelige kan under ingen omstendighet registreres. Andre sensitive opplysninger kan bare registreres dersom dette er «nødvendigt» for å vareta vedkommende myndighets oppgaver.

Som i de andre nordiske landene arbeides det i Danmark med en revisjon av personregisterlovgivningen. Et utvalg skal legge frem sitt forslag innen 1 juli 1997.

Tilsynsmyndigheten

Registertilsynet fører tilsyn med både offentlige og private registerbrukere. Tilsynet består av et råd og et sekretariat. Rådets medlemmer (tilsammen syv personer) blir oppnevnt av justisministeriet. Det fremgår av forarbeidene til loven om offentlige myndigheters registre at rådets medlemmer skal ha «sagkundskap»; rådet skal med andre ord ikke først og fremst bestå av representanter for interesseorganisasjoner.

Registertilsynet er funksjonelt uavhengig fra sentraladministrasjonen i den forstand at justisministeren ikke kan instruere rådets medlemmer.

Registertilsynets avgjørelser som retter seg mot private registeransvarlige kan ikke angripes med administrativ klage, men må eventuelt bringes inn for domstolene. Innenfor offentlig sektor har Registertilsynet bare en rådgivningsfunksjon, og kan ikke treffe rettslig bindende vedtak.

9.5.4 Finland

Lovgivningen

I 1995 ble den finske grunnloven endret slik at den inneholder en mer detaljert katalog over menneskerettigheter enn tidligere. I kapittel II § 8 første ledd heter det nå at:

«Everyone's private life, honour, and home shall be secure. More specific provisions on the protection of personal data shall be prescribed and specified by an Act of Parliament.»

Slik beskyttelse av personopplysninger er blant annet gitt i Henkilörekisterilaki/Personregisterlagen fra 1987 (FFS 471/87), i kraft fra 1988. Loven suppleres med forskrifter som regulerer bruk av registre i forskning, statistikk, spørreundersøkelser, markedsføringsundersøkelser, direktealg, «adresstjänst» samt kredittvurdering (jf Personregisterförordningen FFS 476/87).

Den finske personregisterlagen regulerer opprettelse og bruk av elektroniske og manuelle personregistre i privat og offentlig sektor. Loven beskytter bare opplysninger om fysiske personer, men det er verdt å merke seg at definisjonen av personopplysninger – opplysninger som «kan hänföras till en bestämd fysisk person eller til hans familj eller någon som lever i gemensamt hushåll med honom» – kan føre til at også informasjon om *grupper av mennesker* beskyttes. Formålet med loven er forøvrig ikke bare å beskytte personopplysninger, men også «att garantera statens säkerhet» og «att skapa god registersed» (jf § 1 første ledd).

Grunnleggende krav til registrering av personopplysninger gis i loven § 3:

«När personuppgifter inhämtas, registreras, används och lämnas ut skall den registeransvarige vara aktsam och iakta god registersed samt även i övrigt förfara så att den registrerades personliga integritet, intresser eller rättigheter inte otilbörligt kränks eller att statens säkerhet äventyras.»

Regelen i § 3 suppleres av flere bestemmelser om formålsbestemthetsprinsippet, herunder krav til saklighet (jf §§ 4, 16 og 21).

I loven kapittel 3 gis den registrerte innsynsrett, og den registeransvarlige pålegges plikt til å kontrollere datakvaliteten. "*Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet*" i Kapittel 4 inneholder regler om bl a videregivelse av personopplysninger samt om samkjøring av registre. Samkjøring kan bare skje såfremt visse vilkår er oppfylt, som for eksempel at samkjøringen åpenbart ikke krenker den registrertes integritet, interesser eller rettigheter, eller dersom datasekretessnämnden samtykker i samkjøringen.

Loven oppstiller meldeplikt for en del typer virksomheter, herunder kredittvurderingsvirksomhet (jf § 30). Endelig gis enkelte regler om datasikkerhet, blant annet kriminaliseres «hacking» (inntrång i personregister, jf § 45).

I likhet med de øvrige nordiske land er den finske personregisterloven for tiden under revisjon.

Tilsynsmyndigheten

I Finland overvåkes de registeransvarlige av to organer; dataombudsmannen og datasekretessnämnden (jf Lag om datasekretessnämnden och dataombudsmannen, FFS 474/87).

Dataombudsmannen er utnevnt av regjeringen. Han eller hun har kun rådgivende myndighet, men samtidig vidtgående hjemmel til å foreta undersøkelser (jf §§ 31 – 32). Datasekretessnämnden består av åtte personer. Også disse utnevnes av regjeringen, men i motsetning til dataombudsmannen har datasekretessnämnden kompetanse til å treffe rettslig bindende avgjørelser. I tillegg til å gi konsesjoner bl a for overføring av personopplysninger til utlandet, har nemnden adgang til å gjøre unntak fra personregisterlagen i konkrete tilfeller (jf § 37 første ledd). Nemndens avgjørelser kan bringes inn for «högsta förvaltningsdomstolen» (jf § 38). Dataombudsmannen kan bringe nemndens avgjørelse etter § 37 inn for forvaltningsdomstolen.

9.5.5 Island

Lovgivningen

Islands første personregisterlov ble innført i 1981 (Lov af 25 mai 1981 om systematisk registrering af opplysninger angående private forhold). Den ble erstattet av Lov nr 121 af 28 december 1989 om registrering og behandling af personopplysninger, i kraft fom 1 januar 1990.

Loven gjelder for «systematisk» registrering av opplysninger om «enkeltpersoners, institusjoners, virksomheters eller andre juridiske personers private, økonomiske eller øvrige forhold som med rimelighet kan forlanges unntatt offentlighet» (jf § 1 første og tredje ledd). Loven får anvendelse på både elektronisk og manuell registrering.

Registrering er tillatt dersom den «er et naturlig ledd i den gjeldende virksomhets m v drift, og kun omfatter dem som er tilknyttet det gjeldende aktivitets- eller arbeidsområde, f eks kunder, personale eller foreningsmedlemmer» (jf § 3). Opplysninger om «enkeltpersoners rent private forhold» (dvs opplysninger om rase, politisk tilknytning, religion, straffbare handlinger, seksuelle forhold, helseforhold og «vesentlige sosiale problemer») er undergitt strengere regulering. Slike opplysninger kan ikke registreres uten at registreringen følger av andre lover eller skjer med samtykke fra den som registreres. Tilsynsmyndigheten (se nedenfor) kan tillate registrering av slike opplysninger dersom registreringen anses som nødvendig. Samkjøring av registre som tilhører forskjellige enkeltindivider eller organisasjoner krever tilatelse fra tilsynsmyndigheten, med mindre registrene inneholder trivielle opplysninger som «navn, navnenummer, personnummer, firmanummer, adresse, bopel og postkode» (jf § 6 annet ledd). Konsesjon kreves ellers ved registrering og videregivelse ved visse former for virksomhet, samt for systematisk innsamling og registrering av opplysninger som skal overføres til utlandet for oppbevaring eller behandling (jf loven del 5 – 7 samt § 27).

Ethvert datasubjekt har rett til innsyn i opplysninger om dem selv, med mindre innsyn etter en konkret vurdering må vike for avgjørende hensyn til offentlige eller

private interesser, herunder hensynet til den registrerte selv (jf § 9 annet ledd). Data-subjektet kan dessuten kreve retting eller sletting av uriktige eller misvisende opplysninger (jf § 14).

Tilsynsmyndigheten

Et Datatilsyn (Tölvunefnd) er etablert for å kontrollere at loven blir fulgt. Tilsynets fem medlemmer utnevnes av Justisministeren. Tilsynets formann, nestformann samt ett medlem til skal være jurister. Et av medlemmene skal være edb-spesialist (jf § 30). Tilsynet har vidtgående kompetanse overfor registeransvarlige til å gi bindende pålegg, føre kontroll og kreve opplysninger (jf §§ 32-33). Tilsynets avgjørelser kan ikke klages inn for andre administrative instanser (jf § 31 annet ledd).

9.5.6 Frankrike

Lovgivningen

Den sentrale lovreguleringen av personregistre i Frankrike er lov om databehandling, datafiler og individuelle rettigheter fra 1978 (Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Også andre lover er av betydning for personvernet, se for eksempel den franske forvaltningsloven fra 1979 (Loi no 79-587 du juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public) og offentlighetsloven fra 1978 (Loi no 78-753 du juillet 1978 de la liberté d'accès au documents administratifs, se særlig første kapittel).

Lov om databehandling får anvendelse både på privat og offentlig sektor. I tillegg til elektroniske registre regulerer loven også manuelle registre i den grad slike registre truer private rettigheter. Selv om lovens ordlyd bare beskytter opplysninger om fysiske personer, har loven blitt tolket slik at også opplysninger om juridiske personer til en viss grad beskyttes.

Loven oppstiller i "*Sammendrag av personregisterlovutvalgets utredning*" i kapittel 1 flere grunnleggende prinsipper for behandling av personopplysninger. Flere av prinsippene har inspirert EF-direktivets regler om helautomatisert behandling (artikkel 12 og 15), se nedenfor "*Den enkeltes rett til å motsette seg visse typer persondatabehandling*" i kapittel 11.3.

Datasubjektene gis innsynsrett og rett til å kreve retting av opplysninger om dem selv (se kapittel V). Dersom det er tale om å innhente opplysningene fra dem det gjelder, skal disse informeres om hvorvidt de har plikt til å gi fra seg opplysningene, konsekvensene av at denne plikten ikke oppfylles, samt om retten til innsyn og retting. Behandling av visse former for sensitive opplysninger (som f.eks opplysninger om straffbare handlinger og rase) er undergitt ekstra streng regulering.

Den franske databehandlingsloven gir strengere regler for offentlig sektor enn for privat sektor. Offentlige organer kan kun ta i bruk elektronisk behandling av personopplysninger dersom dette tillates av kommisjonen (eller slik behandling er hjemlet i lov, se nedenfor). For private virksomheter gjelder kun en meldeplikt. Dersom det dreier seg om trivielle behandlingsformer, som åpenbart ikke representerer noen fare for personvernet, kan både private og offentlige virksomheter nøye seg med en forenklet melding til tilsynsmyndigheten.

Tilsynsmyndigheten

Etterlevelse av den franske loven om databehandling overvåkes av en nasjonal kommisjon for databehandling m v (Commission nationale de l' Informatique et des Libertés). Kommisjonen er gitt omfattende myndighet, og har blant annet kompetanse til å forby overføring av personopplysninger til utlandet, samt kompetanse til å gi tillatelse til at offentlige organer kan anvende automatisert databehandling. Kommisjonen, som består av 17 medlemmer, er bredt sammensatt med representanter både fra privat og offentlig virksomhet. Kun tre av medlemmene oppnevnes av regjeringen. De øvrige oppnevnes i hovedsak av andre offentlige institusjoner, herunder folkeforsamlingen, Senatet og Høyesterett.

Kommisjonens avgjørelser kan være gjenstand for administrativ klage.

9.5.7 Tyskland

Lovgivningen

Verdens første personregisterlov ble vedtatt i den tyske delstaten Hesse i 1970. Den samme loven etablerte verdens første tilsynsmyndighet på dette området. I 1977 ble det vedtatt personregisterlovgivning på føderalt nivå. Loven ble i 1990 erstattet med en ny føderal lov om beskyttelse av personopplysninger (Bundesdatenschutzgesetz vom 20 Dezember 1990). I tillegg har de tyske delstatene sine egne lover på området. Disse lovene regulerer hovedsaklig delstatenes egen bruk av personopplysninger.

Den tyske grunnloven inneholder en rekke bestemmelser av betydning for personvern generelt og bruk av personopplysninger spesielt (jf § 1 (1), § 2 (1) § 10 og §13). I en kjent avgjørelse har Tysklands forfatningsdomstol (Bundesverfassungsgericht) lagt til grunn at grunnloven §§ 1 og 2 gir enkeltindividet en rett til å bestemme over opplysninger om seg selv («informationelle Selbstbestimmung»). Avgjørelsen er senere fulgt opp i senere avgjørelser. Det er fremdeles uklart hvor langt prinsippet rekker, men det synes på det rene at vernet favner videre enn personvernreglene i Europarådskonvensjonene.

Den tyske føderale loven om beskyttelse av personopplysninger definerer personopplysninger som informasjon om «personlige eller materielle forhold» om en fysisk person. Både manuell og elektronisk behandling er omfattet av loven (for elektronisk behandling gjelder noe strengere regler). Loven gjelder for privat og offentlig sektor, men delstatslovgivningen har større betydning for offentlige organer i delstatene. Til en viss grad gjelder forskjellige regler for de to sektorene.

Den tyske føderale loven oppstiller visse regler som skiller den fra de fleste andre nasjonale lover.

For det første gis det ikke særregler for behandling av sensitive data. Dette skyldes en oppfatning om at sensitivitet først og fremst er et spørsmål om hvilken sammenheng opplysningen settes inn i, og ikke noe som kan bedømmes på forhånd ut i fra opplysningens innhold.

Et annet særtrekk er at private rettssubjekter som utfører elektronisk persondatabehandling og som sysselsetter mer enn fem personer må oppnevne et *internt databeskyttelsesombud*. Hvis virksomheten behandler personopplysninger manuelt, gjelder det samme dersom virksomheten sysselsetter mer enn 20 personer. Erfaringene med slike interne ombud er delte. Særlig i små virksomheter har det vist seg at ombudene ikke besitter tilstrekkelig ekspertise og ressurser til at kontrollen blir effektiv.

For det tredje pålegger loven private virksomheter en *aktiv informasjonsplikt*; første gang virksomheten registrerer opplysninger om en privatperson, skal denne informeres om dette. Regelen har sin parallell i direktivet artikkel 10 og 11.

I likhet med den svenske loven oppstiller den tyske loven objektivt erstatningsansvar for offentlige organer som bryter lovens bestemmelser. For ikke-økonomisk skade er erstatningsansvaret begrenset oppad til 250 000 DM.

Tilsynsmyndigheten

Den føderale lovgivningen etablerer en føderal databeskyttelseskommissær som skal føre tilsyn og kontroll med at loven overholdes. Kommissæren velges av nasjonalforsamlingen (Bundestag) etter anbefaling av regjeringen, og sitter på åremål (pt fem år) med mulighet til en forlengelse. Kommissæren hører administrativt under innenriksministeren. Tilsynsmyndigheten utfører en rekke inspeksjoner for å kontrollere om lovens regler virkelig blir fulgt i praksis.

Det finnes også egne tilsynsmyndigheter i hver delstat, men disse er bare rådgivende, og har ikke myndighet til å treffe bindende beslutninger.

9.5.8 Storbritannia

Lovgivningen

Den sentrale personregisterlovgivningen i Storbritannia, «the Data Protection Act» fra 1984, trådte i kraft i sin helhet fra 1987. I motsetning til mange andre land finnes det få andre lover av betydning for behandling og beskyttelse av personopplysninger. For eksempel finnes det ingen lov om innsyn i offentlige dokumenter. (Innsyn gis dog i enkelte særlover, se for eksempel Consumer Credit Act fra 1974 og Medical Records Act fra 1990). Konstitusjonen inneholder ingen katalog med ulike menneskerettigheter, og den europeiske menneskerettighetskonvensjon er formelt ikke gjennomført i britisk rett. Forsåvidt gjelder Common Law (domstolsskapte regler med lange tradisjoner) lar det seg neppe utlede noen generell rett til personvern.

Den engelske databeskyttelsesloven får ikke anvendelse på manuell behandling av personopplysninger, og ei heller på opplysninger om juridiske eller avdøde personer.

Et av hovedtrekkene ved den engelske databeskyttelsesloven er at den går langt i å kreve at virksomheter registrerer sin databehandling hos tilsynsorganet (se nedenfor). Informasjonen som gis til tilsynsorganet skal være tilgjengelig for almenheten.

Datasubjektene gis innsynsrett i opplysninger som gjelder dem selv, og loven oppstiller dessuten åtte prinsipper for god databehandling. Prinsippene er langt på vei de samme som i europarådskonvensjonen om databeskyttelse m v (se "[Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse](#)" i kapittel 7).

Det har vært reist kritikk mot loven på flere punkter. For det første brukes mye ressurser på å kontrollere at registreringen formelt har funnet sted, mens det i liten grad legges opp til kontroll av om lovens regler faktisk overholdes. For det andre har det vært hevdet at registreringsapparatet er for tungrodd og byråkratisk sett i forhold til den nytten registreringen gir. Et tredje ankepunkt mot dagens ordning har vært at flere av lovens viktigste regler bare får anvendelse på virksomheter som er registrert, samtidig som det er god grunn til å tro at mange virksomheter unnlater å registrere seg.

Tilsynsmyndigheten

Etterlevelsen av databeskyttelsesloven overvåkes av «the Data Protection Registrar», som oppnevnes av regjeringen for fem år gangen. Tilsynsmyndigheten er

ellers uavhengig av regjeringen. De ansatte er ikke forvaltningstjenestemenn, og tilsynet rapporterer direkte til Parlamentet. I tillegg til å kontrollere at lovens regler blir fulgt, bistår tilsynet virksomheter med å utarbeide egne bransjevise atferdsnormer (se 12.5.9).

Tilsynets avgjørelser kan påklages til «the Data Protection Tribunal», hvis medlemmer oppnevnes av regjeringen. Det er kun den som vedtak retter seg mot som kan påklage vedtaket (ikke den som opplysningene gjelder). Klageorganets rettsforståelse kan bringes inn for the High Court. Engelske domstoler har i større grad enn i de fleste andre land anvendt og derigjennom utdypet databeskyttelsesloven. De fleste avgjørelsene knytter seg til hva som er utilbørlig «bruk» av personopplysninger (blant annet har domstolene vurdert om tilgang til opplysninger i seg selv er bruk i lovens forstand).

9.5.9 Ungarn

Lovgivningen

Ungarn var det første østeuropeiske landet som innførte en lov om persondatabeskyttelse. Loven (Act No LXIII on Protection of Personal Data and Disclosure of Data of Public Interest) ble vedtatt 27 oktober 1992, og trådte i kraft 1 mai 1993. Som lovens tittel antyder kombineres regler om persondatabeskyttelse med regler om offentlighet i forvaltningen. Loven viderefører bl a prinsippet i artikkel 59 i den ungarske Grunnloven fra 1949 (A Magyar Koztarsasag Alkotmanya – for tiden under revisjon):

«Everyone in the Republic of Hungary shall have the right to good reputation, the inviolability of the privacy of his home and correspondence, and the protection of his personal data.»

I en avgjørelse fra 1991 (jf Magyar Kozlony no 30 1991 s 805 814) har den ungarske forfatningsdomstolen lagt til grunn at behandling av personlige opplysninger uten noe klart formål og for vilkårlig fremtidig bruk strider mot forfatningen. Domstolens uttalelser har senere blitt kodifisert i loven om beskyttelse av persondata m v § 7 (2).

Loven om beskyttelse av personopplysninger regulerer både manuell og elektronisk behandling av personopplysninger. Opplysninger om juridiske personer vernes ikke av loven. Loven fokuserer på behandlingen av personopplysninger, og knytter ikke sin regulering til et registerbegrep. Uttrykket «behandling» er vidt definert, og omfatter bl a lagring, oppbevaring, bruk, offentliggjøring og overføring så vel som endring og sletting av personopplysninger.

Loven pålegger enhver som behandler personopplysninger å notisere ombudsmannen (se nedenfor) om aktiviteten. Fra dette gjøres visse unntak; blant annet for behandling som ledd i forskning eller rettslige avgjørelser.

I likhet med annen nyere lovgivning på området oppstiller loven enkelte grunnleggende prinsipper for behandling av personopplysninger. Et særtrekk ved lovgivningen er at den pålegger den behandlingsansvarlige plikt til aktivt å informere datasubjektene om de er pliktige til å gi fra seg opplysninger, og om hva som er formålet med innsamlingen av opplysningene.

Tilsynsmyndigheten

Loven etablerer en ombudsmannsordning som tilsynsmyndighet. I dette ligger at tilsynsmyndigheten kun har rådgivende kompetanse, og ikke kan treffe rettslig bindende vedtak. Ombudsmannen kan ikke selv bringe en sak inn for domstolene.

Datasubjektene kan derimot velge om de vil bringe saken inn for ombudsmannen eller reise sak for de ordinære domstolene. I sistnevnte tilfelle må den behandlingssansvarlige sannsynliggjøre at loven ikke er brutt.

9.5.10 Polen

Lovgivningen

Polen har etter det utvalget erfarer ennå ikke vedtatt noen lov om behandling av personopplysninger, men et utkast er på det nærmeste ferdig og det forventes at det snart vil bli lagt fram for den lovgivende forsamlingen. Lovforslaget har store likhetstrekk med EF-direktivet. På enkelte punkter foreslås imidlertid avvikende reguleringer:

- det foreslås ikke noen rett for datasubjektene til å forby helautomatisk behandling (jf direktivet artikkel 15)
- det foreslås ikke at datasubjektene skal ha rett til å kreve innsyn i dataprogrammers funksjonsmåte (se direktivet artikkel 12)
- den behandlingsansvarlige pålegges ikke noen aktiv informasjonsplikt overfor datasubjektene (jf direktivet artiklene 11 og 12)
- forslaget inneholder ikke noen uttrykkelig plikt for den behandlingsansvarlige til å kontrollere datakvaliteten
- endelig gjør forslaget trolig mer omfattende unntak fra meldeplikten enn direktivet artikkel 18 tillater.

Tilsynsmyndigheten

Det foreslås at det skal etableres en «General Inspector of Personal Data Protection» som skal velges med simpelt flertall i folkeforsamlingen (Sejm) for en fireårsperiode med mulighet for én forlengelse. Generalinspektøren – som overvåker etterlevelsen av loven og som i denne forbindelse har kompetanse til å treffe rettslig bindende beslutninger, skal avgi rapport til folkeforsamlingen. Klager over generalinspektørens avgjørelser skal i henhold til lovforslaget kunne påklages til en forvaltningsdomstol.

9.5.11 USA

Lovgivningen

Den amerikanske lovgivningen om persondatabeskyttelse – både føderale lover og delstatslovgivning – regulerer spesielle sektorer av samfunnslivet (det vi i Norge kaller særlover). Det finnes i liten grad generell lovregulering av spørsmålene, noe som har ført til at beskyttelsen av personopplysninger er ujevn og tilfeldig. USA var ikke desto mindre et av de første landene i verden som vedtok lovgivning om beskyttelse av personopplysninger, jf the «Fair Credit Reporting Act» fra 1970, som blant annet gir datasubjektene rett til innsyn i og retting av opplysninger som kreditvurderingsfirmaer besitter om dem. Den mest omfattende loven på området er the «Privacy Act» fra 1974, men selv denne nøyer seg med å regulere bruk av opplysninger om fysiske personer i føderale statlige organer. Loven får ikke anvendelse på privat sektor, og den etablerer heller ikke noe tilsynsorgan. Loven krever imidlertid at føderale statlige organer melder fra om sine registre til et føderalt register som skal inneholde opplysninger om hvilket formål det enkelte register har, og hvordan datasubjektene kan få innsyn i disse. Dessuten oppstilles en del grunnleggende prinsipper for hvordan personopplysninger skal behandles, som for eksempel at den behandlingsansvarlige i saker av en viss viktighet bør innhente opplysningene fra

den det gjelder, og at videregivelse av opplysninger som hovedregel krever samtykke fra datasubjektet.

Privacy Act er etterhvert supplert av annen lovgivning som for eksempel «the Computer Matching and Privacy Protection Act» fra 1988. Loven forbyr ikke samkjøring av registre, men oppstiller enkelte retningslinjer for hvordan samkjøringen skal foretas. Blant annet kreves det at de registeransvarlige på forhånd avgjør hva formålet med samkjøringen er, hvilken hjemmel den har samt at det må etableres tilsynsrutiner. Det stilles også krav til datakvaliteten; for eksempel må datasubjektet varsles og gis rett til å ta til motmæle før opplysningene fra samkjøringen benyttes som grunnlag for en avgjørelse som retter seg mot datasubjektet.

Som nevnt ovenfor finnes det ikke lovgivning som regulerer behandling av personopplysninger i privat sektor. En rekke private virksomheter har imidlertid anbefalt at OECDs retningslinjer (se 9.2) blir fulgt.

Også amerikanske domstoler, som i større grad enn norske har en rettsskapende funksjon, har tradisjonelt vært tilbakeholdne med å statuere generelle personvernrettigheter for den enkelte. Enkelte høyesterettsdommer fra de senere år kan tyde på at dette er i ferd med å endre seg.

Tilsynsmyndigheten

Som nevnt ovenfor er det ikke etablert noen tilsynsmyndighet i USA. Dette har ført til at lovgivningen etter alt å dømme er lite effektiv. For eksempel viser undersøkelser at unntakene fra de grunnleggende kravene til behandling av personopplysninger ofte benyttes i mye større grad enn lovene selv gir grunnlag for.

9.5.12 Canada

Lovgivningen

Den viktigste lovreguleringen av personvern i Canada er «the Privacy Act» fra 1982. Formålet med loven er

«to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution ...» (s 2)

Som det fremgår, får loven ikke anvendelse på privat sektor, men kun på føderale statlige organers behandling av opplysninger om fysiske personer. Loven oppstiller for øvrig en katalog over prinsipper for behandling av personopplysninger. Blant annet heter det at informasjon ikke skal samles inn medmindre informasjonen skal benyttes direkte i et pågående program eller aktivitet hos institusjonen. Rutinemesig innsamling av informasjon for mulig senere bruk skal med andre ord ikke finne sted. Videre skal opplysninger som hovedregel innhentes fra den det gjelder (men unntakene er mange). Datasubjektene har innsynsrett i opplysninger om dem selv.

En svakhet ved den kanadiske føderale lovgivning er at loven – i likhet med den amerikanske lovgivningen på området – ikke får anvendelse på privat sektor. Heller ikke delstatene (Med unntak av Quebec) har lovregulert persondatabehandling i privat sektor.

Tilsynsmyndigheten

Privacy Act etablerer en «Privacy Commissioner» som skal tilse at lovens regler etterleves. Kommissæren oppnevnes av Parlamentet for syv år av gangen, og rap-

porterer direkte til Parlamentet. I tillegg er det etablert en parlamentskomité som skal føre tilsyn med myndighetenes behandling av personopplysninger.

Kommissæren har langt på vei en ombudsmannsfunksjon, hvis primære oppgave er å behandle klager over de føderale statsorganenes behandling av personlige opplysninger. Tilsynsmyndigheten har ikke kompetanse til å treffe rettslig bindende avgjørelser. Både kommissæren og datasubjektet har imidlertid adgang til å bringe klager inn for en føderal domstol dersom det føderale forvaltningsorganet nekter å gi datasubjektet innsynsrett.

Kommissæren har anbefalt at private virksomheter selv lager atferdsnormer (se 12.5.9) som regulerer behandling av personopplysninger. Dette har blitt fulgt opp (jf for eksempel the Canadian Standards Associations Model Code for the Protection of Personal Information fra 1996 som i stor grad bygger på OECDs retningslinjer).

9.5.13 Japan

Lovgivningen

Den viktigste japanske lovgivningen på området er lov om elektronisk behandlede persondata i forvaltningsorganer fra 1988. Loven er dels basert på OECDs retningslinjer, og dels på bestemmelser i den japanske Grunnloven, jf for eksempel § 13:

«All the people shall be respected as individuals. Their right to life, liberty and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs.»

Den japanske lovgivningen har imidlertid et nokså snevert anvendelsesområde. Lovgivningen får ikke anvendelse på manuell behandling av personopplysninger, og ei heller på privat sektor. Kun statlige forvaltningsorganer er underlagt loven (kommunale og regionle organer faller utenfor).

Loven oppstiller en del grunnleggende prinsipper for behandling av personopplysninger. Prinsippene er i stor grad basert på OECDs retningslinjer. Unntak som gjør at prinsippene ikke behøver å følges er mange og omfattende. For eksempel har ikke datasubjektet krav på innsyn dersom behandlingen har betydning for statsansatte, skatteberegning, politietterforskning, eller «examinations of knowledge and skill, reviews of qualifications etc, assesments of compensation of benefit etc, or other estimates or judgements corresponding to them» (jf § 14 (1) og § 7 (3)).

Opplysninger om statslige forvaltningsorganers behandling av personopplysninger skal sendes til tilsynsmyndigheten (se nedenfor), som publiserer opplysningene i en årlig publikasjon.

Japans føderale lovgivning på området suppleres av lokale regelverk.

Tilsynsmyndigheten

Det er ikke etablert noen uavhengig myndighet til å føre tilsyn med at loven etterleves. Loven hører under den japanske statsministerens kontor.

9.5.14 Australia

Lovgivningen

Australias føderale «Privacy Act» fra 1988 regulerer føderale myndigheters behandling av opplysninger om fysiske personer. I noen grad får loven også anvendelse

på privat sektor (for eksempel kredittopplysningsvirksomhet og virksomhet som benytter fødselsnummer). Loven suppleres av «the Freedom of Information Act» fra 1982 som gir datasubjektene rett til innsyn og retting. I tillegg har enkelte delstater vedtatt egen lovgivning på området.

Personvern har ikke konstitusjonelt vern, og noe slikt generelt vern er heller ikke etablert gjennom rettspraksis. Enkelte avgjørelser har imidlertid stilt opp et formålsbestemthetsprinsipp, som slår fast at bruken av opplysninger begrenses ut i fra formålet med innsamlingen.

Hjørnesteinen i den australske lovgivningen på området er elleve «Information Privacy Principles» som regulerer innsamling, bruk, oppbevaring og videregivelse av personopplysninger. Prinsippene er bl a basert på OECDs retningslinjer, men har vidtgående unntaksmuligheter som reduserer prinsippenes praktiske betydning. Brudd på prinsippene kan forfølges i domstolsapparatet. Det kan kreves erstatning også for ikke-økonomisk tap.

Ett av prinsippene for behandling av personopplysninger går ut på at de behandlingsansvarlige plikter å melde fra til Kommissæren (se nedenfor) om grunnleggende informasjon om hvilke typer personopplysninger de besitter. Opplysningene blir deretter publisert i en årlig rapport («Personal Information Digest»).

EF-direktivet har foranlediget forslag om å regulere bruk av personopplysninger også i privat sektor. Noe av bakgrunnen for dette er frykt for at mangel på slik regulering kan føre til at EU/EØS-land nekter å gi tillatelse til at personopplysninger kan overføres til Australia.

Tilsynsmyndigheten

En «Privacy Commissioner» er oppnevnt av regjeringen, men er funksjonelt uavhengig av denne. Administrativt hører kommisjonæren under en bredere tilsynsmyndighet (the Human Rights and Equal Opportunity Commission). Kommissæren oppnevnes for syv år av gangen. I tillegg er det etablert en komité (the Privacy Advisory Committee) som skal bistå kommissæren blant annet med råd. Komiteen består av seks medlemmer fra ulike samfunnsområder.

Kommissæren skal bl a føre tilsyn og gi råd. I tillegg er tilsynsmyndigheten gitt kompetanse til å tillate at forvaltningsorganer i enkelttilfeller kan fravike lovens regler dersom det offentliges interesser i å fravike reglene er klart tyngre enn det offentliges interesser i at reglene blir fulgt (sk «Public Interest Determinations»). Kommissæren kan også gi rettslig bindende pålegg om opphør av virksomhet som er i strid med loven samt utforme retningslinjer for ulike former for behandling av personopplysninger (herunder samkjøring av registre mellom enkelte offentlige myndigheter).

Flere av delstatene har opprettet uavhengige «Privacy Committees» som fungerer som ombudsmenn. Komiteene kan foreta granskning, men har ikke kompetanse til å treffe rettslig bindende avgjørelser.

9.5.15 New Zealand

Lovgivningen

New Zealands «Privacy Act» er fra 1993. Loven har et omfattende anvendelsesområde, og regulerer de fleste former for manuell og elektronisk behandling av opplysninger om fysiske personer både i privat og offentlig sektor. Kjernen i loven er tolv prinsipper for behandling av personopplysninger. Enkelte særregler gis for offentlige registre, blant annet søker man å unngå at opplysninger i slike registre

utnyttet for kommersielle formål. Det gis også detaljerte regler om samkjøring av informasjonsbaser.

Tilsynsmyndigheten

En «Privacy Officer» skal føre tilsyn med at loven etterleves. Han eller hun er oppnevnt av regjeringen (tilsvarende justisdepartementet), men er ellers uavhengig av denne såvel som av den lovgivende forsamling. I noen henseende har tilsynsmyndigheten i New Zealand mindre kompetanse enn tilsvarende organer i de fleste andre land. For eksempel har tilsynet ikke adgang til å utføre uanmeldte «på-stedet» kontroller. Kommisjæren kan utføre undersøkelser og motta klager over at loven er brutt, men har ikke kompetanse til selv å treffe rettslig bindende avgjørelser. Dersom den ansvarlige ikke retter seg etter kommisjonærens uttalelser, kan saken bringes inn for «the Complaints Review Tribunal», som er en slags nemnd. Nemnda har adgang til å tilkjenne erstatning på opptil NZD \$200,000. Nemndas avgjørelser kan bringes inn for de ordinære domstolene.

Et av de mest fremtredende særtrekkene ved tilsynsmyndigheten er at den har myndighet til å utforme rettslig bindende regler som kan avvike fra lovens bestemmelser. På denne måten utformes særregler for ulike bransjer. Reglene blir til etter omfattede høringer.

Tilsynsmyndigheten kan be om å få opplysninger om den enkelte virksomhet, men det er ikke etablert noe konsesjonssystem eller noen meldepliktsordning.

I tillegg kreves det at enhver virksomhet skal utnevne en egen «Privacy Officer» hvis oppgave likner den tilsvarende tyske ordningen (se ovenfor 9.5.7).

Del II Noen hovedspørsmål

KAPITTEL10

Lovens saklige og geografiske virkeområde**10.1 LOVENS SAKLIGE VIRKEOMRÅDE****10.1.1 Personopplysninger***10.1.1.1 Personregisterlovens definisjon*

Personregisterloven definerer personopplysninger som «opplysninger og vurderinger som direkte eller indirekte kan knyttes til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser» (§ 1 annet ledd). Begrepet er meget vidtrekkende, og omfatter både faktiske opplysninger og vurderinger så lenge opplysningene knyttes direkte eller indirekte til en person. Et navn vil gi en direkte tilknytning, mens f.eks. et bilnummer eller et telefonnummer kan være en indirekte identifikasjon. Det er imidlertid et minstevilkår at den personen som opplysningen gjelder, må kunne identifiseres. Et 11-sifret personnummer vil alltid gi en entydig identifikasjon. Det kan imidlertid også være mulig å identifisere en person uten opplysninger om navn, adresse eller fødselsnummer for eksempel ved opplysninger om yrkeskategori, utseende eller lignende, f.eks. «sorenskriveren i Halden» eller «politimesteren i Oslo». Hva som er å anse som tilstrekkelig identifikasjon, må avgjøres konkret i hvert enkelt tilfelle. F.eks. kan en anonym undersøkelse hvor det registreres opplysninger om hver enkelt elev ved en skole i noen tilfeller sies å utgjøre et personregister, andre ganger ikke. Dette kan avhenge av hvor stor skolen er, hvor entydig klassene er beskrevet, kjønnsfordelingen på skolen og i klassene, om enkelte elever skiller seg merkbart ut m.v.

Statistikkopplysninger vil som regel ikke kunne knyttes til enkeltpersoner slik at den enkelte person kan identifiseres. Dersom statistikken omfatter svært få personer, kan dette unntaksvis medføre at kravet til identifikasjon er oppfylt også for denne typen opplysninger.

Opplysninger om en identifiserbar gruppe personer er ikke å anse som personopplysninger med mindre kravet til identifikasjon er oppfylt også overfor den enkelte person i gruppen.

Loven omfatter opplysninger om både fysiske og juridiske personer, dvs. både opplysninger om enkeltpersoners private forhold og opplysninger om sammenslutninger (ulike selskapstyper) og stiftelser. Det betyr at reglene også gjelder for opplysninger om selskapers eier-, regnskaps-, og produksjonsforhold.

Som det har fremgått, er det ikke opplysningstypen i seg selv som avgjør om opplysningen er en personopplysning slik personregisterloven nytter begrepet, men hvorvidt opplysningen direkte eller indirekte kan knyttes til en person. Det er derfor ikke noe sammenfall mellom begrepet «personopplysning» og begrepet «personlige forhold» som benyttes i andre lover (taushetspliktlovgivning, f.eks. forvaltningsloven § 13) – begrepet personopplysninger er atskillig videre. Forklaringen på dette ligger i at personvernlovgivningen og taushetspliktlovgivningen ivaretar forskjellige hensyn – selv om de også overlapper hverandre delvis. Diskresjonshensynet som er et hovedhensyn bak taushetspliktlovgivningen rekker ikke lenger enn å begrunne restriksjoner på spredning av en kvalifisert type opplysninger; opplysninger om personlige forhold. Det er imidlertid flere hensyn som i mange tilfeller vil være minst like viktige i personvernsammenheng, f.eks. hensynet til fullstendighet og innsyn (jf *"Hva er personvern?"* i kapittel 3).

10.1.1.2 Internasjonale regler

Definisjonen av «personopplysninger» i personregisterloven er sammenfallende med *EF-direktivets* definisjon, med den forskjell at direktivet kun omfatter opplysninger om fysiske personer, jf artikkel 2 a):

«I dette direktiv forstås ved:

- a) «personopplysninger», enhver form for informasjon om en identificeret eller identifiserbar fysisk person («den registrerede»); ved identifiserbar person forstås en person, der direkte eller indirekte kan identifiseres, bl. a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet;»

Direktivet er imidlertid ikke til hinder for at man i norsk lovgivning også lar loven omfatte opplysninger om juridiske personer, jf fortalen nr 24 («dette direktiv berører ikke national lovgivning, der beskytter juridiske personer i forbindelse med behandlingen af oplysninger, der berører dem»).

Europarådskonvensjonen definerer «personopplysninger» slik i artikkel 2 a):

«enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson («datasubjekt»).

10.1.1.3 Utvalgets vurderinger

Kriteriet «som direkte eller indirekte kan knyttes til en identifiserbar person» har flere svakheter. Det kan i visse tilfelle være uklart om en opplysning kan knyttes til en identifiserbar person (f eks ved statistikkopplysninger om noen få personer, se foran).

Personopplysningsbegrepet slik det brukes i personregisterloven er svært vidtrekkende, og favner kan hende videre enn personverninteresser kan begrunne. Utvalget har derfor funnet det naturlig å vurdere om det bør gis en definisjon av personopplysninger som er *snevrere* enn dagens definisjon. En slik løsning er tatt i bruk i andre lover, se f eks forvaltningsloven § 13 om taushetsplikt for opplysninger om «personlige forhold», hvor mindre sensible opplysninger ikke omfattes av taushetsplikten. På den annen side kan en slik snevrere definisjon neppe knyttes opp mot definisjonen i forvaltningsloven § 13 – til det er sistnevnte bestemmelse for snever. Utvalget har også lagt vekt på at direktivets definisjon av personopplysninger langt på vei er sammenfallende med personregisterlovens definisjon. Endelig kan sondringen mellom trivielle og sensible personopplysninger (fremdeles) tillegges betydning på annen måte, f eks ved at behandlingen av følsomme personopplysninger undergis en strengere regulering. Utvalget går etter dette inn for å videreføre dagens definisjon av personopplysninger. Om tilknytningen og/eller identifiseringen er tilstrekkelig, må fremdeles avgjøres konkret. Formålsbestemmelsen i lovforslaget kan gi veiledning i denne vurderingen.

Utvalget har vurdert om loven også bør verne opplysninger om en *gruppe personer*. Et eksempel på at en gruppe personer er gitt vern på andre områder, er strl § 135a. Utvalget finner imidlertid ikke at det er behov for å la personopplysningsbegrepet også omfatte opplysninger om en identifiserbar gruppe personer. Slike opplysninger vil meget sjelden kunne oppfattes som strengt personlige på samme måte som opplysninger om enkeltpersoner, jf det integritets-fokuserte personvernet (3.3.2). Det vil dessuten medføre vanskelige avgrensingsproblemer.

10.1.1.3.1 Særlig om opplysninger om juridiske personer

Personregisterloven får som nevnt anvendelse på opplysninger som kan knyttes til identifiserbare sammenslutninger eller stiftelser, jf § 1 annet ledd. Begrepet «sammenslutninger» omfatter både selskaper og foreninger. På bakgrunn av at personvernlovgivningen i de fleste andre land (se 9.5), samt EF-direktivet kun får anvendelse på opplysninger om fysiske personer, er det grunn til å vurdere om loven fremdeles bør få anvendelse på slike opplysninger.

Problemstillingen var også fremme under forberedelsen av personregisterloven. Både Sandvik-utvalget og Seip-utvalget begrenset utredningene og lovforslagene til å gjelde beskyttelse av opplysninger om fysiske personer. Dette har – i alle fall for Seip-utvalgets del – antagelig sammenheng med at utvalget iht mandatet skulle ta utgangspunkt i «de datasystem som hovedsaklig inneholder opplysninger om fysiske personer i motsetning til 'juridiske personer'» (NOU 1975: 10 side 7). Sandvik-utvalget foreslo i sitt lovutkast enkelte særregler for personer som er næringsdrivende. Departementet la for sin del avgjørende vekt på at det kunne være vanskelig å trekke grensen for hva som er opplysninger om fysiske personer og hva som er opplysninger om juridiske personer, samt at innholdet i mange av lovens bestemmelser logisk innbefattet juridiske personer. (Ot prp nr 2 1977-78 s 26 v sp). Det ble likevel understreket at (op cit):

«Det her nevnte utgangspunkt medfører naturligvis ikke at opplysninger om fysiske personer og juridiske personer i enhver henseende skal behandles likt: Det knytter seg betydelig offentlig interesse til bedriftenes virksomhet, og bedriftsopplysningene kan ikke beskyttes etter samme normer som opplysninger om private forhold. Dessuten har bedriftene generelt større evne til å vareta sine interesser enn den enkelte privatperson.»

Føyen vurderte i sin utredning om loven burde endres slik at den bare fikk anvendelse på opplysninger om fysiske personer (Føyenutredningen s 70), men kom til at en slik endring ikke var ønskelig. Departementet og Stortinget var ved lovrevisjonen i 1987 enig i dette (jf Ot prp nr 34 (1986-87) s 18 og Innst O nr 64 (1986-87) s 5.

Internasjonalt er det etter hva utvalget erfarer bare fire land – Island, Østerrike, Luxemburg og Sveits – som i sin personvernlovgivning verner opplysninger om juridiske personer på en tilsvarende generell måte som den norske loven i dag gjør. Den danske loven om private registre får også anvendelse på opplysninger om juridiske personer, men gjelder bare for privat sektor, og gir heller ikke innsynsrettigheter (med unntak for kredittopplysningsvirksomhet). For å gi et riktig bilde av reguleringen i andre land må det imidlertid også tas med at opplysninger om juridiske personer kan vernes på andre måter enn gjennom generelle lovbestemmelser. For det første kan tilsynsmyndigheten i sine *konsesjonsvedtak* fastsette vilkår om at også juridiske personer skal gis visse rettigheter – et eksempel på dette er at den franske tilsynsmyndigheten (CNIL) i 1984 satte som vilkår for opprettelse av offentlige databaser at juridiske personer som ble registrert i basene bl a skulle gis innsynsrett og mulighet til å kreve retting av feilaktige opplysninger (den franske loven omfatter ikke opplysninger om juridiske personer). For det andre kan opplysninger om juridiske personer være vernet på *bestemte sektorer* (slik som for eksempel i Sverige der juridiske personer er gitt rettigheter bl a overfor kredittopplysningsvirksomhet). For det tredje kan opplysninger om juridiske personer i visse tilfelle *også anses som opplysninger om fysiske personer*, og av den grunn – så langt overlappingen rekker – omfattes av loven. Samlet sett er imidlertid inntrykket at de fleste land velger å utelate opplysninger om juridiske personer fra sin personvernlovgivning.

Utvalget er enig i at også opplysninger om juridiske personer (f eks opplysninger om produksjonsplaner, regnskap etc) ofte vil ha et legitimt behov for vern. Behovet for å verne denne typen av opplysninger er imidlertid i stor grad begrunnet i andre hensyn enn personvern hensyn. Som oftest er det økonomiske interesser som gjør seg gjeldende – i motsetning til tradisjonelle personverninteresser (ikke-økonomiske interesser). Foran i "*Hva er personvern?*" i kapittel 3 er det «integritetsfokuserte» personvernet beskrevet som et ønske om å ha kontroll med opplysninger som *oppleves* som strengt personlige; en juridisk person har ingen slik opplevelse. Ut i fra det «maktfokuserte» personvernet gjør heller ikke de samme hensyn seg gjeldende. Styrkeforholdet mellom store markedsaktører eller myndigheter og juridiske personer er som regel (avhengig av størrelsen på den juridiske person) ikke så skjevt som mellom førstnevnte gruppe og en enkelt fysisk person. Opplysninger om juridiske personer er dessuten ofte regulert av annen lovgivning (se eksempler foran under 6.1).

På denne bakgrunn har utvalget kommet til at opplysninger om juridiske personer ikke direkte bør omfattes av loven. Utvalget peker imidlertid på to viktige presiseringer:

For det første understrekes at loven omfatter opplysninger (om fysiske personer) som knytter seg til juridiske personer (f eks opplysninger om at en person er registrert som innehaver av en virksomhet). Dette innebærer at opplysninger om enkeltmannsforetak alltid vil være opplysninger om fysiske personer og dermed omfattes av loven. Denne typen personopplysninger står på sett og vis i en særstilling, fordi allmenheten som oftest har en berettiget interesse i opplysninger om næringsvirksomheten.

For det andre vil det i utgangspunktet ikke være noe i veien for å gi opplysninger om juridiske personer samme vern som opplysninger om fysiske personer selv om loven ikke krever det. Flere av de materielle bestemmelsene som utvalget foreslår hviler på et bredere tilfang av hensyn enn tradisjonelle personverninteresser, og en frivillig utvidende anvendelse av loven i favør av registrerte juridiske personer kan på endel områder fremstå som naturlig. Utvalgets forslag til endring av dagens rettstilstand behøver derfor ikke nødvendigvis å måtte føre til omlegninger av måten opplysninger er systematisert og oppbevart på i dag.

10.1.1.3.2 Vern av opplysninger om døde personer

Personregisterloven skiller – i hvertfall etter sin ordlyd – ikke mellom opplysninger om døde og levende personer. Rettstilstanden på dette området er derfor noe uvis. Datatilsynet har lagt til grunn at opplysninger om døde personer omfattes av loven dersom opplysningene forteller noe om levende personer (f eks dødsårsaksregisteret). Ny teknologi (f eks gen- og bioteknologi) har gjort problemstillingen mer aktuell enn før, bl a fordi slike opplysninger kan gi ny informasjon om egenskaper hos gjenlevende personer (se nærmere "*Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet*" i kapittel 4).

Utvalget legger til grunn at i de tilfellene de registrerte opplysningene også gir opplysninger om gjenlevende personer (f eks opplysninger om arvelige sykdommer) vil dette være en personopplysning i lovens forstand. Spørsmålet blir videre om det er grunn til å ta et skritt videre og la også opplysninger som *ikke* direkte eller indirekte kan knyttes til en gjenlevende person omfattes av loven.

Flere hensyn kan tale for en slik løsning. For det første vil hensynet til den avdødes gjenlevende slektninger og bekjente kunne begrunne et vern av opplysningene om avdøde. For det andre kan det spørres om hensynet til avdødes ettermæle i seg selv (uavhengig av betydningen for slekten) har krav på vern. Det er grunn til

å tro at de fleste – mer eller mindre ubevisst – ønsker et godt eller i det minste et mest mulig korrekt omdømme også etter ens død. Vissheten om manglende regulering av behandling av opplysninger om døde personer vil derfor kunne få betydning for disposisjoner vedkommende foretar mens han ennå er i live. Hvis loven får anvendelse på opplysninger om avdøde personer, er det f.eks. grunn til å tro at dette gir folk større tiltro til behandling av personopplysninger, noe som er viktig for bransjer og offentlige institusjoner som er avhengige av å innhente personopplysninger fra den opplysningene gjelder, eller som må få vedkommendes samtykke til å innhente slike opplysninger.

Når utvalget likevel ikke foreslår at loven bør omfatte opplysninger om døde personer når opplysningene ikke kan knyttes til noen gjenlevende person, skyldes dette dels at en slik løsning kan få konsekvenser som det er vanskelig å ha oversikt over – for eksempel oppstår vanskelige spørsmål i forhold til arkivlovgivningen og i forholdet til f.eks. historieforskning og annen bruk av opplysninger om døde personer – og dels at opplysninger om døde personer er vernet av andre regler, som for eksempel taushetspliktregelen i forvaltningsloven § 13 første ledd (som omfatter opplysninger om avdødes personlige forhold). Utvalget går etter dette inn for at gjeldende rett videreføres, slik at loven får anvendelse på opplysninger om døde personer dersom disse opplysningene direkte eller indirekte kan knyttes til identifiserbare gjenlevende personer.

10.1.2 Behandling av personopplysninger

10.1.2.1 Registerbegrepet

10.1.2.1.1 Personregisterlovens definisjon

Personregisterloven definerer «personregistre» i § 1 annet ledd annet punktum:

«Med personregistre er ment registre, fortegnelser m.m. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen.»

Loven sonderer med andre ord ikke mellom manuelle og elektroniske registre. Det avgjørende for om en samling personopplysninger utgjør et «personregister», er om opplysningene er samlet systematisk slik at man kan gå inn i registeret og finne igjen opplysninger om en bestemt person. Et kortregister eller et arkiv med hengemapper er etter dette et «personregister» dersom det er ordnet etter personers navn, fødselsnummer eller, men ikke dersom det er ordnet etter journalnummer, saksområde eller lignende tematiske registernøkler, og det ikke finnes noen nøkkel som gjør at man kan finne frem til opplysninger om bestemte enkeltpersoner (jf nærmere Ot prp nr 2 (1977-78) s 69).

Kravet til systematikk har liten selvstendig betydning i relasjon til datamaskinbaserte systemer. Selv om systemet ikke er spesielt tilrettelagt for søk på enkeltpersoner, er det enkelt å foreta endringer slik at personer kan brukes som søkekriterier. Det avgjørende for om slike systemer er personregistre i lovens forstand, er om det er mulig å finne igjen opplysninger om den enkelte registrerte.

Datatilsynet har i sin praksis lagt til grunn at et personregister som inneholder så få opplysninger at man med letthet kan bla igjennom registeret og finne opplysningene om den enkelte, er å anse som et personregister i lovens forstand uavhengig av kravet til systematikk. På den annen side ligger det i begrepet «personregister» at det må dreie seg om en samling av opplysninger om et visst antall personer; opplysninger om to eller tre personer vil ikke utgjøre et personregister. Hvor den nedre grensen går (for antall registrerte) er imidlertid uklart.

Begrepet «personregister» var gjenstand for diskusjon både under forberedelsen av personregisterloven og i forbindelse med senere lovendringer. I Føynutredningen ble det foreslått at man gikk bort fra personregisterbegrepet (jf St meld nr 14 (1983-84) s 82):

«Begrepet slik det står i dag medfører enkelte praktiske problemer, som man vel kan ta stilling til gjennom tolkning fra sak til sak – om problemet kommer på spissen. Det blir imidlertid stadig tydeligere at registerbegrepet i sin nåværende form er kunstig. Det er nærliggende å begrense enhver form for innsamling, lagring og bruk av personopplysninger, idet de moderne hjelpemidlene relativt lett vil kunne brukes til å finne opplysninger fram, uten at de er «lagret systematisk».

Når man i forbindelse med lovrevisjonen likevel valgte å beholde personregisterbegrepet skyldtes dette blant annet at en annen løsning kunne skape problemer når man valgte å videreføre konsesjonsordningen i sin daværende form (jf Ot prp nr 34 (1986-87) s 14).

10.1.2.1.2 Internasjonale regler

Manuell behandling av personopplysninger omfattes av direktivet i den grad personopplysningene inngår eller skal inngå i et personregister. I direktivet artikkel 2 c) er «register med personopplysninger» («register») definert slik:

«enhver strukturert samling af personopplysninger, der er tilgjengelige efter bestemte kriterier, hvad enten denne samling er placeret sentralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grunnlag».

Registerbegrepet har kun betydning for direktivets anvendelse på manuell behandling av personopplysninger, jf artikkel 3 nr 1. Registerbegrepet spiller med andre ord en mer underordnet rolle i EF-direktivet enn i personregisterloven.

I *Europarådskonvensjonen* har man valgt en noe annen løsning; i tillegg til å benytte et behandlingsbegrep, gjør konvensjonen bruk av et «elektronisk dataregisterbegrep», som defineres slik i artikkel 2 b):

«ethvert sett av opplysninger som blir bearbeidet ved elektronisk databehandling».

10.1.2.1.3 Utvalgets vurderinger

Den tekniske utviklingen har ført til at registerbegrepet ikke lenger er like godt egnet som et hensiktsmessig avgrensingskriterium for lovens virkeområde som det var da personregisterloven ble vedtatt i 1978. Dagens søkesystemer gjør at det kan søkes med personer som nøkkel selv om samlingen av opplysninger ikke har dette som formål, se "*Fra registre til annen organisering av personopplysninger*" i kapittel 4.3. Utvalget har også lagt vekt på at man i tråd med EF-direktivet i større grad enn nå vil benytte andre reguleringsmetoder enn konsesjon, og departementets betenkeligheter med å forlate registerbegrepet (se henvisningen ovenfor til Ot prp nr 34 (1986-87)) gjør seg derfor i mindre grad gjeldende.

Utvalget går inn for at loven bør omfatte all elektronisk behandling av personopplysninger. Hva som menes med «behandling», fremgår nærmere under 10.1.2 nedenfor.

For *manuell* behandling av personopplysninger foreslår utvalget at registerbegrepet opprettholdes som avgrensingskriterium. Se 10.1.2.3.3 nedenfor om grensen mellom manuell og hel eller delvis elektronisk behandling.

10.1.2.2 Behandlingsbegrepet

10.1.2.2.1 Gjeldende rett

Personregisterloven gir ikke noen generell definisjon av «behandling av personopplysninger» slik direktivet gjør (se nærmere nedenfor). I loven kapittel 6 gis det riktignok særskilte regler for «databehandlingsforetak», dvs virksomhet som består i å bearbeide personopplysninger *for andre* ved elektroniske hjelpemidler. *Egen* bearbeiding av personopplysninger med elektroniske hjelpemidler omfattes imidlertid ikke av databehandling slik personregisterloven nytter ordet.

10.1.2.2.2 Internasjonale regler

Begrepet «behandling av personopplysninger» («behandling») defineres slik i artikkel 2 b):

«enhver operation eller række af operationer – med eller uden brug af elektronisk databehandling – som personopplysninger gøres til genstand for, f. eks. innsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring samt blokering, slettelse eller tilintetgørelse».

Direktivet får anvendelse på hel eller delvis elektronisk behandling av personopplysninger, samt på manuell behandling av personopplysninger der disse inngår eller skal inngå i et personregister, jf artikkel 3 nr 1.

Fra dette utgangspunktet gjelder visse unntak; direktivet gjelder ikke for behandling av personopplysninger som ikke omfattes av fellesskapsretten, og under enhver omstendighet ikke for behandling som angår den offentlige sikkerhet, forsvar, statens sikkerhet, statens økonomiske tilstand og statens aktiviteter på det strafferettslige området (jf artikkel 3 nr 2). Direktivet omfatter heller ikke fysiske personers utøvelse av rent private eller personlige aktiviteter, se nærmere nedenfor. Selv med disse modifikasjonene er det imidlertid på det rene at direktivet krever at det saklige virkeområdet til den norske loven utvides.

Europarådskonvensjonen definerer «elektronisk databehandling» som:

«følgende operasjoner dersom de utføres helt eller delvis ved hjelp av automatiserte metoder: lagring av opplysninger, utføring av logiske og/eller aritmetriske operasjoner i tilknytning til disse opplysningene samt forandring, sletting, gjenfinning eller spredning av dem;».

10.1.2.2.3 Utvalgets vurderinger

Utvalget går inn for at begrepet «elektronisk behandling» av personopplysninger bør brukes til å avgrense lovens saklige virkeområde, sammen med manuell behandling av personopplysninger der personopplysningene inngår eller skal inngå i et personregister. Utvalget foreslår en definisjon som samsvarer med direktivets definisjon.

EF-direktivet (artikkel 2 b) definerer behandling av personopplysninger slik: *enhver operasjon eller rekke av operasjoner – med eller uten bruk av edb – som personopplysninger gøres til gjenstand for*. Direktivet har videre en eksemplifisering av dette som kan være til hjelp:

- innsamling
- registrering
- systematisering

- oppbevaring
- tilpasning eller endring
- seleksjon
- søking
- bruk
- alle former for videregivelse/utlevering
- sammenstilling/samkjøring/kobling
- blokkering
- sletting eller tilintetgjørelse

En behandling utgjør med andre ord én operasjon eller (i de fleste tilfeller) *en rekke* operasjoner (jf direktivet). En behandling kan derfor innebære f eks både innsamling, registrering, lagring, endring, utlevering og sletting. Det er denne rekken av operasjoner som informasjonssystemet utfører som er en behandling. For eksempel vil en forsker som innhenter personopplysninger fra en utvalgt gruppe personer, kobler disse med opplysninger fra et annet tilgjengelig register og lagrer opplysningene i 5 år for et senere planlagt oppfølgingsprosjekt, kun anses for å utføre én behandling av personopplysninger.

Som det fremgår ovenfor, kan «behandling» av personopplysninger omfatte ulike operasjoner, som f eks innsamling og bruk. Det er imidlertid ikke gitt at det bør være identiske regler for alle former for behandling. I enkelte henseende bør det ved utformingen av reglene skilles mellom ulike former for behandling.

10.1.2.3 Elektronisk og manuell behandling

10.1.2.3.1 Gjeldende rett

Personregisterloven gjelder for «personregistre og for annen bruk av personopplysninger...» uavhengig av om registeret eller bruken av opplysningene skjer manuelt eller elektronisk, jf prgl § 1 første ledd. Det er imidlertid visse forskjeller m h t hvilke regler som gjelder for henholdsvis manuelle og elektroniske registre, se prgl § 7 (innsynsrett) og § 9 (konsesjonsplikt).

10.1.2.3.2 Internasjonale regler

EF-direktivets saklige virkeområde er avgrenset til å gjelde behandling av personopplysninger, og direktivet skiller her mellom elektronisk og manuell behandling. I utgangspunktet gjelder direktivet for all elektronisk behandling, mens manuell behandling kun omfattes dersom personopplysningene inngår eller vil inngå i et personregister. Det er også i direktivet visse forskjeller m h t hvilke regler som gjelder for henholdsvis manuelle registre og elektroniske behandlinger av personopplysninger; f eks knytter direktivet i utgangspunktet meldeplikten til de elektroniske behandlingene (artikkel 18 nr 1), men overlater til medlemslandene å bestemme i hvilken grad manuell behandling også skal omfattes av meldeplikten (nr 5).

10.1.2.3.3 Utvalgets vurderinger

Ut i fra personvern hensyn knytter det seg ikke alltid de samme betenkeligheter til manuelle personregistre som til forskjellige typer elektronisk behandling av personopplysninger. Manuelle registre gir ikke de samme muligheter for kobling, spredning og gjenbruk av den informasjonen som er lagret. Dersom opplysningene skal benyttes som beslutningsgrunnlag, gjør imidlertid de samme personvern hensynene

seg gjeldene også her (se ovenfor under 3.3.4 om det beslutningsfokuserede personvernet). Innsamling av enkelte opplysninger (særlig strengt personlige opplysninger) kan dessuten i seg selv oppleves som et inngrep i den personlige integriteten (se 3.3.2 om det integritetsfokuserede personvernet) som kan begrunne at behandling av slike opplysninger bør underlegges en eller annen form for regulering og kontroll. Det er også av betydning at ny teknologi (f eks scanningutstyr) i stadig større grad visker ut skillet mellom papirbasert manuell behandling og behandling med elektroniske hjelpemidler. Loven bør derfor fremdeles omfatte opprettelse og bruk av manuelle personregistre.

Loven omfatter all *elektronisk behandling* av personopplysninger. I og med at direktivet bare omfatter manuell behandling i den grad personopplysningene inngår eller skal inngå i et personregister, er det nødvendig å trekke en grense mellom manuell og (helt eller delvis) elektronisk behandling (se mer om dette i SOU 1997: 39 side 343-345).

Behandling av personopplysninger i maskinlesbar form vil klart representere en elektronisk behandling. Selve overføringen av en persons utseende eller stemme til et vanlig (analogt) lyd- eller videobånd (uten lagring) vil etter utvalgets syn ikke omfattes av direktivets begrep «elektronisk behandling». Videre antar utvalget at heller ikke fjernsynsovervåkning som bygger på digital teknikk og hvor bilde og lyd ikke lagres, men bare vises på en monitor ikke omfattes. Noe mer usikkert er det om behandling av personopplysninger som ikke finnes i maskinlesbar form, f eks bilder og lyd lagret i analogt format (f eks på ett negativ eller et vanlig lyd- eller videobånd) omfattes av direktivet. Direktivet sier uttrykkelig at lyd- og billedopptak omfattes, jf artikkel 33 og fortalen pkt 14-17, men gir lite veiledning om hvilke krav som stilles til slike opptak for at de skal omfattes. Etter utvalgets syn er det muligheten for å søke i materiale slik at enkeltpersoner enkelt kan gjenfinnes som er noe av det sentrale ved «elektronisk behandling», og som bør være avgjørende for hvorvidt noe er å anse som elektronisk behandling. På denne bakgrunn antar utvalget at direktivets regler om «elektronisk behandling» normalt ikke får anvendelse på lyd- og billedopptak som lagres analogt. Loven bør heller ikke i utgangspunktet få anvendelse på slike opptak, men enkelte av lovforslagets bestemmelser bør gis tilsvarende anvendelse for elektronisk overvåking og opptak i forbindelse med slik overvåking, se "*Fjernsynsovervåking og annen elektronisk overvåking*" i kapittel 14.

10.1.3 Offentlig og privat virksomhet

10.1.3.1 Gjeldende rett

De fleste kapitlene i personregisterloven får anvendelse på både offentlig og privat sektor, jf loven § 1 tredje ledd. Reglene i "*Personregisterloven med forskrifter*" i kapittel 5 til 8 vil som oftest bare ha betydning for privat virksomhet. Uttrykket «organ for stat eller kommune» skal tillegges samme betydning som det tilsvarende uttrykket i forvaltningsloven, jf Ot prp nr 2 (1977-78) s 69 høyre spalte. Dette innebærer at også f eks offentlige undervisnings-, forsknings-, og helseinstitusjoner omfattes av loven, selv om denne typen institusjoner ikke utøver tradisjonell forvaltningsmyndighet. Et offentlig eid selskap som driver virksomhet av privatrettslig karakter betraktes derimot ikke som et «organ for stat eller kommune», jf op cit s 69.

Selv om loven får anvendelse på både privat og offentlig virksomhet, betyr ikke det at disse likestilles i forhold til alle reglene i loven. Et eksempel på dette finnes i loven § 7 annet og tredje ledd, der den registrerte gis en videregående innsynsrett i personregistre i organ for stat eller kommune (innsynsretten er behandlet i "*Individuelle personverngarantier*" i kapittel 11 nedenfor).

10.1.3.2 Internasjonale regler

Et karakteristisk trekk ved *direktivet* er at reglene for offentlig og privat sektor i utgangspunktet er de samme. Dette har for det første sammenheng med hensynet til effektiv harmonisering over landegrensene; grensedragningen mellom privat og offentlig sektor kan variere nokså meget fra land til land, og ut i fra direktivets formål ville det være uheldig om slike forskjeller førte til et ulikt beskyttelsesnivå i de ulike landene. Den andre hovedbegrunnelsen for at direktivet i utgangspunktet likebehandler offentlig og privat sektor er at borgernes rettsbeskyttelse ikke bør avhenge av hvor opplysningene om dem behandles.

Direktivet gjelder ikke for behandlinger av personopplysninger på områder som ikke omfattes av fellesskapsretten, og bl a heller ikke behandling av personopplysninger som angår den offentlige sikkerhet, forsvar, statens sikkerhet, statens økonomiske tilstand og statens aktiviteter på det strafferettslige området (jf direktivet artikkel 3.1 og 3.2). Dette innebærer at EU- og EØS-landene står fritt til selv å bestemme utformingen av reglene på dette området. Også her må man imidlertid ta hensyn til europarådskonvensjonen, se nærmere nedenfor.

I henhold til *Europarådskonvensjonen* artikkel 3 nr 1 forplikter partene seg til å anvende konvensjonen på elektroniske persondataregistre og elektronisk databehandling av personopplysninger både i den offentlige og i den private sektor. Dette behøver ikke å innebære at reguleringen er den samme for de to sektorene, se bl a konvensjonen artikkel 9.

10.1.3.3 Utvalgets vurderinger

Utvalget går inn for at loven fremdeles bør omfatte både offentlig og privat sektor, og gir i det vesentlige sin tilslutning til departementets vurdering av de samme spørsmål i forbindelse med utarbeidelsen av personregisterloven, se Ot prp nr 2 (1977-78) s 17 – 25. Også behandling av personopplysninger i private sektor kan være av stor betydning for den enkelte. I den senere tid har det dessuten vært tendenser til at oppgaver som tradisjonelt har blitt utført av det offentlige overlates til private. Dette skjer ofte ved at private virksomheter overtar totalansvaret for f eks yting av tjenester, men også ved at det offentlige setter ut enkelte ledd i utføringen av sin virksomhet til private aktører («outsourcing»). I tillegg til at denne utviklingen kan gjøre det vanskeligere enn før å skille mellom offentlig og privat virksomhet, ville det være uheldig om en endret arbeidsfordeling førte til mindre betryggende regulering og behandling av personopplysninger. Denne utviklingen er derfor slik utvalget ser det, ytterligere ett argument for at både offentlig og privat virksomhet bør reguleres av loven, og for at beskyttelsesnivået bør være det samme i offentlig og privat sektor.

At beskyttelsesnivået bør være det samme i offentlig og privat sektor betyr ikke nødvendigvis at regelverket på alle områder må være identisk. Utformingen av regler om behandling av personopplysninger må ses i sammenheng med annen rettslig regulering av henholdsvis offentlig og privat sektor. Mens forvaltningsorganer som regel er underlagt en rekke lover som oppstiller krav til saksbehandlingen og andre rettssikkerhetsgarantier (jf for eksempel forvaltningsloven), står private rettssubjekter oftest mye friere. Det er flere grunner til dette skillet. Dels har utøvelse av offentlig myndighet tradisjonelt blitt ansett som mer inngripende enn beslutninger tatt av private rettssubjekter, slik at det av den grunn er særskilt viktig å gi borgerne rettssikkerhetsgarantier. Videre er det som oftest opp til borgerne selv om de vil ha kontakt med private rettssubjekter, mens det ikke sjelden er en plikt å ha kontakt med offentlige myndighetsorganer. Endelig vil det ved utformingen av regler for privat sektor gjerne være en viktig målsetting å sikre konkurransedyk-

tighet i forhold til utenlandske bedrifter, og ellers unngå å legge hindringer i veien for nyetableringer eller omstillinger som av bedriftsøkonomiske grunner fremstår som ønskelige.

I enkelte sammenhenger har utvalget blant annet på bakgrunn av disse grunnleggende forskjellene vurdert om det er hensiktsmessig å gi forskjellige regler for privat og offentlig virksomhet. Hovedkonklusjonen er at det ikke er grunn til å trekke et slikt skille.

10.1.3.4 Særlig om unntak for rent personlige aktiviteter

Personregisterloven gjelder ikke for rent personlige aktiviteter. Dette følger av at loven bare får anvendelse på «privat næringsvirksomhet, foreninger eller skiftelser», se personregisterloven § 1 tredje ledd. For at en person skal anses som næringsdrivende, må virksomheten være av økonomisk karakter og ha et visst omfang.

EF-direktivet har også et unntak for denne type bruk av personopplysninger, jf artikkel 3 nr 2 annet strekpunkt:

«Dette direktiv gjelder ikke for sådan behandling af personopplysninger som foretages af en fysisk person med henblikk på udøvelse af rent personlige eller familiemæssige aktiviteter.»

Utvalget går inn for å opprettholde rettstilstanden på dette punktet, og forslår at denne typen behandling av opplysninger heller ikke for fremtiden bør omfattes av loven. Utvalget mener at dette bør fremgå uttrykkelig av loven.

10.1.4 Sensitive personopplysninger

10.1.4.1 Gjeldende rett

Uttrykket «sensitive personopplysninger» er en hensiktsmessig fellesnevner for særlig følsomme personopplysninger som bør undergis et særskilt vern. I personregisterloven § 6 (saklighetskrav) og § 9 (konsesjonsplikt) er følgende opplysninger undergitt særskilt regulering:

1. opplysninger om rase, eller politisk eller religiøs oppfatning
2. opplysninger om at en person har vært mistenkt, tiltalt eller dømt for straffbare forhold
3. opplysninger om helseforhold eller bruk av rusmidler
4. opplysninger om seksuelle forhold, eller
5. andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordning mellom ektefeller og forsørgelsesbyrde.»

10.1.4.2 Internasjonale regler

Direktivet artikkel 8 forbyr i utgangspunktet all behandling av personopplysninger om rasemessig eller etnisk bakgrunn, politiske, religiøs eller filosofisk overbevisning, medlemskap i fagforening og opplysninger om helse eller seksuelle forhold.

I henhold til nr 2 bokstav a) kan behandling av personopplysninger likevel finnes sted hvis den registrerte samtykker i dette. I nr 2 bokstav b) tillates behandling av slike opplysninger dersom dette er nødvendig for å overholde arbeidsrettslige forpliktelser, mens bokstav c) åpner for behandling av sensitive personopplysninger der dette er nødvendig for å beskytte noens vesentlige interesser og vedkommende selv ikke er i stand til å samtykke i behandlingen. Bokstav d) gjør det mulig

for visse typer sammenslutninger å behandle sensitive personopplysninger som ledd i sammenslutningens virksomhet og på visse nærmere vilkår. Endelig heter det i e) at sensitive personopplysninger kan behandles dersom de gjøres allment tilgjengelig av de registrerte eller dersom behandlingen er nødvendig for at rettskrav kan fastsettes, gjøres gjeldende eller forsvares.

I nr 3 heter det at begrensningene i adgangen til å behandle sensitive personopplysninger ikke gjelder dersom behandlingen av opplysningene er nødvendig for å gjennomføre enkelte helsetjenester. Det forutsettes imidlertid at den som utfører helsetjenestene har taushetsplikt.

I *Europarådskonvensjonen* artikkel 6 heter det følgende om «særkatogrier av opplysninger»:

«Personopplysninger som åpenbarer rasemessig opprinnelse, politiske oppfatninger samt religiøs eller annen tro, så vel som personopplysninger vedrørende helse eller seksualliv, kan ikke behandles elektronisk med mindre intern lovgivning gir tilstrekkelig vern. Det samme skal gjelde for personopplysninger som gjelder domfellelser for straffbare handlinger.»

Hvor mye som skal til før vernet er «tilstrekkelig» i konvensjonens forstand, overlates til partenes skjønn.

10.1.4.3 Utvalgets vurderinger

Som det fremgår foran, favner begrepet «personopplysninger» vidt. Hvor sterkt personverninteressene (se "*Hva er personvern?*" i kapittel 3) gjør seg gjeldende, vil imidlertid variere sterkt, blant annet avhengig av hvor følsomme opplysningene er, og hva de skal brukes til. I relasjon til en del bestemmelser gjør direktivet det nødvendig å undergi spesielt følsomme personopplysninger særskilt lovregulering, og utvalgets forslag er i tråd med dette. Den nærmere omtalen av de ulike kategoriene av opplysninger som regnes som sensitive, og hvordan den nærmere implementeringen bør finne sted, følger i merknadene til § 2 nr 8. Utvalget peker allerede her på at lovforslagets oppregning i tråd med direktivet skiller seg noe fra oppregningen som personregisterloven i dag inneholder; blant annet regner direktivet opplysninger om fagforeningstilhørighet som sensitive, mens opplysninger om familieforhold ikke er nevnt. Endringene er imidlertid ikke ment å innebære noen endring av rettstilstanden (bortsett fra tilføyelsen av opplysninger om fagforeningstilhørighet), se merknadene til lovforslaget § 2 nr 8.

10.2 LOVENS GEOGRAFISKE VIRKEOMRÅDE

10.2.1 Gjeldende rett

Personregisterloven har ingen bestemmelse om lovens geografiske virkeområde og spørsmålet er heller ikke drøftet i lovens forarbeider. Spørsmålet om lovens geografiske virkeområde må derfor avgjøres på annet grunnlag, herunder alminnelige interlegale prinsipper.

Et sikkert utgangspunkt er at loven gjelder for personregistre og annen bruk av personopplysninger i visse typer virksomheter som drives fra fastlandsnorge. Det antas at loven også gjelder på norske skip og på anlegg og innretninger på kontinentalsokkelen, jf Lovavdelingens uttalelser 298/81 E og 2115/83 E. Loven antas imidlertid ikke å få anvendelse på Svalbard og Jan Mayen, jf lov 17 juli 1925 nr 11 om Svalbard § 2 og lov 27 februar 1930 nr 2 om Jan Mayen § 2.

Loven gjelder som hovedregel ikke for personregistre i utlandet selv om opplysningene i registrene kan knyttes til norske personer. Det foreligger derimot

meldeplikt for den som vil overføre personopplysninger til utlandet når formålet med innføringen er å innføre opplysningene i et register, jf personregisterloven § 36 og forskrift 21 desember 1979 § 8-1. Overføringen skal meldes i god tid før overføringen finner sted og Datatilsynet kan nekte eller sette vilkår for overføringen. Samme regler gjelder for overføring av hele registre til utlandet.

10.2.2 EF-direktivet

Direktivet artikkel 4 har bestemmelser om hvilket lands lovgivning som skal anvendes på behandling av personopplysninger, og vil ha betydning for norsk lovs anvendelse når den behandlingsansvarlige er etablert i utlandet.

Hovedregelen er at det lands lov skal anvendes hvor den behandlingsansvarlige er etablert. Hvis den behandlingsansvarlige er etablert i flere land, f eks ved datterselskaper eller filialer, vil opplysninger som kan knyttes til det enkelte etableringssted reguleres av det lands lov hvor etableringsstedet er.

Hvis den behandlingsansvarlige ikke har etableringssted innen EØS-området, men benytter hjelpemidler som er plassert innenfor dette området, skal det lands lov gjelde hvor dette utstyret er plassert, med mindre hjelpemidlene bare benyttes til transitt.

Som det fremgår ovenfor er hovedregelen at det er den behandlingsansvarliges etableringssted som er avgjørende for valg av hvilket lands lovgivning som skal anvendes på all behandling av personopplysninger som den behandlingsansvarlige foretar, uavhengig av hvor behandlingen – herunder innsamlingen av opplysningene – faktisk finner sted. Norsk lov vil dermed ikke kunne anvendes på innsamling av opplysninger i Norge dersom den behandlingsansvarlige er etablert i en annen EØS-stat. Dette antas ikke å avvike i særlig grad fra gjeldende rett. Datatilsynet vil imidlertid ikke lenger ha adgang til å stille vilkår for overføring av personopplysninger til andre EØS-stater. Derimot vil tilsynet ha kontrollmyndighet over all behandling av personopplysninger som foregår i Norge, f eks innsamling av opplysninger, jf direktivet artikkel 28.

10.2.3 Utvalgets vurderinger

Utvalget legger EF-direktivets regler til grunn og foreslår at loven skal gjelde for behandling av personopplysninger når den behandlingsansvarlige er etablert i Norge, herunder på norske skip eller på anlegg eller innretning på kontinental-sokkelen. Hvis den behandlingsansvarlige har hovedsete i en annen EØS-stat og datterselskap eller filial i Norge, vil norsk lov gjelde for all behandling av personopplysninger knyttet til den norske filialens/datterselskapets virksomhet. Loven vil gjelde for all behandling av personopplysninger som kan knyttes til en behandlingsansvarlig etablert i Norge, også når opplysningene kun gjelder personer i utlandet.

Utvalget foreslår at norsk lov skal gjelde når en behandlingsansvarlig som er etablert utenfor EØS-området benytter hjelpemidler plassert i Norge ved behandlingen av personopplysningene, med mindre disse hjelpemidlene bare benyttes til å transportere personopplysningene via Norge. Utvalget vil presisere at uttrykket «hjelpemidler» omfatter alt slags utstyr, både elektronisk og ikke-elektronisk. Utvalget legger til grunn at det må benyttes hjelpemidler til praktisk talt all behandling av personopplysninger, slik at loven vil gjelde for all behandling av personopplysninger som finner sted i Norge når den behandlingsansvarlige er etablert utenfor en EØS-stat med mindre Norge bare er transitt land.

Jan Mayen er en del av Norge og hører dermed under EØS-området. Utvalget foreslår derfor at loven også gjøres gjeldende for Jan Mayen.

Svalbard er derimot ikke en del av EØS-området, og blir å anse som tredjeland i forhold til direktivet artikkel 25 og 26. Hovedregelen er at personopplysninger bare kan overføres til tredjeland når dette landet sikrer en tilstrekkelig beskyttelse. For å sikre en fri utveksling av personopplysninger mellom fastlandsnorge og Svalbard foreslår utvalget at loven også skal gjelde for Svalbard. Utvalget vil dessuten bemerke at også andre hensyn tilsier at loven skal gjelde for Svalbard. Det synes uheldig at en virksomhet etablert på Svalbard skal kunne behandle personopplysninger uten å være underlagt regulering.

KAPITTEL11

Individuelle personverngarantier**11.1 ALLMENT OM INDIVIDUELLE PERSONVERNGARANTIER**

Med «personverngarantier» mener utvalget tiltak som ivaretar personvernet. Enkelte slike garantier er «kollektive» fordi de utøves av myndigheter og virksomheter på vegne av mange enkeltindivider. Datatilsynets virksomhet, herunder tilsynets myndighetsutøvelse og informasjonsvirksomhet knyttet til melde- og konsesjonsplikten er eksempler på slike kollektive personverngarantier.

Personvernlovgivningen inneholder også bestemmelser som gir rettigheter for den enkelte registrerte. Dette er rettigheter som skal sette den enkelte i stand til selv å ivareta sine interesser. Bestemmelser som gir rett til innsyn, sletting og retting er eksempler på slike individuelle personverngarantier. Det er opp til den enkelte å benytte garantiene og de får primært virkning for vedkommende person. Slike bestemmelser innebærer imidlertid også en plikt for den behandlingsansvarlige til å etterkomme krav fra den registrerte, eventuelt igangsette visse tiltak selv uten noe krav fra den registrerte (for eksempel bestemmelsene om varslingsplikt, se 11.2.6).

Individuelle personverngarantier forutsetter ofte godt orienterte og aktive borgere. Trolig vil kun en forholdsvis liten del av befolkningen benytte disse garantiene. I tiden framover vil mengden av personopplysninger som behandles sannsynligvis øke kraftig. I tillegg er det grunn til å anta at utvekslingen av personinformasjon mellom flere aktører vil øke i omfang og frekvens, samtidig som kompleksiteten i persondatabehandlingene øker, se 4.2 og 4.3. På denne bakgrunn er det rimelig å anta at det i tiden framover vil bli en enda mer krevende oppgave for den enkelte å vareta personvernet gjennom de individuelle garantiene.

Dersom de individuelle garantiene skal ha mer enn symbolfunksjoner, er det imidlertid nødvendig å legge forholdene bedre til rette for at garantiene skal være effektive hjelpemidler for folk flest. Noe kan vinnes ved en bedre praktisk og teknologisk tilrettelegging for effektiv bruk av de eksisterende personverngarantiene. Personverndirektivet foranlediger i tillegg flere individuelle garantier.

I dette kapitlet behandles ulike regler som skal sikre den enkeltes rett til innsyn, herunder den behandlingsansvarliges selvstendige varslingsplikt, den enkeltes rett til å motsette seg visse typer behandlinger og behandlingsansvarliges plikt til å rette, slette og supplere. Avslutningsvis behandles noen fellesspørsmål om tidsfrister og kostnader.

11.2 DEN ENKELTES RETT TIL INNSYN**11.2.1 Oversikt**

Personregisterloven, personverndirektivet og europarådskonvensjonen har en rekke bestemmelser som gir den enkelte mulighet for kunnskap om persondatabehandling. I det følgende skal innsynsspørsmålene behandles etter følgende inndeling:

- *Plikt for tilsynsmyndigheten* til å føre en allment tilgjengelig fortegnelse over melde- og konsesjonspliktige persondatabehandling.
- *Plikt for den behandlingsansvarlige* som ikke er undergitt melde- eller konsesjonsplikt til å gjøre informasjon om persondatabehandling allment tilgjengelig.
- *Rett for den enkelte* til å få innsyn i generell informasjon om formål, opplysn-

- ingstyper, kilde for opplysningene m m.
- *Rett for den enkelte* til å få innsyn i innholdet av konkrete behandlinger som gjelder en selv.
 - *Plikt for de behandlingsansvarlige* til å informere den enkelte registrerte person om visse generelle forhold knyttet til behandlingen («den behandlingsansvarliges opplysningsplikt»).

Rett for den enkelte til innsyn i behandlingsregler («logikken») hører også naturlig inn under innsynsreglene som behandles i dette avsnittet (11.2). Denne innsynsretten er likevel skilt ut til særskilt behandling under "*Innsyn i behandlingsregler («logikken»)*" i avsnitt 11.4 på grunn av sammenhengen med direktivet artikkel 15 som behandles i "*Den enkeltes rett til å motsette seg visse typer persondatabehandling*" i avsnitt 11.3.

Bestemmelsene om innsyn er direkte og/eller indirekte knyttet opp til omfanget og innholdet av en melde- og konsesjonsordningen, se "*Regulering og kontroll*" i kapittel 12. Spørsmålet om utgifter knyttet til innsynet drøftes under 11.6.2.

11.2.2 Plikt for tilsynsmyndigheten til å føre allment tilgjengelig fortegnelse over meldepliktige og konsesjonspliktige persondatabehandlinger

11.2.2.1 Personregisterloven § 4

Personregisterloven § 4 etablerer en plikt for Datatilsynet til å «føre en systematisk fortegnelse over personregistre som er gitt konsesjon etter § 9.» Fortegnelsen skal etter loven være tilgjengelig for alle. Datatilsynet har ikke prioritert føringen av et slikt register, og det foreligger i dag ingen slik fortegnelse som er lett tilgjengelig. Dette skyldes primært det meget høye antall konsesjoner som har vært gitt siden loven trådte i kraft. Antallet årlige henvendelser om innsyn i § 4-registeret er mindre enn én. Interesserte kan kreve innsyn i bestemte konsesjonssaker ved å ta direkte kontakt med Datatilsynet, jf offentlighetsloven § 2 annet ledd.

11.2.2.2 Personverndirektivet artikkel 21 nr 2

Personverndirektivet fastsetter at tilsynsmyndighetene skal føre et register over meldepliktige behandlinger etter bestemmelser gitt i medhold av artikkel 18. Registeret skal minst inneholde de samme opplysninger som meldinger om persondatabehandlinger minst skal inneholde. Det kan gjøres unntak for behandlinger som kun har til formål å føre et register, dersom dette registeret er offentlig eller tilgjengelig for alle med en legitim interesse i innsyn.

11.2.2.3 Europarådskonvensjonen

Europarådskonvensjonen artikkel 8 a synes å forutsette en tilsvarende fortegnelse som fastsatt i direktivet, men etablerer ingen klar plikt til å opprette et slikt register.

11.2.2.4 Utvalgets vurderinger

Utvalget foreslår en ordning der melde- og konsesjonsplikt må ses i sammenheng, se "*Regulering og kontroll*" i kapittel 12. En sentral fortegnelse bør inneholde opplysninger om både konsesjons- og meldepliktige persondatabehandlinger.

Det er ingen automatikk i at en oversikt over behandlinger skal bli et nyttig virkemiddel for ivaretagelsen av personvernet. For det første kreves det at fortegnelsen inneholder opplysninger om persondatabehandlinger som det er viktig for

den enkelte å kjenne til. Dette kravet ivaretas gjennom avgrensningen av konsesjons- og meldepliktordningen, se "*Utvalgets vurderinger*" i avsnitt 12.5. Det er også en forutsetning at en oversikt over konsesjons- og meldepliktige behandlinger blir lett tilgjengelige for folk flest. Dessuten må fortegnelsen være systematisk ordnet, ha høy kvalitet, gode søkefunksjoner og for øvrig være enkel å bruke. Under de nevnte forutsetninger kan en fortegnelse over persondatabelandlinger være et nyttig hjelpemiddel for varetakelse av personvern og åpenhet i samfunnet.

For det første kan en fortegnelse over visse persondatabelandlinger være nyttig for den som aktivt ønsker å utøve sin rett til innsyn, retting og sletting av personopplysninger. Utvalget antar imidlertid at slik utøvelse av innsynsrett m m normalt vil være foranlediget av konkrete hendelser, og at enkeltpersoner sjelden vil benytte en fortegnelse over persondatabelandlinger for deretter å henvende seg til den behandlingsansvarlige. Det vil også åpenbart ha betydning hvor tilgjengelig fortegnelsen er – tilgang til fortegnelsen via f eks Internett eller et annet elektronisk medium vil øke sannsynligheten for bruk betraktelig.

En allment tilgjengelig fortegnelse over persondatabelandlinger vil i tillegg gi den enkelte en bedre oversikt og kontroll over de persondatabelandlinger som foretas, og på den måten varetta den enkeltes interesse i diskresjon, se "*Interesseteorien*" i avsnitt 3.4.2.

Fortegnelsen vil for det tredje bidra til offentlighet og åpenhet om offentlig og privat sektor. De saksforhold en fortegnelse vil gi opplysning om, vil for offentlig sektors vedkommende også kunne forekomme i saksdokumenter som er offentlige i henhold til offentlighetsloven § 2 annet ledd. En fortegnelse over persondatabelandlinger gjør imidlertid at opplysningene samles og gjøres langt lettere tilgjengelig enn uten en slik oversikt. En oversikt som f eks omfatter sentrale persondatabelandlinger innen trygdeataten, vil kunne gi ny innsikt i trygdeataten's behandling av personopplysninger.

En fortegnelse over viktige persondatabelandlinger vil også kunne være til nytte for Datatilsynets kontroll- og informasjonsvirksomhet. Dette er imidlertid nært knyttet til spørsmålet om omfang og innretning av melde- og konsesjonspliktordningene, se "*Utvalgets vurderinger*" i avsnitt 12.5.

Art 21 nr 2 i direktivet forutsetter at *tilsynsmyndigheten* skal «føre registeret». Utvalget legger til grunn at det må være tilstrekkelig at Datatilsynet har full bestemmelsesrett over fortegnelsen, og at rene driftsoppgaver vil kunne utføres av andre.

Det er mulig at visse persondatabelandlinger, f eks av beredskapshensyn, ikke bør med i fortegnelsen. Det bør derfor være en mulighet for Kongen til å gjøre unntak for slike behandlinger.

11.2.3 Plikt for behandlingsansvarlige som ikke er undergitt melde- eller konsesjonsplikt til å gjøre informasjon om persondatabelandlinger allment tilgjengelig

11.2.3.1 Personverndirektivet artikkel 21 nr 3

En del typer behandlinger av personopplysninger er ikke undergitt meldeplikt etter artikkel 18, og opplysninger om disse vil derfor heller ikke bli samlet i fortegnelsen hos tilsynsmyndigheten. For å sikre offentlig tilgjengelighet til informasjon om disse, fastsetter artikkel 21 nr 3 at registeransvarlige (eller annen myndighet) plikter å stille opplysninger som nevnt i artikkel 19 bokstav a-e til rådighet for enhver som anmoder om det.

Personregisterloven og Europarådskonvensjonen inneholder ikke lignende bestemmelser.

11.2.3.2 Utvalgets vurderinger

EF-direktivet krever at også de ansvarlige for *ikke* melde- eller konsesjonspliktige behandlinger må i hovedsak ha tilsvarende oversikt som den direktivet krever at de meldepliktige skal ha. Forskjellen mellom meldepliktige og ikke meldepliktige blir primært kravet om innsending av opplysningene til tilsynsmyndigheten.

Fastsattelsen av hvilke behandlinger som skal være meldepliktige og hvilke som skal være frie, skjer på grunnlag av antagelser om hvilke behandlingstyper som har størst personvernmessig betydning. Det vil imidlertid alltid være usikkerhet knyttet til denne grensen. Derfor bør ikke skillet mellom meldepliktige og ikke meldepliktige behandlinger på dramatisk måte få betydning for graden av innsyn for den enkelte. Med bestemmelsen i artikkel 21 nr 3 sikrer man behovet for innsyn samtidig som man unngår unødvendig kostnadskrevenne ordninger.

Utvalget antar at den plikt som artikkel 21 nr 3 innebærer, ikke vil medføre noe særlig merarbeid for de behandlingsansvarlige. De aktuelle behandlingstypene er så sentrale at den behandlingsansvarlige lett kan fremskaffe disse, se merknadene til lovforslaget § 16.

11.2.4 Retten til innsyn i generell informasjon om behandlingen (formål og opplysningstyper mm)

11.2.4.1 Gjeldende rett

Personregisterloven § 7 tredje ledd gir en rett for alle til å få vite hvilke *typer* opplysninger som er tatt inn i registeret, både elektronisk lagrede og manuelle. Bestemmelsen gjelder bare for offentlige registre. Denne retten har man uansett om man selv er registrert i registeret eller ikke. Retten kan for så vidt sies å være av samme karakter som retten etter offentlighetsloven til å bli kjent med dokumenter. Etter fjerde ledd kan Kongen ved forskrift bestemme at retten til å vite hvilke typer opplysninger som er registrert, skal gjelde også overfor private registre. Denne forskriftshjemmelen er ikke benyttet.

Det kan også hevdes å eksistere en rett til å få opplysninger om formålet med et konsesjonspliktig register, hvem som er registeransvarlig og forøvrig om hvilke regler som gjelder for registeret og som er fastsatt i henhold til personregisterloven § 11 (slik direktivet i visse tilfeller gir krav på, se 11.2.4.2). Innsynsrett i slike generelle forhold kommer imidlertid ikke klart til uttrykk i lovteksten, i det en må sammenholde personregisterloven § 4 om innsyn i fortegnelsen over konsesjonspliktige registre med §§ 6 og 11. Denne delen av innsynsretten har dessuten levet under vanskelige kår, fordi det ikke har eksistert noe lett tilgjengelig ajourført register i henhold til personregisterloven § 4.

11.2.4.2 Internasjonale regler

Direktivet artikkel 12 gir den registrerte en rett til å få opplyst hos den behandlingssansvarlige om det behandles personopplysninger om en selv, om formålet med behandlingen, hvilke opplysningstyper som brukes, kilden for og mottakerne av opplysningene, samt i visse tilfeller «logikken» bak visse behandlinger («logikk-innsynet» behandles i fremstillingen under 11.4). Art 13 åpner for å gjøre en rekke unntak fra denne innsynsretten, se 11.2.5.

Retten etter artikkel 12 til å få denne typen generell informasjon om behandling fra den behandlingsansvarlige gjelder kun for de som selv er registrert hos vedkommende. Dersom man ikke selv er registrert, kan man imidlertid for de meldepliktige eller konsesjonspliktige behandlingene kreve innsyn i de samme

opplysningene hos tilsynsmyndigheten, jf direktivet artikkel 21 nr 2. For ikke meldepliktige behandlinger skal opplysningene være offentlig tilgjengelig hos den behandlingsansvarlige, jf artikkel 21 nr 3.

Etter *Europarådskonvensjonen* artikkel 8 a har alle rett til å få opplyst om det eksisterer et edb-basert register, hvilket formål registeret har og hvem som er registeransvarlig. Opplysningene skal formidles på en forståelig måte, og innsynet skal kunne skje uten uforholdsmessig forsinkelse og kostnad. Konvensjonen inneholder i artikkel 9 unntaksbestemmelser som ligner unntaksbestemmelsene i EF-direktivet artikkel 13.

11.2.4.3 Utvalgets vurderinger

Utvalget ser enhver persons rett til generell informasjon i behandlingen av personopplysninger som et viktig og nødvendig supplement til den enkeltes rett til innsyn i personopplysninger om dem selv. Denne innsynsretten er langt på vei en forutsetning for en hensiktsmessig praktisering av innsyn i opplysninger om den enkelte, og vil bli stadig viktigere i årene framover etterhvert som omfang, kompleksitet og sammenvevingen av ulike persondatabelandlinger tiltar.

Etter utvalgets mening er det av avgjørende betydning for personvernet at innsynsretten etter personregisterloven § 7 videreføres og styrkes. I en ny lov bør således innsynsretten utvides til også å omfatte rett til innsyn i opplysningstyper og formål.

Utvalget har vurdert om det bare er de som ikke er melde- eller konsesjonspliktige som skal ha plikt til å gi innsyn til alle som ber om det i disse generelle opplysningene, eller om også de som er melde- eller konsesjonspliktige skal gi slikt innsyn. I følge direktivet er det bare de som ikke er melde- eller konsesjonspliktige som skal ha slik plikt (for de melde- og konsesjonspliktige behandlingene kan innsyn kreves hos tilsynsmyndigheten, jf artikkel 21 nr 2).

Å gi innsyn i generell informasjon til alle som ber om det vil representere et visst merarbeid for den behandlingsansvarlige. Utvalget antar imidlertid at omfanget av merarbeidet vil være relativt beskjedent i og med at de aktuelle opplysningstypene er så sentrale, og forutsatt generelle i formen, at den behandlingsansvarlige lett må kunne fremskaffe disse. Dersom den som ønsker innsyn må henvende seg ulike steder alt etter om behandlingene er meldepliktig eller ikke, vil dette gi vedkommende en dårlig oversikt over de behandlingene som foretas. Utvalget foreslår at plikten til å gi generell informasjon om en persondatabelandling i loven pålegges både den behandlingsansvarlige og Datatilsynet.

11.2.5 Retten til innsyn i opplysninger om en selv

11.2.5.1 Personregisterloven § 7

Den sentrale bestemmelsen om innsyn er i dag personregisterloven § 7 første ledd. Bestemmelsen gir i utgangspunktet den enkelte rett til innsyn i opplysninger om dem selv når opplysningen lagres eller bearbeides ved hjelp av elektroniske hjelpemidler. Uttrykket «elektroniske hjelpemidler» må forstås vidt, og omfatter i utgangspunktet alle hjelpemidler for digital behandling av skrifttegn (tekst), bilde og lyd.

Loven gir etter sin ordlyd bare innsynsrett i opplysninger om den som krever innsynet. Loven løser ikke spørsmålet om foreldres innsyn i opplysninger om deres mindreårige barn, men Datatilsynet har i sin praksis antatt at foreldre har en slik innsynsrett.

Loven gjør unntak fra innsynsretten når det dreier seg om registre som bare skal anvendes til utarbeidelse av statistisk materiale, forskning og generelle planer. I slike tilfelle har ikke den enkelte et *krav* på å få innsyn, men bestemmelsen oppstiller heller ikke noe forbud. Den som rår over opplysningene kan således praktisere et *mer-innsyn* (se 11.4.4) for så vidt det ikke følger av andre bestemmelser at opplysningen ikke skal gis videre. Unntakene for statistikk, forskning og generelle planer gjelder selv om dette til tider vil kunne omfatte meget sensitivt materiale. Unntakene må bli sett på bakgrunn av at disse behandlingene ofte gjelder store datamengder, og at det ikke er opplysninger om enkeltmennesker som står sentralt, men det *helhetsbildet* som det totale materialet danner. Vanligvis vil slik behandling av personopplysninger heller ikke direkte berøre de mennesker opplysningene omhandler, bli fordi opplysningene ikke benyttes til å treffe beslutninger.

Innsynsretten gjelder ikke opplysninger «som det må anses utilrådelig at vedkommende får kjennskap til, av hensyn til personens helse eller forholdet til andre personer som står vedkommende nær.» Bestemmelsen er identisk med første del av forvaltningsloven § 19 første ledd, bokstav c, som også inneholder en betinget rett til å kreve at partens *representant* skal få tilgang til opplysningene. En slik rett kan ikke antas å gjelde etter personregisterloven.

Personregisterloven § 7 annet ledd gir utvidet innsyn innen offentlig sektor, idet også opplysninger som behandles *manuelt* er gjenstand for innsynsrett. Henvisningen til forvaltningsloven § 18 i andre punktum innebærer at forvaltningslovens regler om unntak for innsyn i *interne dokumenter* går foran hovedregelen om innsynsrett. Denne henvisningen innebærer imidlertid også en henvisning til bestemmelsen i § 18 tredje ledd som gir rett til innsyn i visse *faktiske opplysninger* i interne dokumenter. Når unntakene fra partsinnsynsretten i forvaltningsloven § 19 ikke er nevnt i personregisterloven § 7, er det trolig fordi flere av de opplysningstyper som der er omhandlet bare i liten grad omhandler personopplysninger om den person som krever innsynet (med unntak av forvaltningsloven § 19 første ledd bokstav c).

I tillegg til personregisterlovens bestemmelser er innsyn regulert i Datatilsynets konsesjoner. Med hjemmel i personregisterloven § 11 har Datatilsynet i enkelte tilfelle fastsatt bestemmelser om innsyn i registre som går ut over bestemmelsen i § 7. I konsesjonene kan det også være gjort konkrete unntak fra innsynsreglene med hjemmel i personregisterloven § 7 femte ledd.

I fjerde ledd gis Kongen fullmakt til å fastsette utvidet anvendelse av innsynsreglene i annet og tredje ledd i forhold til privat sektor. Utvidelsene kan skje områdevis eller for særlige registre. Slik utvidelse er fastsatt i personregisterforskriften (21 desember 1979) § 1-5, som gir innsynsrett i manuelle personalregistre i privat sektor.

11.2.5.2 EF-direktivet artikkel 12

Artikkel 12 gir på samme måte som personregisterloven § 7 den enkelte en rett til å kreve innsyn i hvilke opplysninger som blir behandlet om han eller henne. Direktivet avviker fra personregisterloven § 7 ved at den likestiller innsyn i opplysninger i manuelle personregistre og opplysninger som behandles elektronisk. Informasjon om behandlingene skal gis på en lett forståelig måte. Innsynsretten skal kunne utøves «frit og uhindret, med rimelige mellomrum og uten større ventetid eller større udgifter».

Etter artikkel 13 kan det i lov eller i medhold av lov gjøres en rekke unntak fra innsynsretten slik den er beskrevet i artikkel 12 når slike innskrenkninger er nødvendige av hensyn til statens sikkerhet, forsvaret, den offentlige sikkerhet, til beskyttelse av vesentlige økonomiske eller finansielle interesser eller for varetakelse av

bestemte kontroll-, tilsyns- og reguleringsoppgaver. Det kan også gjøres unntak når det er nødvendig for forebygging, etterforskning, avsløring og rettsforfølging i straffesaker og ved brudd på visse etiske regler. Artikkel 13 inneholder også en hjemmel for å gjøre unntak når det er nødvendig for beskyttelsen av den registrertes interesser eller for å beskytte andres rettigheter eller friheter.

Etter artikkel 13 nr 2 kan det i eller i medhold av lov også gjøres innskrenkninger i innsynsretten dersom opplysningene «udelukkende behandles med vitenskapelig forskning for øje eller kun oppbevares i form af personopplysninger i det tidsrum, som kræves for at udarbejde statistikker.» Forutsetningen er at opplysningene ikke anvendes til å treffe tiltak eller avgjørelser mot bestemte personer *og* at det ikke er risiko for krenkelse av privatlivets fred. Denne adgangen til unntak er snevrere enn etter ordlyden i personregisterloven § 7 første ledd annet punktum som generelt unntar personopplysninger som bare benyttes i statistikk, forskning og generelle planer.

11.2.5.3 Europarådskonvensjonen artikkel 8 b

Etter konvensjonen artikkel 8 b gis det rett til innsyn i opplysninger om den enkelte. Opplysningene skal formidles på en forståelig måte, og innsynet skal kunne skje uten uforholdsmessig forsinkelse og kostnad.

Konvensjonen inneholder i artikkel 9 unntaksbestemmelser som ligner unntaksbestemmelsene i EF-direktivet artikkel 13. Konvensjonen krever at unntaket «[...] er et nødvendig tiltak i et demokratisk samfunn [...]» og unntar statistikk og forskning når dette åpenbart ikke setter personvernet i fare. Også denne unntakshjemmelen er snevrere enn etter personregisterloven § 7, men videre enn etter personverndirektivet artikkel 13 nr 2, som ikke stiller krav om at faren skal være åpenbar.

11.2.5.4 Utvalgets vurderinger

11.2.5.4.1 Oversikt

Også på dette området ser utvalget det som påkrevet å supplere og presisere retten til innsyn. Blant annet går utvalget inn for å likestille retten til innsyn i manuelle og elektronisk lagrede opplysninger (11.2.5.4.2), dernest diskuteres mulige unntak for innsynsrett i interne dokumenter (11.2.5.4.3), ut i fra hensynet til den registrerte selv (11.2.5.4.4) og for statistikk, forskning og generelle planer (11.2.5.4.5). Avslutningsvis sies noe om innsynsrett for umyndige (11.2.5.4.6).

11.2.5.4.2 Utvidet innsyn i forhold til private

Spørsmålet er om innsynsretten skal utvides til også å gjelde for manuelle personregistre i private virksomheter. Dagens lov gir like regler i forhold til innsyn i enkeltopplysninger i edb-registre i offentlig og privat sektor. Etter utvalgets mening bør en i tråd med personverndirektivet likestille innsynsrettighetene i offentlig og privat sektor. Dette innebærer samme innsynsrett enten det gjelder opplysninger på papir eller i maskinlesbar form.

Utvalget antar at en slik utvidelse vil ha beskjedne praktiske konsekvenser. Det finnes allerede i dag eksempler på opplysningsplikter/innsynsretter innen privat sektor i henhold til særlovgivning, se f.eks forsikringsavtaleloven § 17-2 som gir forsikringstakeren rett til å kreve utskrift av livsforsikringsregisteret. I tillegg antar utvalget at det i henhold til kontrakt, kutymen og praksis innen flere bransjer gis innsyn i opplysninger om kunden selv. En bestemmelse om innsynsrett i private man-

uelle personregistre vil derfor dels innebære en utvidelse og dels en bekreftelse av eksisterende innsynspraksis.

Innsyn i private manuelle registre vil bli berøre virksomheter som ikke forestår maskinell behandling men i stedet manuelt håndterer forholdsvis begrensede mengder personopplysninger. For disse vil belastningen som følge av en utvidet innsynsrett trolig bli liten. En utvidelse til private manuelle registre vil imidlertid også føre til at den enkelte kan kontrollere at opplysninger slik de har innkommet til en behandlingsansvarlig i privat sektor er de samme som de opplysningene som er lagt til grunn ved en etterfølgende edb-behandling. Slikt innsyn er i utgangspunktet aktuelt for mange store virksomheter og for store informasjonsmengder, men i praksis vil trolig kun et fåtall benytte seg av en rett til innsyn i saksmapper m v. Dersom det faktisk foreligger strid eller usikkerhet om opplysninger i papirdokumenter, kan det uansett være urimelig å nekte et innsyn som kan bidra til en avklaring av spørsmålet. Særlig gjelder dette dersom opplysningene skal benyttes til å treffe beslutninger som får rettslige eller viktige konsekvenser for den enkelte.

11.2.5.4.3 Unntak for innsyn i interne dokumenter

Innsynsretten i offentlige manuelle personregistre gjelder ikke for interne dokumenter som kan unntas fra innsyn, jf henvisningen i § 7 annet ledd til forvaltningsloven § 18. En slik begrensning gjelder ikke for elektroniske registre. Begrunnelsen for dette bygger på en forutsetning om at det er forskjellige typer opplysninger som lagres elektronisk og som oppbevares manuelt i et saksomslag, på utfylte skjemaer o l, jf Ot prp nr 2 (1977-78) side 74 høyre spalte:

«Når opplysninger blir lagret eller bearbeidet ved bruk av edb, vil man i praksis kunne sondre mellom de vanligvis kortfattede opplysninger som finnes på bånd, skiver, m v, og de ofte mer omfattende opplysninger som ligger i et saksomslag, på utfylte skjemaer o l.»

Etter utvalgets syn bør unntaket for enkelte interne dokumenter (jf forvaltningsloven) gjelde uavhengig av om opplysningene er lagret elektronisk eller manuelt. Med dagens og fremtidens stadig økende bruk av edb, kan en ikke legge til grunn at opplysningene som lagres elektronisk er annerledes – mindre omfattende – enn de som lagres manuelt.

Forvaltningsloven § 18 gjelder offentlige myndigheter og passer ikke for privat sektor. Etter utvalgets syn bør imidlertid unntaket for enkelte interne dokumenter gjelde også for disse. Dette kan gjøres ved at man i loven definerer hva som i privat sektor er å regne som interne dokumenter. Dette er i dag gjort i personregisterforskriften § 1-5 annet ledd for interne dokumenter i manuelle personalregistre.

11.2.5.4.4 Unntak fra innsyn av hensyn til de registrerte eller personer som står dem nær

Unntaket i personregisterloven § 7 for opplysninger som det vil være utilrådelig å gi av hensyn til helsetilstand m v, bør fortsatt gjelde. Utvalget kan imidlertid ikke se at det eksisterer noen god grunn for å avskjære muligheten til å gi opplysningene til den registrertes representant, slik som for parter etter forvaltningsloven § 19 første ledd bokstav c.

I noen tilfeller vil innsyn i opplysninger om en selv innebære at en indirekte også gis innsyn i opplysninger om andre, uten at dette nødvendigvis medfører at en blir nektet innsyn i opplysningene. For eksempel vil dette kunne være tilfelle ved innsyn i opplysninger fra gen-materiale. Slike disposisjoner vil indirekte også si noe

om arvelige disposisjoner hos andre enn en selv. Bruk av genetisk informasjon er regulert av bioteknologiloven (lov 5 aug 1994 nr 56). Forøvrig vil utvalget understreke den enkeltes etiske ansvar i forbindelse med innsyn i og bruk av personopplysninger om en selv som indirekte også gir informasjon om andre.

11.2.5.4.5 Unntak fra innsynsrett for statistikk, forskning og generelle planer

Personregisterloven § 7 første ledd kan etter sin ordlyd vanskelig ses å være i full overensstemmelse med Europarådskonvensjonen artikkel 8, idet det ikke i den norske loven er noe krav om at unntaket åpenbart ikke skal innebære noen fare for krenkelse av personvernet. Mulighetene for å gjøre unntak er enda snevrere etter personverndirektivet artikkel 13 nr 2. Datatilsynets *praksis* ved fastsettelse av konsesjonsvilkår for slike registre har imidlertid vært i overensstemmelse med direktivets bestemmelse, og tilsynets praksis bør lovfestes. Kongen bør ha hjemmel til å gjøre unntak fra innsynsreglene.

11.2.5.4.6 Innsynsrett for umyndige

Utvalget har vurdert å foreslå egne aldersgrenser for utøvelse av innsynsrett etter loven, men fant det vanskelig å finne frem til en ensartet aldersgrense. Hvilke rettigheter det er naturlig å tildele den umyndige vil i noen grad følge av den umyndiges handleevne, jf vergemålsloven (lov 22 april 1927 nr 3) "*Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet*" i kapittel 4. Dessuten kan det være behov for i noen tilfeller å utøve skjønn mht om det skal gis innsyn for foreldre i tillegg til den umyndige. Man bør i denne sammenhengen se på hensynene bak innsynsreglene; innsynsretten er en forutsetning for at man skal kunne hevde sine øvrige rettigheter etter loven (f eks kreve retting eller sletting). Dersom ønsket om innsyn er begrunnet i andre hensyn, bør det utvises større varsomhet med å gi andre enn den registrerte selv innsyn i opplysningene.

11.2.6 De behandlingsansvarliges opplysningsplikt overfor de registrerte, EF-direktivet artikkel 10 og 11

11.2.6.1 Innledning

Datatilsynet har gjort løse anslag over hvor mange registre «gjennomsnittsnordmannen» er registrert i og antyder 500 registre. Folk flest har neppe konkret kunnskap om alle persondatabelhandlingene som angår dem selv. Dermed kan det også være vanskelig å kreve innsyn. Det er blant annet på denne bakgrunn en bør se personverndirektivets bestemmelser om aktiv opplysningsplikt for de behandlingsansvarlige overfor de registrerte. Informasjonen skal gis uavhengig av forespørsel fra de registrerte.

11.2.6.2 Behandlingsansvarliges informasjonsplikt når personopplysninger samles inn fra de registrerte – artikkel 10

Personverndirektivet fastsetter en plikt for den behandlingsansvarlige til å gi informasjon om hvem som er behandlingsansvarlig og formålet med behandlingen. I tillegg skal det gis opplysninger som er nødvendige for å sikre den enkelte en rimelig behandling av opplysningene om ham/henne. Enkelte eksempler på hva slags informasjon som kan være nødvendig er regnet opp i artikkel 10 bokstav c.

Plikten gjelder bare informasjon vedrørende behandlingen av opplysninger om den registrerte selv. Det er gjort unntak for informasjon som den registrerte allerede er kjent med. I tillegg kan det gjøres unntak i medhold av artikkel 13.

Direktivet forutsetter at den behandlingsansvarlige gjør vurderinger av hva den registrerte er kjent med, og hva som er nødvendig for en rimelig behandling av opplysningene. Såvel generell kunnskap om svakheter ved selve behandlingen som kunnskap om individuelle forhold må trekkes inn i vurderingen. En kan ikke ut i fra artikkel 10 utlede noen undersøkelsesplikt for at den behandlingsansvarlige skal få nødvendig kunnskap om relevante forhold. En slik undersøkelsesplikt kan imidlertid tenkes å hvile på annet grunnlag. Prinsippet om forsvarlig saksbehandling innen offentlig forvaltning innebærer bl a en forpliktelse til forsvarlig saksutredning, jf forvaltningsloven § 17 første ledd og § 37 første ledd.

11.2.6.3 Behandlingsansvarliges informasjonsplikt når personopplysninger ikke er samlet inn hos de registrerte – artikkel 11

Artikkel 11 omhandler de tilfelle der det er andre enn den registrerte selv som er kilde for opplysninger om den registrerte. Hovedregelen er at den behandlingsansvarlige skal gi informasjon om den behandlingen som opplysningene om den registrerte skal inngå i. Det er i hovedsak den samme informasjonen som skal gis etter denne bestemmelsen som etter artikkel 10. Dette innebærer bl a at bestemmelsen forutsetter en tilsvarende konkret vurdering av hva som er nødvendig å gi informasjon om for å sikre en rimelig behandling av personopplysningene. Informasjonen til den registrerte skal gis ved registrering av personopplysningen eller senest ved videregivelse av opplysningen. Informasjonsplikten er uavhengig av om opplysningen videregis eller ikke.

I artikkel 11 nr 2 gjøres en rekke unntak fra informasjonsplikten. For det første gjelder ikke informasjonsplikten når den registrerte allerede er kjent med de nødvendige opplysninger. For det andre gjelder unntak når registrering eller utlevering av personopplysninger eksplisitt er fastsatt ved lov. For det tredje er det gitt en mer skjønnsmessig adgang til å gjøre unntak dersom det er umulig eller uforholdsmessig vanskelig å gi informasjon om behandlingen til den registrerte. Dette vil kunne ha særlig betydning ved behandling av personopplysninger for forsknings- og statistikkøyemed. Dersom det gjøres unntak skal medlemsstatene fastsette nødvendige garantier, dvs andre tiltak som er egnet til å sikre den registrerte en rimelig behandling av opplysningene.

11.2.6.4 Relevant norsk lovgivning

Det finnes i personregisterloven ikke en tilsvarende generell bestemmelse om informasjonsplikt for registreier. For kredittopplysningsforetak gjelder det imidlertid en gjenpartsplikt når kredittopplysninger om personer som ikke er næringsdrivende blir gitt i skriftlig form. I slike tilfelle skal den det gis opplysning om sendes en kopi av kredittopplysningen eller annen melding.

Etter forvaltningsloven § 17 annet og tredje ledd har forvaltningsorganer som hovedregel en plikt til å forelegge opplysninger om en part som de mottar til uttalelse fra parten. Dette gjelder enten opplysningen mottas etter initiativ fra forvaltningen eller opplysningen sendes inn på andre aktørers initiativ. Retten til å få seg forelagt opplysninger om en selv som forvaltningsorganet mottar fra andre, er begrenset til «parter» i vedkommende sak slik dette begrepet er definert i forvaltningsloven § 2 e. Dette er en klart snevrere gruppe enn de registrerte. Forvalt-

ningsloven § 17 får dessuten kun anvendelse på enkeltvedtak, se forvaltningsloven § 3.

11.2.6.5 Stortingets vedtak 21 april 1994

Stortinget traff 21 april 1994 vedtak der det bl a het følgende:

«Stortinget ber Regjeringen legge fram forslag til endringer i lov om personregistre, slik at eieren av et personregister som hovedregel plikter å varsle personene som registreres eller er registrert, om registreringen, dens omfang og formålet med denne.»

Utvalget er i sitt mandat bedt om å vurdere og legge fram forslag til lovbestemmelser i tråd med vedtaket.

11.2.6.6 Utvalgets vurderinger

Utvalget ser på informasjonsplikten etter direktivet som et viktig supplement til retten til innsyn i personopplysninger om en selv. Begrunnelsen er primært at det kan være svært vanskelig for de registrerte å tilegne seg den kunnskap som skal til for at innsynsretten skal bli brukt. Informasjonsplikten kan fungere som varsel om persondatabehandling som den registrerte ikke har kunnskap om, og som påminnelse om betydningen av kjente handlinger. På den annen side er personvernet neppe tjent med en for stor strøm av informasjon fra en rekke avsendere til registrerte personer. Faren er da at mengden av informasjon kan bli så stor at det snarere skapes en følelse av maktesløshet enn av aktivitetslyst. Informasjonsplikten etter artikkel 10 og 11 i direktivet må også vurderes ut fra den samlede informasjonstilgangen for den enkelte, jf oversikten i "*Oversikt*" i avsnitt 11.2.1 og opprettelsen av en oversikt over melde- og konsesjonspliktige persondatabehandling. Dessuten må informasjonsplikten utformes slik at kostnadene og ulempene for de behandlingsansvarlige ikke blir for store.

Når det gjelder informasjonsplikten når opplysninger samles inn fra den registrerte selv (artikkel 10), antar utvalget at dette vil innebære lite praktisk arbeid og små utgifter for de behandlingsansvarlige. Samtidig må slik informasjon anses som ønskelig ut fra hensynet til ivaretagelse av personvern. Når det derimot gjelder informasjon til de registrerte i de tilfelle der opplysningene er samlet inn fra andre, vil dette normalt gjøre det nødvendig å sende brevpost. Dersom mengden av slike forsendelser blir stor, kan dette innebære en betydelig kostnad for de behandlingsansvarlige.

Utvalget ønsker på denne bakgrunn å finne fram til en ordning der informasjonsplikten konsentreres rundt tilfelle der informasjon er spesielt ønskelig ut fra hensynet til personvernet. Dette kan oppnås ved å tilpasse varslingsplikten innenfor de rammer direktivet og Stortingets vedtak setter. For de nærmere detaljene vises til merknadene til lovforslaget §§ 20 og 21. Utvalget nøyer seg her med å understreke at varslingsplikten ikke er nødvendig der den registrerte allerede kjenner til persondatabehandlingen, og at det er tilstrekkelig å varsle første gang vedkommende behandlingsansvarlig innhenter opplysningene. Varsel kan dessuten ofte gis via kommunikasjon som uansett finner sted mellom den behandlingsansvarlige og den registrerte – de fleste persondatabehandling som finner sted inngår som ledd i en virksomhet hvor det oppstår kontakt mellom den registrerte og den behandlingsansvarlige. I slike tilfelle er det ikke nødvendig med en egen varslingsforsendelse for å oppfylle informasjonsplikten.

11.3 DEN ENKELTES RETT TIL Å MOTSETTE SEG VISSE TYPER PERSONDATABEHANDLING

11.3.1 Den registrertes rett til å motsette seg at bestemte personopplysninger blir behandlet

11.3.1.1 EF-direktivet artikkel 14

Direktivet artikkel 14 fastsetter en rett for den enkelte til å motsette seg at bestemte personopplysninger om ham selv blir gjenstand for behandling. Innsigelsesretten etter artikkel 14 må ses i sammenheng med retten etter artikkel 15. I tillegg er spørsmålet nært knyttet opp til retten til sletting av opplysninger, jf artikkel 12 bokstav b som viser til artikkel 15 nr 1.

Det er knyttet flere forutsetninger til rettigheten etter artikkel 14 bokstav a. For det første er retten avgrenset til to av de seks kategorier av persondatabehandlinger som etter direktivet artikkel 7 regnes som legitime. Den første kategorien gjelder behandlinger som er nødvendige ut i fra hensynet til samfunnsmessige interesser eller offentlig myndighetsutøvelse (bokstav e). Den andre kategorien gjelder behandlinger som er nødvendig for at behandlingsansvarlige og/eller de tredjemenn personopplysningene videregis til skal kunne forfølge sine «legitime-interesser», jf avveiningen mellom slike legitime interesser og den enkeltes grunnleggende rettigheter (artikkel 7 bokstav f i f).

Dersom persondatabehandlingen kommer inn under en av de nevnte behandlingkategoriene og den registrerte framsetter «berettiget innsigelse» mot behandlingen, plikter den registeransvarlige å avstå fra å behandle denne opplysningen. Det er uklart hvor mye som skal til for at innsigelsen skal anses å være «berettiget». Begrunnelsen for innsigelsen må være knyttet til den registrertes *særlige situasjon*, fordi det allerede er foretatt en generell interesseavveining som har resultert i at behandlingen i utgangspunktet anses lovlig. Det er anledning til å begrense retten etter artikkel 14 bokstav a i eller i medhold av nasjonal lovgivning.

Innsigelsesretten etter artikkel 14 bokstav b gjelder persondatabehandlinger som er ledd i *markedsføring*. En grunnforutsetning må her være at behandlingen er lovlig i tråd med bestemmelsene i artikkel 7. *Selv om* behandlingen er lovlig etter disse bestemmelsene gir artikkel 14 nr b den enkelte rett til å motsette seg at behandling av opplysninger om ham selv skjer for markedsføringsformål.

Som et alternativ til å nekte all behandling som ledd i markedsføring, gir direktivbestemmelsen den enkelte en rett til å kreve varsel før første gangs videregivelse av opplysninger. Likestilt med dette er første gangs behandling på vegne av tredjemann når behandlingen skjer for markedsføringsformål. Bestemmelsen synes å innebære en rett til f eks å kreve et varsel dersom et adresseringsforetak overfører (selger) opplysninger og mottakeren vil anvende opplysningene til markedsføring. Varselet ligner på informasjonsplikten i artikkel 11, men gjelder også dersom opplysningen er samlet inn fra den registrerte selv.

Til slutt i artikkel 14 forpliktes nasjonalstatene til å iverksette de tiltak som er nødvendig for at rettighetene i forhold til markedsføring blir kjent blant de registrerte. Det kreves med andre ord informasjonstiltak eller lignende, men det er ikke fastsatt noe nærmere om hvem som skal gjennomføre tiltakene.

11.3.1.2 Personregisterloven § 8 a

Man har både etter personregisterloven §§ 8a og 28 og forskriften § 2-1 krav på å få sitt navn sperret mot utsendelse av adressert reklame. Reservasjonsretten gjelder både adressert reklame og telefonmarkedsføring. For å effektivisere denne retten er

dessuten adresseringsforetakene i konsesjonen fra Datatilsynet pålagt å merke sendingene med kilde for adresseopplysningen.

Paragraf 8a kom inn i loven ved lovendringen i 1987 (lov 12 juni 1987 nr 55). Bestemmelsen kom som et følge av forslag fra Føyen-utredningen. Som begrunnelse het det bl a i utredningen:

«Det er etter hvert blitt svært vanlig at alle mulige abonnementsregistre, medlemsregistre, kunderegistre, leverandørregistre osv, benyttes for utsendelse av direkte adressert reklame. Bestemmelsene om sletting (sperring) for utsendelse av direkte reklame slik de er etter den någjeldende loven og forskriftene, er spredd på flere forskjellige steder, og de er nokså uoversiktlige. Den foreslåtte bestemmelsen tar sikte på å fastsette en generell rett for den enkelte til å kreve en samling av personopplysninger sperret mot slike utsendelser til seg.»

Det er ut over dette ikke noen adgang til å nekte visse typer behandling av personopplysninger etter norsk rett.

11.3.1.3 Utvalgets vurderinger

11.3.1.3.1 Innsigelsesretten etter direktivet artikkel 14 a

Retten til å motsette seg behandling gir rett til å motsette seg at enhver behandling av personopplysninger skjer (f eks lagring), men den enkelte må også kunne motsette seg behandlingen på mindre omfattende måte.

Utvalget ser artikkel 14 a som et utslag av en grunnleggende rettighet til å råde over opplysninger om en selv. Med de begrensninger som ligger i bestemmelsen, blir imidlertid regelen svært lite praktisk. I tillegg må det gjøres unntak av hensyn til ytringsfrihet og pressefrihet. Utvalget legger til grunn at direktivet artikkel 14 nr 1 er tilstrekkelig gjennomført dels ved at lovforslaget gir den registrerte enkelte rettigheter (se for eksempel lovforslaget §§ 25 og 26 om rett til å kreve opplysninger slettet) og dels ved at slike beføyelser kan utledes fra ulovfestede personvernprinsipper (se som eksempel Rt 1952 side 1217).

11.3.1.3.2 Reservasjonsrett for bruk av personopplysninger om en selv i markedsføringsøyemed

Dagens bestemmelse i personregisterloven § 8a om at en person kan kreve sitt navn sperret i et personregister mot bruk til utsending av reklame og liknende publikasjoner bør videreføres i den nye loven. Den økende mengden av adressert reklame oppleves av mange som en belastning. Det er derfor viktig at den enkelte forbruker gis en effektiv rett til å reservere seg mot adressert reklame. På grunn av det stadig økende antall adresserings- og distribusjonsforetak er det imidlertid ofte blitt vanskelig for den enkelte å få oversikt over hvilke registre som inneholder opplysninger om en selv, og dermed tilsvarende vanskelig å framsette krav om sletting til hvert enkelt foretak etter personregisterloven § 28. I denne forbindelse har Datatilsynet foreslått opprettelsen av et sentralt reservasjonsregister, som vil innebære at de som ønsker seg slettet fra *alle* registre i adresserings- og distribusjonsforetak, kan oppnå dette gjennom framsettelse av bare *ett* krav om sletting – rettet til det sentrale registeret. En plikt for adresserings- og distribusjonsselskapene til å oppdatere («vaske») sine registre mot det sentrale reservasjonsregisteret, vil bety en forenkling og effektivisering av utøvelsen av retten til å kreve seg slettet av registre etter § 28 og til å kreve sitt navn sperret etter § 8a.

Opprettelsen av et sentralt reservasjonsregister er omtalt av Datatilsynet i Datatilsynets årsmeldinger for 1993 og 1994 (St meld nr 23 1994-95, side 18 og St meld nr 27 1995-96, side 18). I følge de samme stortingsmeldingene, samt St meld nr 33 1994-95 om Personvern og telekommunikasjon støtter Justisdepartementet forslaget og uttaler at det arbeides aktivt i departementet med disse planene (side 16).

Utvalget foreslår at det nedfelles i loven at de som markedsfører direkte skal vaske sine registre mot et sentralt reservasjonsregister, se merknadene til lovforslaget § 28. Plikten bør i utgangspunktet gjelde generelt, ikke bare for adresserings- og distribusjonsforetak.

11.3.2 Rett til i visse tilfeller å kreve manuell behandling av personopplysninger

11.3.2.1 EF-direktivet artikkel 15

EF-direktivet artikkel 15 nr 1 gir en rett for den enkelte til å nekte å la seg undergi visse fullstendig automatiserte avgjørelser. Bestemmelsen omhandler avgjørelser vedrørende personlige forhold som har rettsvirkninger for den enkelte eller som berører den enkelte i vesentlig grad, og som i sin helhet er truffet på grunnlag av edb-behandling av opplysninger. Avgjørelser om ervervsevne, kredittverdighet, pålitelighet og adferd er eksempler på avgjørelsestyper som omfattes.

Et første kriterium etter artikkel 15 nr 1 er at avgjørelsen skal innebære *en vurdering eller beskrivelse av personlige forhold*. Eksempler på dette er personlige ferdigheter, evner og personlighetstrekk. En rekke behandlinger må således anses å falle utenfor bestemmelsen allerede i utgangspunktet. Avgjørelse i f eks en byggesak er basert på opplysninger om byggeplaner m v og ikke fundert på beskrivelser av personlige forhold. Et avslag på søknad om arbeidsledighetstrygd med den begrunnelse at søkeren er skyld i egen ledighet, vil derimot i utgangspunktet kunne falle inn under de avgjørelseskategorier som er basert på beskrivelser av personlige forhold. Derimot ikke den enkelte avgjørelse av størrelse på pensjon og andre ytelser når det kun er inntekts- og formuesforhold som legges til grunn for resultatet. Avgrensningen av hva som skal regnes som «bestemte personlige forhold» må generelt sies å være relativt uklar.

Det andre kriteriet etter artikkel 15 nr 1 er at avgjørelsen har *rettsvirkninger* for den enkelte. Dette innebærer trolig at avgjørelsen skal kunne håndheves ved hjelp av rettssystemet. Direktivet likestiller dessuten avgjørelser som berører den enkelte i vesentlig grad med avgjørelser som har rettsvirkninger. Et mulig eksempel på avgjørelser som berører den enkelte i vesentlig grad kan være utarbeidelse av kundeprofiler og andre atferdsmønstre når disse selges/spres til mange tilbydere av varer og tjenester og således danner bakgrunn for en rekke salgshenvendelser m v til den enkelte.

Det tredje kriteriet er at behandlingen av opplysningene kun skjer ved edb-behandling, dvs at den videre behandlingen av opplysningene *kun* skjer i et data-maskinsystem. En manuell etterkontroll av resultatet fra edb-behandlingen, f eks i form av en rimelighetskontroll, vil gjøre at behandlingen ikke kan nektes.

Fra hovedregelen om rett til å nekte å bli undergitt avgjørelser som kun er basert på edb-behandlinger, gjelder to viktige unntak i artikkel 15 nr 2 bokstavene a og b.

Etter bokstav a skal den omtalte retten til å nekte ikke gjelde når den helt automatiserte avgjørelsen skjer som ledd i inngåelsen eller oppfyllelsen av en *kontrakt*. Dette forutsetter at det er den registrerte selv som har anmodet om inngåelsen eller oppfyllelsen av kontrakten, eller at det eksisterer tiltak som er egnet til å ivareta den registrertes legitime interesser (f eks i form av en uttalerett for den registrerte). Såle-

des vil f eks en fullstendig automatisert kredittvurdering *ikke* gi rett til å nekte slik behandling dersom behandlingen skjer som ledd i inngåelse av en låneavtale som den registrerte selv har bedt om. Retten til å nekte gjelder heller ikke selv om det er kredittvurderingsforetaket som har tatt initiativet til behandlingen, så lenge den registrerte kan vareta sine legitime rettigheter gjennom en uttalerett el l.

I følge artikkel 15 nr 2 bokstav b skal det heller ikke eksistere noen rett til å nekte fullstendig automatisert behandling når denne behandlingen er *hjemlet i lov*. Forutsetningen er at det i lovgivningen er vedtatt bestemmelser til ivaretagelse av den registrertes legitime interesser.

Den norske personregisterloven og europarådskonvensjonen om personvern inneholder ingen bestemmelser om rett til å nekte helt automatiserte avgjørelser.

11.3.2.2 Utvalgets vurderinger

Når en ser hele artikkel 15 under ett, synes unntakene å være så vidtfavnende at det kun blir i de helt spesielle tilfellene at retten til å nekte fullstendig automatisert behandling etter artikkel 15 nr 1 vil være i behold. Hvor stor betydning bestemmelsen får for personvernet vil bli avhenge av hvor strenge krav som stilles til tiltakene for å vareta personvernet. Det er kun hvis disse tiltakene er tilfredsstillende at manuell vurdering ikke kan kreves. Datatilsynet kan ta stilling til om tiltakene er tilfredsstillende. En kan ikke utelukke en samfunnsutvikling der de typer fullstendig automatiserte beslutninger hvor nektelsesretten gjelder blir vanligere. Det er derfor mulig at en norsk lovbestemmelse etter mønster av artikkel 15 vil kunne påvirke utformingen av de automatiske behandlingene i en – sett fra personvernens syn – positiv retning.

Det er grunn til å understreke at direktivet kun regulerer avgjørelsesmåten hos beslutningsorganet, og ikke legger begrensning på retten til å få avgjørelser overprøvet av domstolene. Videre er det ofte klageadgang for avgjørelser som et beslutningsorgan treffer, noe som hindrer etableringen av fullstendig automatiserte rutiner innen de aktuelle avgjørelsestypene. Utvalget legger til grunn at nektelsesretten og unntakene fra denne ikke får betydning for klageretten så lenge denne ikke er begrenset i lovgivningen. Selv om den enkelte ikke kan nekte å la seg undergi fullstendig automatiserte beslutninger fordi det gjelder inngåelse av kontrakt, kan Datatilsynet påpeke forhold som ut i fra et personvernssynspunkt er uheldig. Dersom behandlingsrutinene f eks er basert på for lav datakvalitet, må Datatilsynet kunne påpeke forholdet, og eventuelt gi pålegg om at kvalitetsmangelen skal avhjelpes.

11.4 INNSYN I BEHANDLINGSREGLER («LOGIKKEN»)

11.4.1 Krav på innsyn i logikken til visse typer persondatabehandlinger, EF-direktivet artikkel 12 bokstav a, tredje strekpunkt

Direktivet artikkel 12 bokstav a tredje strekpunkt gir enhver rett til «at få vite, hvilken logik der ligger bag edb-behandlingen af oplysningerne om den pågældene [...]», i det minste i slike tilfelle som er regulert i artikkel 15 nr 1. Det redegjøres for innholdet av artikkel 15 ovenfor i 11.3.2. Innsynet i behandlingsregler («logikken») hører naturlig inn under retten til innsyn (11.2). Innsynet i behandlingsregler er likevel skilt ut til særskilt behandling i dette avsnittet på grunn av sammenhengen med regelen i direktivet artikkel 15.

Direktivets bestemmelser om rett til logikkinnsyn er knyttet til konkrete behandlinger av personinformasjon om den enkelte. Henvisningen til artikkel 15 innebærer at behandlingene må ha ledet ut i en *avgjørelse* som har rettslig eller annen vesentlig betydning for vedkommende. Logikkinnsynet etter direktivet

gjelder med andre ord ved visse avgjørelser av konkrete saker. Bestemmelsen får derfor preg av å være et krav om *begrunnelse* og innebærer f.eks. ingen plikt til å etablere innsynsrett i logikken bak en edb-behandling *forut* for en avgjørelse. Dette er en viktig presisering, fordi en rett til et slikt innsyn uavhengig av konkrete avgjørelser ville innebære en forpliktelse til å gi innsyn i alle mulige behandlingsregler innenfor en avgjørelsestype til enhver tid. Dermed får regelen mer et preg av å støtte opp under den enkeltes varettagelse av sine interesser i konkrete saker, snarere enn å støtte den enkeltes behov for generelt å orientere seg om behandlingsmåter og *mulige* framtidige beslutningssituasjoner. Dersom en skal trekke sammenligninger til dagens offentligrettslige reguleringer, er det som nevnt mest nærliggende å se en rett til logikkinnsyn i sammenheng med forvaltningslovens regler om begrunnelse for enkeltvedtak og regler om veiledning og partsinnsyn.

11.4.2 Relevant norsk lovgivning – spesielt om forvaltningslovens veilednings- og begrunnelsesplikt

Forvaltningen har generell veiledningsplikt etter forvaltningsloven § 11. Avhengig av den enkeltes informasjonsbehov og innholdet av konkrete forespørsler fra publikum, er det nærliggende å forutsette at forvaltningen også må kunne redegjøre for automatiserte behandlingsregler, dvs. for den «logikk» som er implementert i systemet.

Forvaltningsloven har dessuten regler om begrunnelsesplikt for offentlig forvaltning. Etter § 25 skal begrunnelsen «vise til de regler vedtaket bygger på, med mindre partene kjenner reglene». Forvaltningsorganet skal også gjengi innholdet av reglene, dersom dette er nødvendig for at partene skal forstå vedtaket. Dette må forstås slik at forvaltningen har en plikt til å gjengi innholdet av rettsregler som er gjenstand for automatisert anvendelse i et saksbehandlingssystem. Dersom det automatiserte vedtaket skal kunne begrunnes i detalj, er det imidlertid også nødvendig å forklare de rettslige behandlingsreglene i de aktuelle edb-programmene, med andre ord «logikken» i behandlingen.

Også innen særlovgivningen finnes eksempler på spesielle regler om begrunnelse som i konkrete tilfelle kan synes å forutsette forklaringer av «logikken i edb-programmer». Således plikter f.eks. ligningsmyndighetene etter ligningsloven § 8-9 nr 2 å opplyse til skattyter om hvorledes ligningsmyndigheten har kommet fram til fastsetting av inntekt og formue. I den grad fastsetting skjer maskinelt, vil en utlegning av framgangsmåten nødvendigvis måtte ta utgangspunkt i vedkommende edb-rutine.

11.4.3 Utvalgets vurderinger

Utvalget legger til grunn at i den grad omfattende automatisering gjennomføres, tilsier den enkeltes interesse i opplysthet at det finnes tilgjengelige forklaringer som viser hva innholdet av den automatiske behandlingen er.

Direktivets bestemmelse om retten til å få forklart logikken i visse datamaskinprogrammer må ses på bakgrunn av at anvendelse av rettsregler og andre regler i dag ofte skjer ved hjelp av datamaskinsystemer. I så fall er det den automatiserte regelansvaret som reellt sett avgjør utfallet av saksbehandlingen. Riktignok vil det regelmessig være slik at reglene i edb-programmene uttrykker innholdet i regler som finnes i vanlig språk, f.eks. i lov, forskrift eller kontrakt. Programmene gir imidlertid et presist uttrykk for bestemte tolkningsvalg blant flere mulige. Det kan lett tenkes å være uenighet mellom f.eks. et avgjørelsesorgan og en part om riktigheten av slike valg. En plikt til å måtte forklare innholdet av visse datamaskinprogram-

mer, kan derfor ses som en forutsetning for en tilstrekkelig opplysning om innholdet i rettsanvendelsen, f eks med tanke på domstolsprøving.

Utvalget mener at sentrale deler av vår forvaltningslovgivning innebærer krav om at offentlige forvaltningsorganer i visse situasjoner må kunne gjøre rede for «logikken» i de datamaskinprogrammer som er bestemmende for vedtakets rettslige innhold. Slike forpliktelser gjelder uavhengig av om vedtakstypen er fullstendig automatisert, representerer en personlighetsprofil m v. Sett på en slik bakgrunn får direktivets bestemmelse om «logikkinnsyn» formelt sett ingen store konsekvenser for offentlig forvaltning. Reelt sett kan en slik bestemmelse imidlertid føre til større grad av bevissthet om at et slikt krav om innsyn og forklaring er aktuelt og legitimt.

På privat sektor finnes det ingen generelle bestemmelser som gir rett til innsyn i eller å få forklart behandlingsreglene (logikken) i datamaskinsystemer. Imidlertid er det i dag trolig et meget lite antall datamaskinsystemer som omfattes av personverndirektivet artikkel 12 bokstav a tredje strekpunkt jf artikkel 15 nr 1, hvilket innebærer at kravet om logikkinnsyn har meget begrenset rekkevidde. Et mulig eksempel på behandlinger som omfattes av bestemmelsen er systemer for vurdering av kredittverdighet der det ikke skjer noen manuell etterprøving av resultatet fra den maskinelle behandlingen. Slike tjenester er aktuelle og kan i fremtiden bli praktisk viktige innen enkelte virksomhetsområder. Det er f eks lansert «bankkiosker» med fullautomatisert behandling av søknader om lån til forbrukerkjøp. Utvalget legger likevel til grunn at det kun vil være begrenset anvendelse av automatiserte tjenester der det ikke finnes noen form for adgang til manuell overprøving av beslutningen.

Bestemmelsen vil innebære tilleggs kostnader for de behandlingsansvarlige. Hvor stor denne utgiften vil bli, er bl a avhengig av tilgjengelige verktøy for utvikling av forklaringsmoduler, og kvaliteten av de kravspesifikasjoner og dokumentasjon som uansett er planlagt for vedkommende persondatabehandling. Jo mer detaljert og nøyaktig systemdokumentasjon som finnes, jo mindre ekstrakostnader må det antas å påløpe. Utvalget minner om at det bl a også ut i fra hensynet til regnskapsmessig reviderbarhet stilles krav til systemdokumentasjon, noe som igjen vil gjøre det lettere å gjennomføre direktivets krav.

11.4.4 Mer-innsyn

Utvalget ønsker å understreke at de også i fremtiden vil være slik at en manglende innsynsrett ikke innebærer noe forbud mot å gi innsyn også i andre tilfelle (med mindre det på lovlig måte er etablert taushetsplikt), og utvalget vil anbefale at et slikt mer-innsyn vurderes.

11.5 PLIKT TIL Å RETTE, SLETTE OG SUPPLERE

11.5.1 Personregisterloven § 8

Personregisterloven § 8 pålegger plikt til å rette, slette og supplere personopplysninger som er uriktige, ufullstendige eller ulovlige å ta inn i et register dersom manglene kan få betydning for den registrerte. Den registeransvarlige skal også sørge for at virkningene av manglene blir minst mulig.

Loven gir Datatilsynet myndighet til å gi pålegg om retting, sletting eller supplering. Slikt pålegg kan f eks tenkes gitt etter henvendelse fra den registrerte selv, eller som resultat av gransking som Datatilsynet gjennomfører som ledd i sitt kontrollarbeid. Datatilsynets kompetanse til å kreve endring innebærer at tilsynet har en rett til å avgjøre om konkrete personopplysninger er korrekte, lovlige eller fullstendige. Avgjørelse i slike saker er enkeltvedtak og kan påklages til Justisdepartementet.

Plikten til å rette på mangler ved opplysninger gjelder når mangelen kan få betydning for den registrerte. Etter ordlyden gjelder dette vilkåret også for sletting av opplysninger som det ikke er anledning til å ta inn i registeret. I slike tilfelle må trolig den ulovlige bruken alltid anses å ha betydning for den registrerte, slik at ulovlige opplysninger alltid skal slettes.

Loven krever ikke at mangelen ved opplysningen faktisk får betydning, men forutsetter bare at dette er en mulighet (jf ordet «kan»). Det er vanskelig generelt å angi hvilken sannsynlighetsgrad som kreves. Jo mer alvorlig virkning feilen kan få for den registrerte, jo lavere sannsynlighetsgrad kreves før mangelen må avhjelpes.

11.5.2 EF-direktivet artikkel 12 bokstavene b og c

I henhold til EF-direktivet artikkel 12 bokstav b har de registrerte rett til å få endret mangelfulle opplysninger. Direktivet nevner to konkrete mangelstyper. I tillegg viser direktivet mer generelt til situasjoner der behandlinger ikke er i overensstemmelse med direktivet. Fremhevingen av ufullstendighet og uriktighet er en *eksemplifisering* av mangler som kan kreves rettet av den registrerte. Artikkel 12 bokstav b må for øvrig ses i sammenheng med artikkel 6 som stiller krav til lovlighet og rimelighet av behandlinger, formålsangivelse for behandlinger samt krav til personopplysningers kvalitet.

Artikkel 12 bokstav b stiller opp retting, sletting og blokkering som aktuelle tiltak for å rette mangler ved opplysninger. Retten til å få opplysninger *supplert* nevnes ikke uttrykkelig, men kan trolig innfortolkes i retten til å kreve opplysninger rettet.

I direktivet artikkel 12 bokstav c gis den enkelte en rett til å kreve å få rettet, slettet eller blokkert mangelfulle opplysninger som den registeransvarlige har videregitt til tredjemann. Unntak gjelder der dette er umulig eller uforholdsmessig vanskelig. Direktivet krever ikke at manglene skal ha betydning for den registrerte for at tiltak overfor tredjemenn skal kunne kreves. En annen forskjell mellom personregisterloven og direktivet er at direktivet knytter tiltakene i bokstav c til *videregivelse* av mangelfulle opplysninger til tredjemann, mens det etter personregisterloven § 8 er følgen av feilen som er avgjørende.

Direktivet fastsetter i artikkel 28 nr 3 annet strekpunkt at også tilsynsmyndigheten skal kunne kreve personopplysninger blokkert, slettet eller tilintetgjort.

11.5.3 Europarådskonvensjonen artikkel 8 bokstavene c og d

Europarådskonvensjonen artikkel 8 bokstav c forplikter landene til å gi de registrerte rett til å få opplysninger om dem selv rettet eller slettet dersom opplysningene er behandlet i strid med konvensjonen artikkel 5 om krav til datakvalitet og artikkel 6 om vilkår for behandling av spesielt sensitive opplysninger. Artikkel 5 bokstavene a til e spesifiserer hva slags mangler ved personopplysninger den registrerte kan kreve endring av. De tiltak som skal kunne kreves gjennomført etter konvensjonen (retting og sletting), representerer derimot et lavt presisjonsnivå og må formentlig tolkes i lys av artiklene 5 og 6 slik at ethvert brudd på krav til datakvalitet og behandling av sensitive opplysninger kan møtes med et relevant tiltak.

Etter artikkel 8 bokstav d er statene forpliktet til å gi regler som gir rett til en selvstendig prøving («å klage eller på annen måte bringe saken videre») av krav fra den registrerte om retting eller sletting.

11.5.4 Utvalgets vurderinger

11.5.4.1 Plikt til å rette, slette og supplere uriktige eller ulovlige opplysninger

Utvalget går inn for en videreføring av dagens § 8, med enkelte endringer.

For det første bør Datatilsynet gis kompetanse til også å pålegge sperring av personopplysninger i tilfeller hvor de uriktige opplysningene av forskjellige grunner ikke kan eller bør rettes eller slettes (for eksempel fordi dette er pålagt i lov eller forskrift).

For det andre bør restitusjonsregelen i dagens § 8 første ledd annet punktum utvides slik at den behandlingsansvarlige også plikter å rette opp uheldige følger av at det er gitt eller brukt ulovlige opplysninger.

Dersom det er uenighet mellom den behandlingsansvarlige og den registrerte om riktigheten av en opplysning, bør Datatilsynet normalt ikke ha myndighet til å kreve opplysningen rettet eller slettet. Dette gjelder spesielt dersom opplysningen inngår som et beslutningsgrunnlag for f.eks. et enkeltvedtak. Det er naturlig at avgjørelsen i slike spørsmål avgjøres av de som benytter opplysningen som beslutningsgrunnlag, eventuelt av klageinstansen der det er klageadgang. Datatilsynet kan i slike tilfeller pålegge supplering av opplysningen og vil forøvrig ha en ombudsmannsrolle ved vurderingen av om opplysninger bør rettes/slettes. Dette er i samsvar med Datatilsynets praksis i dag, se Datatilsynets høringsuttalelse referert i Ot prp nr 77 (1991-92) side 16 venstre spalte der det heter at Datatilsynet normalt ikke vil gi påbud om sletting av opplysninger som fører frem til vedtak. Løsningen harmonerer også med prinsippet bak arkivloven § 9 d (se nærmere om forholdet til arkivloven nedenfor).

11.5.4.2 Sletting av personopplysninger når det ikke lenger er saklig grunn for oppbevaring, samt den enkeltes rett til å kreve opplysninger slettet

Utvalget mener det er viktig at det i loven innføres regler om når personopplysninger skal slettes. I dag fastsettes slike bestemmelser av Datatilsynet i konsesjonene. Utgangspunktet bør være at opplysningene skal slettes når det ikke lenger er saklig grunn for oppbevaring. Datatilsynet bør ha myndighet til å pålegge sletting i de tilfeller det mener det ikke foreligger saklig grunn til oppbevaring, se nærmere merknadene til lovforslaget § 26. I tillegg foreslår utvalget at den enkelte registrerte kan kreve slik sletting dersom visse vilkår er oppfylt.

11.5.4.3 Forholdet til offentlige arkiver

Spørsmål om sletting og retting av personopplysninger har en side til regelverket for *offentlige arkiver* (se generelt om forholdet til arkivreglene under 6.1.9 og merknadene til § 26). Behovet for å kunne slette og rette personopplysninger slik at feilaktig informasjon ikke misbrukes kan komme i konflikt med behovet for å bevare arkivmateriale.

Da personregisterloven ble utarbeidet ble ikke denne problemstillingen i særlig grad vurdert. Den manglende avveiningen av arkivhensyn mot personvernens hensyn førte dels til at det gjeldende arkivregelverket og personregisterloven med forskrifter i noen grad strider mot hverandre, og dels til at det er fare for at Riksarkivaren og Datatilsynet treffer tilsynelatende motstridende vedtak.

Forholdet mellom arkivhensyn og personvernens hensyn ble hensyntatt da den nye arkivloven ble utarbeidet (loven er ennå ikke satt i kraft, jf 6.1.9), jf Ot prp nr 77 (1991-92) s 16. I arkivloven heter det i § 9 bokstav c at offentlig arkivmateriale bare kan *kasseres* når dette er hjemlet i arkivforskriften. Dette kasseringforbudet går

foran regler i eller i medhold av andre lover. Om *retting* heter det i arkivloven § 9 bokstav d at arkivmateriale ikke kan rettes på en slik måte at tidligere uriktige eller ufullstendige opplysninger blir slettet, dersom disse har hatt noe å si for saksforberedelsen, vedtak eller annet som etter formålet med arkivloven bør kunne dokumenteres. Både for bokstav c og d er det imidlertid gjort *unntak for personregisterloven* og vedtak fattet i medhold av denne. I arkivloven § 9 første ledd bokstav c heter det at:

«Personregister eller delar av personregister kan likevel slettast etter føresegnene i [personregisterloven]. Slik sletting kan først gjerast etter at det er innhenta fråsegn frå Riksarkivaren.»

Dette innebærer at Riksarkivaren skal *høres* før sletting eventuelt finner sted. Riksarkivaren kan på denne måten komme med synspunkter på om f.eks. retting eller supplering bør velges istedenfor sletting. Det fremgår imidlertid av arkivloven at det er Datatilsynet alene som *avgjør* om det skal gis pålegg om sletting iht personregisterloven § 8 annet ledd.

I arkivloven § 9 bokstav d om *retting* av ufullstendige eller uriktige opplysninger heter det at vedtak om sletting i medhold av §§ 8 og 11 i personregisterloven gjelder uinnskrenket, dvs. at slike vedtak går foran reglene i arkivloven. (En tilsvarende regel er gitt i arkivloven § 18 om innskrenket råderett over private arkiver.)

Utvalget har drøftet om avveiningen av personvern hensyn mot arkiv hensyn til sier at reglene om sletting bør endres. Sletting er en ugjenkallelig handling som kan føre til at arkivmateriale går tapt for alltid. I Datatilsynets konsesjoner er dette fanget opp ved at overføring til godkjent arkivinstans kan tre i stedet for sletting. Utvalget går inn for en løsning som forhåpentligvis kan rydde av veien noe av den uklarheten som i dag i praksis råder om forholdet mellom Riksarkivarens kassasjonsvedtak og Datatilsynets konsesjonsbestemmelser om sletting.

I enkelte tilfelle vil imidlertid bevaring av opplysningen ha så stor negativ betydning for den registrerte at sletting bør kunne skje såfremt dette ikke strider mot lov.

11.6 NOEN FELLESPØRSMÅL

11.6.1 Tidsfrister for å etterkomme krav fra de registrerte

11.6.1.1 Gjeldende rett

Det finnes bare spredte eksempler på krav til hvor raskt de behandlingsansvarlige skal gi svar på henvendelser fra de registrerte og ellers utføre plikter i forhold til de registrerte. Forskriftene til personregisterloven §§ 1-1 og 12 bestemmer at svar på henvendelser om innsyn i personregister i henhold til § 7 i loven skal gis snarest mulig og senest innen én måned. For innsyn i hvilke opplysningstyper som er tatt inn i offentlige registre, skal svar skje umiddelbart (forskriften § 1-3). De to førstnevnte bestemmelsen tilsvare stort sett det som gjelder for offentlig forvaltning, se forvaltningsloven § 11a. Dersom henvendelsen begrunner tidkrevende undersøkelser, vil det her være tilstrekkelig at det foreløpige svaret foreligger innen fristen. Melding om utlevering av kredittopplysninger om privatpersoner til den omspurte skal sendes *samtidig* med avgivelsen av kredittopplysningen (personregisterloven § 19).

11.6.1.2 EF-direktivet

Innsyn etter direktivet artikkel 12 skal skje «uden større ventetid». I artikkel 11 er det bestemt at melding til den registrerte skal sendes «ved registreringen af oplysningerne, eller senest når oplysningerne første gang videregives til tredjemand». For øvrig er det i direktivet ikke fastsatt nærmere bestemmelser om frister for hvor raskt de registrerte skal motta svar på henvendelser og meldinger fra de behandlingsansvarlige for øvrig.

11.6.1.3 Utvalgets vurderinger

Utvalget mener det er av stor betydning for effektiviteten av de individuelle garantiene at de behandlingsansvarlige reagerer raskt på henvendelser fra de registrerte, og for øvrig utfører sine plikter overfor de registrerte uten unødige forsinkelser. Selv om den totale arbeidsbelastning kan gjøre det vanskelig å prioritere slike oppgaver, er det grunn til å vente at de behandlingsansvarlige vil etablere rutiner for effektivt innsyn m v. Dette vil gjøre det lettere å etterleve slike forpliktelser.

Utvalget vil foreslå at det gis regler om frister i en rekke situasjoner der den behandlingsansvarlige skal bidra til realisering av individuelle garantier etter loven. Det bør imidlertid presiseres at det er tilstrekkelig å gi et midlertidig svar dersom forholdene tilsier en lengre svartid enn én måned.

11.6.2 Kostnader knyttet til de registrertes rettigheter

11.6.2.1 Gjeldende rett

Praktiseringen av slike individuelle garantier som er behandlet i dette kapittelet innebærer kostnader for de behandlingsansvarlige, f eks i form av arbeid med å gi innsyn, ta utskrifter av opplysninger m v. Også de registrerte vil imidlertid ha kostnader på lignende måte, både i form av arbeid og utlegg.

Det er ikke gitt noen generell bestemmelse om adgang til å ta seg betalt for innsyn m v etter personregisterloven. Derfor må det kreves spesiell hjemmel for at slik betaling kan være lovlig. En slik hjemmel finnes i personregisterloven § 20 annet ledd for skriftlige meldinger til de registrerte fra kredittopplysningsselskaper med opplysninger om hvilke kredittopplysninger om de registrerte som selskapet har.

11.6.2.2 EF-direktivet

EF-direktivet inneholder enkelte spredte bestemmelser om de registrertes betalingsforpliktelser i samband med praktisering av innsyn m v. I artikkel 12 heter det at innsyn skal kunne skje «uden større udgifter». Innsigelsesretten etter artikkel 14 bokstav b (markedsføring) skal skje «uden utgifter». I tilknytning til de øvrige bestemmelser som gir anvisning på individuelle personverngarantier er det ikke fastsatt noe om hvilken betaling som kan kreves.

11.6.2.3 Utvalgets vurderinger

Personvernet vil neppe være tjent med ordninger som påfører de behandlingsansvarlige store ekstrautgifter. Utvalget har derfor gjennomgående lagt vekt på å skape rasjonelle ordninger som ikke går lenger enn det som er godt saklig begrunnet. Dermed vil en i utgangspunktet også redusere de behandlingsansvarliges behov for å kreve godtgjørelse for å gi innsyn m v. Betaling for å benytte seg av individuelle garantier (innsynsrett m v) er lite ønskelig av flere grunner. For det første innebærer betaling en ny terskel som kommer i tillegg til terskelen å overhode tørre, orke eller

ta seg tid til å benytte seg av sin rett etter loven. For det andre kan betaling innebære en forskjell mellom de som kan ta seg råd og de som ikke kan ta seg råd til å benytte sin rett. Å ta betaling kan på denne måten brukes som et virkemiddel for den behandlingsansvarlige til å holde folk unna, og unngå flest mulig forespørsler om innsyn m v.

På denne bakgrunn mener utvalget at det klare utgangspunktet må være at all praktisering av de individuelle personverngarantiene i utgangspunktet ikke skal koste den registrerte noe. Innsyn må i utgangspunktet være en driftsutgift for den behandlingsansvarlige. Samtidig medgir utvalget at det kan oppstå situasjoner der praktiseringen av rettigheter etter loven kan bli så omfattende og tidkrevende at det kan oppstå uakseptable belastninger for enkelte behandlingsansvarlige. Utvalget mener derfor det er grunn til å åpne opp for at det i forskrift kan gis regler om betaling i slike spesielle tilfelle.

KAPITTEL12

Regulering og kontroll**12.1 OVERSIKT**

Lovregler som gir uttrykk for hvordan personopplysninger kan brukes (materielle regler) gir ikke i seg selv gode nok garantier for at bruk av personopplysninger skjer på en tilstrekkelig forsvarlig måte. I en del tilfeller er det derfor nødvendig å supplere lovens generelle regler med andre styringsmekanismer, som f.eks. krav om tillatelse for behandling av personopplysninger og hjemmel for kontrollordninger. I tillegg er det veldig viktig med gode opplysningstiltak og effektiv veiledning om hvilke regler som gjelder.

Problemstillingene knyttet til valg av regulerings- og kontrollordninger har forbindelseslinjer til flere andre temaer i denne utredningen. Stillingen til organet som skal stå for regulering og kontroll i praksis, Datatilsynet, behandles i "*Tilsynsmyndigheten*" i kapittel 18, mens de administrative og økonomiske konsekvensene av de regulerings- og kontrollordningene utvalget foreslår fremgår av "*Økonomiske og administrative konsekvenser av utvalgets forslag*" i kapittel 20. Enkelte materielle regler omtales i dette kapitlet (se 12.5.7), se forøvrig "*Individuelle personverngarantier*" i kapittel 11.

Kapittel 12 er bygget opp slik at det først gis en redegjørelse for gjeldende rett (12.2) og internasjonale regler (12.3), og deretter følger utvalgets vurderinger i 12.5.

12.2 GJELDENDE RETT**12.2.1 Personregisterlovens konsesjonsordning***12.2.1.1 Hovedregel – konsesjonsplikt*

Loven etablerer en konsesjonsordning for etablering av personregistre. Konsesjonsplikten er regulert i § 9. Det kreves samtykke fra Kongen (konsesjon) for opprettelse av alle personregistre som skal gjøre bruk av edb. I tillegg kreves konsesjon for opprettelse av manuelle personregistre som inneholder sensitive opplysninger. Øvrige personregistre (manuelle registre uten sensitive personopplysninger) er ikke konsesjonspliktige, men er regulert av de alminnelige reglene i personregisterloven. Hva som er sensitive opplysninger i lovens forstand fremgår av § 9 første ledd nr 1-5. Det dreier seg om opplysninger om rase, politisk eller religiøs oppfatning, kriminalitet, helse, seksuelle forhold eller opplysninger om enkelte familieforhold.

Konsesjonsmyndigheten er delegert til Datatilsynet ved kgl. res. av 21. desember 1979.

Når Datatilsynet gir konsesjon for opprettelse av personregistre skal det også fastsettes vilkår etter § 11. Vilkårene skal bestemme hvilke typer opplysninger registeret kan inneholde, og hva registeret kan brukes til. Det kan også settes andre vilkår som har betydning for bruken av registeret eller som kan begrense de ulemperne opprettelsen og bruken av registeret ellers kunne medføre.

Konsesjonsspørsmålet avgjøres ved en interesseavveining. Personverninteresser veies opp mot interessene bak opprettelsen av registeret. Personregisterloven § 10 sier at det skal «vurderes om opprettelse og bruk av personregisteret kan volde problemer for den enkelte som ikke kan løses tilfredsstillende ved regler etter § 11. Dersom slike problemer kan oppstå, må det overveies om de blir oppveid av hensyn

som taler for at registeret blir opprettet.» Dette gir Datatilsynet en meget vid skjønnsmyndighet.

På grunn av den mengden personregistre som opprettes og den omfattende konsesjonsplikten personregisterloven i dag fastsetter har Datatilsynet på mange områder utarbeidet typekonsesjoner. Disse trer i stedet for individuelt utarbeidede konsesjoner i det enkelte tilfellet. Noen eksempler på områder hvor det er gitt standardkonsesjoner er:

- Virksomhetskonsesjon – adresserings- og distribusjonsvirksomhet
- Virksomhetskonsesjon – databehandlingsvirksomhet
- Virksomhetskonsesjon – kredittopplysningsvirksomhet
- Virksomhetskonsesjon – adresserings- og distribusjonsvirksomhet
- Klientregistre under lov om sosiale tjenester
- Reisebyråets kunderegister
- Legens pasientregister
- Lyd- og billedopptak
- Kirkegårdsregister
- Barneverntjenestens klientregister

Det finnes også en rekke andre standardkonsesjoner. Innenfor forskning har Datatilsynet utarbeidet rammekonsesjoner som setter visse generelle vilkår. Mer detaljerte vilkår blir individuelt tilpasset i en tilleggskonsesjon for det enkelte forskningsprosjektet. I praksis har dette fungert som en forskriftsregulering, men konsesjonene har ikke vært behandlet etter reglene for forskrifter i forvaltningsloven kapittel VII.

12.2.1.2 Unntak fra konsesjonsplikten

12.2.1.2.1 Forskriftsregulerte personregistre

For å unngå en rutinemessig konsesjonsbehandling av en stor mengde like registre og registre som er trivielle ut fra et personvernssynspunkt, har en funnet det nødvendig å innsnevre området for konsesjonsplikten i forhold til ordlyden i § 9. I personregisterforskriften "*Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte*" i kapittel 2 er det derfor gitt en rekke fritak fra konsesjonsplikten etter personregisterloven § 9 annet ledd i kombinasjon med diverse materielle bestemmelser. Også for disse registrene gjelder imidlertid de alminnelige reglene i lovens kapittel 2 og 3. Følgende registre er fritatt fra konsesjonsplikt etter forskriften:

- foreningers medlemsregistre (§ 2-2)
- kunde-, abonnent- og leverandørregistre (§ 2-3)
- kunderegistre i banker og finansinstitusjoner (§ 2-4)
- katalogfirmaregistre (§ 2-5)
- leietaker- og sameieregistre (§ 2-6)
- registre for utsendelse av trykksaker o.l. (salgsstøttereregistre) (§ 2-7)
- katalog-, låner- og utlånsregistre (§ 2-8)
- advokaters, revisorers og fonds- og eiendomsmegleres klientregistre (§ 2-9)
- legers, tannlegers, psykologers og annet godkjent helsepersonells registre (§ 2-10)
- aksjeeierregistre (§ 2-11)
- personalregistre (§ 2-12)
- forlagenes personregistre for utgivelse av leksika (§ 2-13)
- dags- og ukepressens personregistre (§ 2-14)
- registre over offentlige representanter (§ 2-15)
- protokollføring av mekling (§ 2-16)

- forskningsregistre (§ 2-17)
- domstolenes registre (§ 2-18)
- elektronisk arkiv (§ 2-19)
- aktivitetslogg i et edb-system eller datanett (§ 2-20)
- personregistre som utleveres elektronisk (§ 2-21)

Det er i forskriften gitt nærmere vilkår for konsesjonsfritakene.

12.2.1.2.2 Personregistre opprettet med hjemmel i lov

En rekke personregistre innenfor offentlig forvaltning er opprettet ved egen lov (f eks Strafferegisteret, se nærmere "*Sikring av personopplysninger*" i kapittel 15). Slike registre er fritatt for konsesjonsplikt etter personregisterloven § 41. Andre bestemmelser i personregisterloven (f eks om innsyn) vil imidlertid også gjelde for disse registrene så sant ikke avvikende regler er fastsatt i eller i medhold av i hjemmelsloven. Iht § 41 skal det også for disse registrene fastsettes regler etter personregisterloven § 11, i den utstrekning det ikke er fastsatt noe annet i eller i medhold av hjemmelsloven.

12.2.1.2.3 Personregistre unntatt fra lovens anvendelsesområde

Iht kgl res 21 desember 1979 er enkelte personregistre unntatt fra lovens anvendelsesområdet (bøker, tidsskrifter el l som etter personregisterloven § 1 er personregistre eller inneholder personregistre – og som er publisert før lovens ikrafttredelse). Bruken av disse registrene er ikke underlagt lovregulering.

12.2.2 Meldeplikt

Med hjemmel i personregisterloven § 36 tredje ledd er det i forskrift av 21 desember 1979 "*Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger*" i kapittel 8 gitt nærmere regler om overføring av personopplysninger til utlandet. Forskriften § 8-1 første ledd erstatter den plikt til å innhente samtykke som oppstilles i personregisterloven § 36 med en meldeplikt. Forskriften gir Datatilsynet hjemmel til å nekte eller sette vilkår for overføringen, jf første ledd tredje punktum.

Overføringen skal meldes til Datatilsynet på fastsatt skjema «i god tid» før overføringen finner sted, jf forskriften § 8-1 første ledd annet punktum. Hva som kan antas å ligge i begrepet «i god tid» kan variere fra sak til sak, men hovedsynspunktet må være at Datatilsynet skal ha rimelig tid til å sette seg inn i saken slik at overføringen eventuelt kan nektes eller det kan knyttes vilkår til overføringen. Det antas imidlertid ikke å foreligge noen plikt for den meldingspliktige til å avvente noen aksept fra Datatilsynet (jf Eva I E Jarbekk; Personvern og overføring av personopplysninger til utlandet, Complex 4/96, TANO, Oslo 1996). Når Datatilsynet trenger ekstra tid for å behandle en melding, kan imidlertid tilsynet kreve at overføringen utsettes mens saken behandles. I slike tilfeller foreligger det en plikt til å avvente Datatilsynets avgjørelse.

Det er fastsatt unntak fra meldeplikten når Norge har plikt til å foreta slik overføring etter folkerettslig overenskomst eller som følge av medlemsskap i internasjonal organisasjon, jf § 8-1 annet ledd.

12.2.3 Materielle regler

Gjennom personregisterlovens konsesjonssystem er Datatilsynet tildelt omfattende myndighet mht å avgjøre hvilke opplysninger et personregister kan inneholde og hva registeret kan brukes til m v (personregisterloven § 11). Loven har imidlertid også enkelte materielle regler. Med materielle regler menes regler som direkte gir uttrykk for hvordan personopplysninger kan eller ikke kan brukes; f eks §§ 6 og 17. Først og fremst er imidlertid slike bestemmelser gitt i forskrifter til loven (f eks forskrift av 21 desember 1979 som fritar enkelte typer personregistre fra konsesjonsplikt under visse gitte vilkår). Bestemmelsene omtales ikke nærmere her.

12.2.4 Rådgivning

I personregisterloven § 3 annet ledd heter det i nr 2 at Datatilsynet skal «gi råd og rettleiing om spørsmål om personvern og datasikring til dem som planlegger å opprette personregistre», og i samme paragraf nr 4 plikter Datatilsynet «etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om bruk av personregistre eller generelle spørsmål som gjelder bruk av personopplysninger».

12.2.5 Annen kontroll

Personregisterloven § 5 gir Datatilsynet vid hjemmel til å gjennomføre ulike kontrolltiltak. I motsetning til konsesjon, som er en forhåndsgodkjenning, er meningen med kontroll etter § 5 å undersøke om lovens bestemmelser og vedtak i medhold av denne faktisk blir fulgt. Datatilsynet kan kreve tilgang til opplysninger uhindret av regler om taushetsplikt, og kan kreve adgang til steder der personregistre, billedopptak (jf loven kapittel 9 a) og tekniske hjelpemidler finnes. Personalet på stedet har bistandsplikt overfor Datatilsynets medarbeidere. Datatilsynets kompetanse er mindre vidtgående enn den kompetanse som tilkommer politi- og påtalemyndighet etter straffeprosesslovens regler om tvangsmidler. Tilsynet kan for eksempel ikke ta beslag i dokumenter eller registre. Datatilsynet kan heller ikke selv foreta sletting (men det kan gis pålegg om sletting etter § 8, som deretter eventuelt kan følges opp med anmeldelse dersom pålegget ikke etterkommes).

12.3 INTERNASJONALE REGLER

12.3.1 Europarådskonvensjonen

Konvensjonen artikkel 4 nr 1 fastslår at det skal treffes tiltak for å gjennomføre hovedprinsippene for datavern i konvensjonen kapittel II. Videre følger det av artikkel 10 at partene plikter å innføre hensiktsmessige kontrollordninger for brudd på hovedprinsippene for datavern i konvensjonen kapittel II. Endelig krever artikkel 6 at spesielle kategorier av personopplysninger bare kan behandles dersom lovgivningen gir «tilstrekkelig» vern.

Vurderingen av hva som er «hensiktsmessig» kontroll og «tilstrekkelig» vern er overlatt til det enkelte land.

12.3.2 EF-direktivet

12.3.2.1 Hovedregel – meldeplikt

Artiklene 18 og 19 gjelder meldeplikten til tilsynsmyndigheten. Her etablerer direktivet en tilsynsordning hvor hovedregelen er meldeplikt til tilsynsmyndigheten for all elektronisk behandling av personopplysninger. Manuell behandling omfattes

ikke av meldeplikten. Iht artikkel 18 nr 5 kan imidlertid medlemsstatene bestemme at også enkelte eller alle manuelle behandlinger skal være underlagt meldeplikt eller en forenklet form for meldeplikt. Direktivet åpner for at medlemsstatene kan gjøre en rekke unntak fra dette utgangspunktet i artikkel 18 nr 2, 3 og 4 (forenklet eller ingen meldeplikt). Direktivet pålegger videre en strengere kontroll (konsesjonsplikt) for visse behandlinger i artikkel 20.

Artikkel 19 bestemmer hvilke opplysninger som minst skal gis til tilsynsmyndigheten (se "*Innholdet i meldingen*" i avsnitt 12.5.4.3). Det er opp til medlemsstatene å gi regler om hvordan endringer i de innmeldte opplysningene skal meldes, jf artikkel 19 nr 2.

12.3.2.2 Unntak fra meldepliktsordningen

12.3.2.2.1 Forenklet meldeplikt eller ingen meldeplikt

Artikkel 18 nr 2 gir medlemsstatene adgang til å bestemme at behandlinger hvor det ikke er sannsynlig at de registrertes rettigheter eller friheter krenkes, kun underlegges en forenklet meldeplikt, eller fritas helt fra meldeplikten. Slik forenklet eller fritakelse fra meldeplikt forutsetter at medlemsstatene fastsetter bestemmelser om behandlingens formål, hvilke opplysninger eller typer opplysninger som behandles, hvilke registrerte eller kategorier av registrerte det er snakk om, hvem opplysningene kan videregis til, samt hvor lenge opplysningene kan oppbevares.

Alternativt (eventuelt i tillegg) kan medlemsstatene utpeke en person (f eks en dataombudsman) som får i oppgave å sikre at de registrertes rettigheter og friheter ikke krenkes som følge av behandlingen. Denne personen skal bl a ha til oppgave å kontrollere at den nasjonale lovgivningen som er gitt i medhold av direktivet følges opp, samt å føre et register over de behandlinger som gjøres av den registeransvarlige. Registeret skal inneholde opplysninger som angitt i artikkel 21 nr 2.

Medlemsstatene kan videre, iht artikkel 18 nr 3, bestemme at meldeplikten ikke skal gjelde for behandlinger som har som formål å føre et register som i henhold til lov eller administrative bestemmelser skal være offentlig tilgjengelig generelt eller for personer som kan godtgjøre å ha en slik legitim interesse. Dette vil for eksempel omfatte Løsøreregisteret og Elektronisk grunnbok. Disse registrene omfattes i dag av konsesjonsfritaket i personregisterloven § 41. Fritaket etter § 41 er imidlertid videre enn etter direktivet fordi det ikke oppstilles noe krav om at opplysningene i registeret skal være offentlig tilgjengelig.

Endelig kan det etter direktivet gjøres unntak fra meldeplikten for den typen behandlinger som er omhandlet i artikkel 8 nr 2 litra d) (intern behandling av sensitive opplysninger i en stiftelse, forening eller annet allmennyttig organ), jf artikkel 18 nr 4.

12.3.2.2.2 Konsesjonsplikt eller lovregulering

Medlemsstatene pålegges å sikre at det skal være adgang til å kontrollere behandling av personopplysninger som potensielt innebærer *særlig risiko* for enkeltpersoners rettigheter før behandlingen settes i verk (dvs en konsesjonsordning), jf artikkel 20. Det er opp til medlemslandene å fastsette hvilke behandlinger som antas å innebære en slik særlig risiko.

Den forutgående kontrollen foretas av tilsynsmyndigheten etter mottatt melding fra den behandlingsansvarlige, eller den foretas av den personen som i virksomheten er utpekt til å ha ansvaret for personvernet (en type «persondataombud»). Vedkommende skal i tvilstilfelle høre tilsynsmyndigheten.

Kontrollen kan også bestå i at de aktuelle typer behandlinger reguleres i nasjonal lovgivning, jf artikkel 20 nr 3.

12.4 FØYENUTREDNINGEN

Spørsmålet om reguleringsformer ble sist vurdert i 1987 i forbindelse med regjeringens og Stortingets behandling av Føyenutredningen.

Et hovedspørsmål i Føyenutredningen var hvilken reguleringsform man burde bygge på i framtiden. Føyen mente at det beste alternativet for regulering av bruk av personopplysninger var det som var lovfestet i personregisterloven, men at en slik ordning forutsatte en vesentlig økning av Datatilsynets bemanning. Hvis dette ikke skjedde, mente Føyen at man burde gå bort fra konsesjonsbehandlingen for personregistre og i stedet ha flere materielle normer i loven. Datatilsynet burde i så fall gjøres til et organ med flere ombudsliknende oppgaver og en viss myndighet til å gi forbud og påbud.

Under *høringsrunden* gikk mange instanser inn for å beholde konsesjonsordningen. Det ble bl a pekt på at konsesjonsordningen sikrer en grundig forhåndsvurdering av registrene, at den gir impulser til kritisk vurdering av bruken av personopplysninger og at publikum får tillit til registerførerene (jf Ot prp nr 34 (1986-87) s 11 – 12). De av høringsinstansene som gikk inn for en innsnevring av eller avskaffelse av konsesjonsordningen, begrunnet dette med at det ville være en forenkling. Under høringen kom det for øvrig frem motforestillinger mot det alternative forslag som Føyen la fram, og som i stor grad bygde på flere materielle bestemmelser i loven. Hovedargumentet var at slike regler lett ville bli for vage og generelle, samtidig som de ikke ville passe for alle typer virksomheter.

Justisdepartementet kom til at man ikke burde foreslå å gå bort fra konsesjonsordningen for personregistre. Det ble lagt vekt på konsesjonsordningens fordeler, og på at Datatilsynet selv ønsket å beholde en konsesjonsordning uavhengig av om personalressursene ble økt. Endelig ble det vektlagt at større endringer i reguleringsformen ville medføre atskillig merarbeid, og at dette tilsa varsomhet med å foreta større endringer så lenge det var usikkert om den nye ordningen ville innebære en bedring (jf Ot prp nr 34 (1986-87) s 13 – 14).

I Stortinget var *Justiskomiteen* enig i at konsesjonsordningen burde opprettholdes. Komiteen pekte bl a på at konsesjonsordningen bidrar til god kommunikasjon mellom de registeransvarlige og Datatilsynet, og at Datatilsynet bedre er i stand til å følge den tekniske og administrative utviklingen på nært hold (jf Innst O nr 64 for 1986-87 s 3 – 4).

12.5 UTVALGETS VURDERINGER

12.5.1 Overordnete hensyn og målsettinger

Selv om EF-direktivet og andre internasjonale regler legger visse føringer på hvordan reguleringen av behandling av personopplysninger skal skje (se ovenfor), er det enkelte land gitt betydelig frihet til selv å treffe rettspolitiske valg om hvilke reguleringsmetoder som bør benyttes, og til å bestemme det nærmere forholdet mellom disse. Utvalget vil her kort peke på visse overordnede hensyn og målsettinger ved utformingen av regulerings- og kontrollsystemet. Den nærmere avveiningen av disse hensynene knyttes til en vurdering av de ulike regulerings- og kontrollmetodene, se nedenfor 12.5.2 – 12.5.9.

Ett gitt utgangspunkt er å ivareta de ulike personverninteressene (jf 3.3 og 3.4) på en god måte. Ønsket om å realisere denne målsettingen kan imidlertid ikke ses isolert – også andre hensyn må tas i betraktning. Denne avveiningen må først og

fremst skje i utformingen av lovens materielle regler, men har også en side til valget av reguleringsmetoder. Utvalget har sett det særlig viktig å utforme reguleringen slik at den skaper tillit. Tillit er viktig i tre relasjoner. For det første er det viktig at borgerne har tillit til at behandling av personopplysninger skjer på en forsvarlig måte. Det er derfor svært viktig med tillit mellom den registrerte og den behandlingssansvarlige. Tillit er også viktig i forholdet mellom de registrerte og tilsynsorganet, samt i forholdet mellom tilsynsorganet og de det føres tilsyn med. For å unngå unødig polarisering og sikre tilsynsorganets legitimitet ser utvalget det som formålstjenlig at kontroll og annen myndighetsutøvelse suppleres med rådgivning og andre former for veiledning. Endelig er det viktig at reguleringen og kontrollen er effektiv og ikke fremstår som unødig omfattende.

12.5.2 Behov for bredt spekter av virkemidler

Personregisterloven gjør i dag bruk av flere reguleringsformer, ved at den kombinerer en omfattende konsesjonsplikt med materielle normer, rådgivning og etterfølgende kontroll (se nærmere ovenfor 12.2 om gjeldende rett). Utvalget foreslår at man også i fremtiden benytter flere ulike reguleringsmåter. Konsesjonspliktordningen foreslås videreført, men blir mindre omfattende enn i dag (se 12.5.5) og avløst av en rekke tiltak som bl a er fundert på en meldeplikt (12.5.4) i kombinasjon med mer vidtrekkende tilsynsoppgaver fra Datatilsynet. Utvalget foreslår dessuten at Datatilsynet som i dag skal ha rett og plikt til å gi råd til dem som planlegger å behandle eller allerede behandler personopplysninger, samt til å gjennomføre etterfølgende kontroller (12.5.6). Også materielle regler bør stå sentralt i reguleringen, og utvalget foreslår at denne reguleringsformen benyttes i større grad enn i dagens lov (12.5.7). Det vil dessuten som i dag være behov for regulering i forskrift (12.5.3). Videre foreslås regler om internkontroll (12.5.8), og endelig har utvalget vurdert bransjevise atferdsnormer (dvs retningslinjer vedrørende personvern som er utarbeidet av de behandlingsansvarlige selv), se 12.5.9.

Utvalget vil understreke behovet for å se de ulike typene reguleringsformer i sammenheng. Det er ikke slik at meldeplikten er ment å erstatte dagens konsesjonsplikt. Men det er utvalgets syn at innføringen av en meldeplikt sammen med frigjorte ressurser til tilsynsmyndighetens rådgivnings- og kontrollvirksomhet, samt innføringen av mer detaljerte materielle regler som direkte gir uttrykk for hvordan personopplysninger kan eller ikke kan brukes *tilsammen* vil sikre et godt personvern for den registrerte, og vil minske behovet for en så omfattende konsesjonsplikt som loven har i dag. Utvalget antar at *antallet* konsesjoner/meldinger etter den nye loven ikke vil bli mer omfattende enn dagens konsesjonsordning, mens den totale arbeidsbelastningen for tilsynet i tilknytning til konsesjons- og meldeplikt vil bli vesentlig redusert, se "*Økonomiske og administrative konsekvenser av utvalgets forslag*" i kapittel 20.

12.5.3 Kort om forholdet mellom lov og forskrift

Utvalget har lagt stor vekt på at en ny lov i større grad enn personregisterloven skal gjenspeile den reelle reguleringen av personopplysninger. En så generell lov som lovforslaget legger opp til må likevel suppleres av forskrifter slik at reguleringen sett under ett tilfredsstillende krav til nyanser og presiseringer, og lovforslaget inneholder en rekke forskriftshjemler. Enkelte av forskriftene må foreligge allerede når loven trer i kraft, mens andre kan utarbeides dersom det viser seg å være behov for dem.

Det er viktig at forskriftene til enhver tid er mest mulig oppdaterte. Det kan på denne bakgrunn være hensiktsmessig å vurdere om Kongens forskriftskompetanse på enkelte områder bør delegeres til Datatilsynet (for eksempel forskrift om internkontroll og utforming av meldeskjemaet). I vurderingen må det legges vekt på at forskriftsverket er det styringsverktøyet regjeringen har når Datatilsynet blir faglig uavhengig regjeringen og departementet.

12.5.4 Meldeplikt

12.5.4.1 Meldeplikt som virkemiddel

Meldeplikt kjennetegnes ved at den som ønsker å sette i gang en viss form for behandling av personopplysninger, må orientere tilsynsorganet før behandlingen iverksettes. Meldeplikten åpner for at tilsynsmyndigheten (på bakgrunn av meldingen) kan gripe inn og treffe vedtak eller på annen måte kommunisere med den som melder fra, men ordningen forutsetter ikke noen obligatorisk oppfølging av meldingen. Hvor langt tilsynsmyndigheten vil gå i å behandle meldingene, må langt på vei avgjøres av tilsynsmyndigheten selv. Et annet kjennetegn ved meldeplikten er at behandlingen som utgangspunkt kan sette igang uten at det foreligger noen tillatelse på forhånd. Et eventuelt vedtak fra tilsynsmyndigheten om at behandlingen krever konsesjon eller på annen måte er ulovlig, vil som regel bli fattet først etter at behandlingen har pågått i noen tid.

I motsetning til EF-direktivet, der meldeplikt er hovedregelen (artikkel 18), er meldeplikt i dag kun benyttet i ett tilfelle i personregisterloven, se ovenfor 12.2.2 om meldeplikt ved overføring av personopplysninger til utlandet. Vi har derfor i Norge svært begrenset erfaring med bruk av meldeplikt. Erfaringer fra andre land er delte. Det første gjelder også for erfaringer med meldepliktordninger på andre samfunnsområder, som f.eks. innen plan- og bygningsretten og konkurranseretten. En vurdering av fordeler og ulemper med en meldepliktsordning på det foreliggende sakfeltet må derfor nødvendigvis tuftes på et mindre fundert grunnlag enn vurderingen av konsesjonsplikten ovenfor.

For det første synes på det rene at en meldeplikt vil binde opp atskillig mindre arbeidskapasitet hos Datatilsynet enn en konsesjonsordning. Den frigjorte arbeidskapasiteten kan i stedet benyttes til krevende konsesjonssaker eller til andre reguleringsmåter som for eksempel rådgivning. Ettersom det i mindre grad vil finne sted en oppfølging av den enkelte melding, kan også saksbehandlingsrutinene gjøres mer fleksible enn i dag. Meldingene vil videre etterhvert utgjøre et betydelig erfaringsmateriale, blant annet fordi ny teknologi kan gjøre det mulig å behandle meldinger atskillig mer kostnads- og formåls effektivt enn tidligere.

Samtidig er det klart at meldeplikt har sine klare begrensninger som tiltak. Erfaringene fra meldeplikten i prisloven viser at et system med en omfattende meldeplikt lett kan bli svært tungvint og legge betydelige kostnader på såvel de meldepliktige som på meldingsmottakerne (jf NOU 1991: 27 s 166 flg). Behandlingen eller gjennomgåelsen av meldingene må videre jevnt over bli atskillig mer overfladisk enn en behandlingen av en søknad om konsesjon. Hvis det viser seg at behandlingen var konsesjonspliktig, og ikke bare meldepliktig, kan det dessuten ha oppstått økonomisk tap eller annen og mindre reparerbar skade før tilsynsmyndigheten rekker å gripe inn. Slik er det imidlertid også i dag med registre som det feilaktig ikke søkes om konsesjon for. I tillegg kan det være fare for at den meldepliktige regner manglende reaksjon fra tilsynsorganet som en «godkjenning» av behandlingen, selv om den manglende oppfølgingen skyldes helt andre årsaker, for eksempel manglende ressurser eller prioritering av andre oppgaver. Denne faren

kan imidlertid formentlig i stor grad ryddes av veien gjennom informasjon, f eks på meldeskjemaene.

12.5.4.2 Hvilke behandlingstyper bør være meldepliktige?

EF-direktivet trekker opp rammer for hvilke typer behandlinger som skal være undergitt meldeplikt. Det enkelte land gis imidlertid relativt store muligheter for å tilpasse meldeplikten til nasjonale forhold, se ovenfor under 12.3.2.

Et meldepliktsystem må hvile på de to grunnleggende forutsetningene om at; 1) meldingene skal være nyttige for formålet å fremme personvern og 2) utgiftene knyttet til meldesystemet skal stå i forhold til denne nytten. Utvalget har lagt stor vekt på å unngå at meldeplikten blir utformet slik at den oppfattes som et rituale uten innhold. Det ville være uheldig dersom kvaliteten på opplysningene generelt ble dårlig, og ordningen må derfor legges opp slik at det finnes rutiner for oppdatering av meldingene.

Etter utvalgets syn bør meldeplikten fylle følgende funksjoner:

- Etablere en kontakt mellom Datatilsynet og den behandlingsansvarlige
- Gi grunnlag for å formidle regelinformasjon til de meldepliktige og bidra til å høyne bevissthetsnivået om personvernsspørsmål hos disse
- De samlede meldingene skal utgjøre en vesentlig del av Datatilsynets kunnskapsbasis for tilsynets prioritering av arbeidsoppgaver, særlig i relasjon til kontroll, veiledning og regelverk
- Sikre offentlighet med hensyn til de behandlinger som foretas, se "*Plikt for tilsynsmyndigheten til å føre allment tilgjengelig fortegnelse over meldepliktige og konsesjonspliktige persondatabehandlinger*" i kapittel 11.2.2.

Ved vurderingen av hvilke behandlinger som bør være meldepliktige, har utvalget tatt det samme utgangspunktet som EF-direktivet; meldeplikt for all elektronisk behandling av personopplysninger. I tillegg foreslår utvalget at opprettelse av manuelle sensitive personregistre blir meldepliktig. Det betyr at meldeplikten i utgangspunktet erstatter alle de konsesjonspliktige behandlingene etter dagens lov. På grunn av at registerbegrepet er fjernet som hovedbegrep, blir virkeområdet i utgangspunktet noe videre enn dagens konsesjonsordning. Ettersom målsettingen er at konsesjonsplikten sammen med meldeplikten ikke skal være mer omfattende enn dagens konsesjonsordning, er det behov for å gjøre visse unntak fra utgangspunktet om meldeplikt for all elektronisk behandling. Et eksempel på innsnevringen er behandling av personopplysninger i forbindelse med bruk av vanlig tekstbehandlingsutstyr som heller ikke etter den nye loven bør være omfattet av meldeplikt eller konsesjonsplikt.

Det er i dag i forskrift fastsatt en rekke unntak fra konsesjonsplikten, og utvalget antar at flere av disse unntakene bør videreføres (som unntak fra meldeplikten) i forskrifter til den nye loven (f eks opprettelse av medlemsregistre, enkle former for kunderegistre mv). Behovet for forskriftsregulering av slike typer behandlinger må imidlertid antas å bli langt mindre etter den nye loven i og med at behandlingene vil være underlagt mer detaljerte regler i loven. Utvalget forutsetter at det blir økt bruk av bransjevisse atferdsnormer, og at behandlingene vil være underlagt regler om internkontroll. Det forutsettes også at Datatilsynet vil få mer ressurser til å drive aktivt tilsyn med de som behandler personopplysninger.

12.5.4.3 Innholdet i meldingen

EF-direktivet fastsetter i artikkel 19, bokstavene a) til f) at følgende opplysningselementer skal innhentes fra de meldepliktige:

- Navn og adresse på behandlingsansvarlige og eventuelt dennes representant
- Behandlingens formål
- En beskrivelse av kategorier av registrerte personer og opplysningstyper
- Hvem opplysninger videregis til
- Planlagt overførsel av opplysninger til tredjeland
- En beskrivelse av behandlingssikkerheten

Direktivet forutsetter at det blir etablert rutiner for oppdatering av disse opplysningstypene. Et virkemiddel for å sikre kvalitet og oppdaterte opplysninger vil være å gjøre meldingen tidsbegrenset, slik at ny melding må sendes etter en viss tid.

Meldinger med et slikt innhold vil imidlertid ikke uten videre være av særlig verdi for Datatilsynet. Forutsetningen for at meldingene skal bli nyttige, er særlig at opplysningene gir grunnlag for å prioritere innsatsen innen rettsinformasjon, veiledning og kontroll. Det er derfor viktig at meldingene gir en beskrivelse av de viktigste indikatorer for personverntrusler (for eksempel om grunnlaget for behandlingen, måten opplysningene blir hentet inn på, om det benyttes lukket eller åpent system, om det eksisterer faste rutiner for ivaretagelsen av den enkeltes rett til innsyn, retting, sletting og supplering mv). Det er også viktig at det på meldingene gis til en viss grad formaliserte opplysninger slik at det er mulig å skille ut kategorier av behandlinger. Utvalget antar på denne bakgrunn at det vil være nødvendig å supplere og detaljere de opplysninger som er regnet opp i direktivet, se merknadene til lovforslaget § 32.

12.5.4.4 Behandlingen av meldingene

Et problem med dagens omfattende konsesjonsordning er at det binder mye arbeidskapasitet hos Datatilsynet. Overgangen til et system med meldeplikt i kombinasjon med en mer begrenset konsesjonsordning bør derfor samlet sett føre til en klart redusert arbeidsmengde for Datatilsynet sammenlignet med dagens konsesjonssystem. En slik omlegging med mindre «pliktmessig» saksbehandlingssarbeid, vil legge forholdene til rette for langt mer omfattende tilsyns- og veiledningsvirksomhet enn i dag. Dette forutsetter at meldepliktordningen legges opp slik at behandlingen av meldingene blir vesentlig mindre arbeidskrevende enn dagens behandling av konsesjonssøknader. Den største forskjellen mellom konsesjonsplikt og meldeplikt vil for den behandlingsansvarlige være at man ved en meldeplikt ikke behøver å avvente et samtykke fra Datatilsynet. Den som har sendt meldingen kan likevel motta en kvittering for at meldingen er mottatt, men kvitteringen innebærer ikke noen stillingtagen til innholdet i meldingen. Den behandlingsansvarlige har selv risikoen for at virksomheten er lovlig. Se forøvrig "[Omleggingen av konsesjonsordningen – meldeplikt](#)" i avsnitt 20.3.2 hvor det administrative opplegget for en meldepliktsordning er nærmere skissert.

12.5.5 Konsesjonsplikt

12.5.5.1 Konsesjonsplikt som reguleringsform

Ved at det kreves en tillatelse før behandlingen av personopplysninger kan finne sted, sikres man for det første – i motsetning til kontroll ved eget tiltak – at saken presenteres for tilsynsmyndigheten. For det andre kan konsesjonsbehandling føre til en grundig individuell vurdering av om konsesjon skal gis eller ikke. Dette

avhenger av i hvilken grad konsesjonsbehandlingen er standardisert, og vil som regel forutsette at konsesjonsplikten ikke er for omfattende (jf dagens ordning med omfattende konsesjonsplikt og relativt utbredt bruk av rammekonsesjoner). Ettersom vurderingen av behandlingen skjer *før* behandlingen finner sted, hindres det at det oppstår skade eller andre uheldige virkninger som senere må repareres. Dette vil være kostnadsbesparende. Ved at det kan stilles vilkår i konsesjonen, gis også tilsynsmyndigheten mulighet til en fleksibel og smidig regulering. Datatilsynet har dessuten gjennom en årrekke ervervet betydelig erfaring om bruk av konsesjoner, og det er hensiktsmessig at disse erfaringene kommer til nytte også i tiden fremover.

På den annen side kan en konsesjonsordning være forbundet med klare ulemper. For det første kan ordningen binde opp arbeidskapasitet, slik at det blir for få ressurser til andre reguleringsformer, som for eksempel rådgivning og annen kontroll. For det andre tar konsesjonsbehandling relativt lang tid, noe som kan virke frustrerende for søkerne og fremstå som unødig omstendelig. Dette kan få uheldige samfunnsmessige konsekvenser.

Utvalget foreslår på denne bakgrunnen at konsesjon kun benyttes der hensynet til personvernet gjør det sterkt ønskelig med en grundig forhåndsvurdering av personvernkonsekvensene av en planlagt behandling. En slik løsning er i tråd med EF-direktivet artikkel 20 (se ovenfor 12.3.2). Den nedre grensen for hvilke behandlinger som skal undergis konsesjonsplikt vil samtidig utgjøre den øvre grensen for meldeplikt.

12.5.5.2 Hvilke behandlingstyper bør undergis konsesjonsplikt?

12.5.5.2.1 Innledning

Utvalget mener at det kun er de behandlinger som typisk kan forventes å representere en særlig stor trussel for personvernet som bør undergis konsesjonsplikt, jf også EF-direktivet artikkel 20 nr 1 («særlig risiko»).

Etter dagens regler er opprettelse av personregistre alltid konsesjonspliktig dersom det brukes elektroniske hjelpemidler. Med den teknologiske utviklingen som har funnet sted de siste årene, er dette etter utvalgets syn en lite hensiktsmessig regel. En rekke personregistre som enten ikke er eller i svært liten grad kan sies å være en fare for personvernet, er underlagt konsesjonsplikt. Eksempler på slike registre er ulike foreningers medlemsregistre, aksjeeierregistre og leietaker- og sameiereregistre. Disse er i utgangspunktet konsesjonspliktige, men er alle fritatt fra konsesjonsplikt i henhold til forskrifter til personregisterloven. Det er imidlertid også en rekke elektroniske registre som ikke er egnet for typeregulering i forskrift (f.eks. fordi antallet er lite), men hvor konsesjonsplikt åpenbart er en lite hensiktsmessig og unødig ressurskrevende reguleringsform. Eksempler på slike registre er septiktankregisteret, laksefiskere i sjø i Nordland og leverandørregisteret for slakt. Utvalget ser det som hensiktsmessig dersom konsesjonsplikten kan avgrenses mer presist slik at behovet for forskrifter som unntar fra konsesjonsplikt blir mindre.

Ved vurderingen av når det er behov for en særskilt grundig regulering (hvilket EF-direktivet ikke tar stilling til), har utvalget på denne bakgrunn sett hen til særlig to forhold: 1) hvilke typer opplysninger som behandles og 2) hva opplysningene skal brukes til. Utvalget foreslår for øvrig at man viderefører dagens ordning med at Kongen kan unnta visse former for behandling av personopplysninger fra konsesjonsplikt.

12.5.5.2.2 *Skillet mellom manuell og elektronisk behandling*

Etter utvalgets syn bør elektroniske og manuelle behandlinger som hovedregel likestilles. Det vil si at i den grad kriteriene nedenfor tilsier at behandlingene bør være konsesjonspliktig, gjelder dette uavhengig av om behandlingen skjer elektronisk eller manuelt (såfremt de opplysningene som inngår i den manuelle behandlingen inngår eller skal inngå i et personregister). Riktignok gir manuelle registre i utgangspunktet ikke den samme muligheten for effektiv utlevering og gjenbruk av opplysninger som de elektronisk lagrede opplysningene, og slike registre har tradisjonelt derfor ikke vært ansett for å representere den samme faren for personvernet. Med dagens muligheter til effektivt å scanne inn manuelt lagrede opplysninger blir det imidlertid liten forskjell mellom de to lagringsformene. Utvalget antar at det avgjørende bør være personopplysningenes innhold og hva de brukes til – uavhengig av hvilken teknologi som benyttes. En slik løsning forhindrer også en adgang til omgåelse av konsesjonsplikten ved å velge manuell registrering fremfor elektronisk.

12.5.5.2.3 *Personopplysningenes innhold*

I likhet med dagens ordning mener utvalget at det kan være behov for særskilt betryggende regulering av behandling av personopplysninger som kan karakteriseres som *sensitive*, jf personregisterloven § 9 annet ledd nr 1-5. Direktivet forutsetter også en særskilt regulering av behandling av sensitive opplysninger. Det er imidlertid ikke gitt at behandling av sensitive opplysninger i seg selv *alltid* skal utløse konsesjonsplikt, slik regelen er i dag for manuelle registre. Dette forholdet må ses i sammenheng med hva formålet med behandlingen er – dvs hva opplysningene skal brukes til, se nærmere om dette nedenfor og videre i merknadene til § 33.

12.5.5.2.4 *Hva skal opplysningene brukes til?*

Det forekommer at behandlingen av personopplysninger munner ut i en avgjørelse som er av så stor betydning for den det gjelder at det er særlig viktig å sikre at opplysningene behandles på en forsvarlig måte (se "[Det beslutningsfokuserte personvernet](#)" i avsnitt 3.3.4 om det beslutningsfokuserete personvernet). Slike hensyn har begrunnet særskilte rettssikkerhetsgarantier på andre områder, jf for eksempel forvaltningslovens saksbehandlingskrav når det skal treffes enkeltvedtak (se forvaltningsloven §§ 2, 3 og kapittel IV – VI).

Utvalget foreslår på denne bakgrunn at behandling av sensitive personopplysninger som kan munne ut i en avgjørelse som er bestemmende for bestemte personers rettigheter eller plikter, skal være konsesjonspliktig. Alle øvrige behandlinger vil i utgangspunktet være meldepliktig dersom de skjer ved hjelp av elektroniske systemer. Det samme gjelder for manuell behandling av sensitive personopplysninger som inngår eller skal inngå i et personregister.

Utvalget har forøvrig vurdert hvorvidt bruk av personopplysninger til et annet formål enn det opplysningene opprinnelig var innsamlet for, kan være et egnet kriterie for grensdragningen mellom meldepliktige og konsesjonspliktige behandlinger. Utvalget har kommet til at dette ikke ville være hensiktsmessig. I stedet foreslår utvalget en ny bestemmelse som begrenser adgangen til å anvende personopplysninger til andre formål enn de som opprinnelig og uttrykkelig var angitt som formål, se merknadene til lovforslaget § 8. Dersom det på et senere tidspunkt er aktuelt å bruke opplysningene til et annet formål utløser dette ny meldeplikt. Dersom det nye formålet er konsesjonspliktig, oppstår det en plikt til å søke ny konsesjon.

12.5.5.3 Særskilt om forskning

12.5.5.3.1 Oversikt

Mange forskningsprosjekter forutsetter opprettelse av personregistre og faller derfor inn under personregisterlovens område. Datatilsynet behandler årlig en rekke søknader i forbindelse med slike prosjekter. Interessen i gode forskningsresultater kan av og til komme i konflikt med grunnleggende personverninteresser (se for eksempel NOU 1993:22 «Pseudonyme helseregistre» "[Personregisterloven med forskrifter](#)" i kapittel 5 som beskriver grunnleggende interesser og verdier ved opprettelse og bruk av helseregistre).

Nedenfor beskrives først dagens ordning (12.5.5.3.2), deretter gis en kort oversikt over hvilke hovedproblemstillinger som reises ved igangsettelse av forskningsprosjekter (12.5.5.3.3), før det til slutt redegjøres nærmere for utvalgets forslag under "[Utvalgets vurderinger](#)" i avsnitt 12.5.5.3.4.

12.5.5.3.2 Dagens ordning

For å ivareta kontakten mellom forskere og Datatilsynet har Norges forskningsråd opprettet Datafaglig sekretariat. Sekretariatet er lagt til Norsk samfunnsvitenskapelig datatjeneste (NSD). Sekretariatet gir informasjon og veiledning og fungerer som et kontaktledd mellom

forskningsinstitusjoner/enkeltforskere og Datatilsynet. Datatilsynet har gitt rammekonsesjoner til Norges forskningsråd, medlemmene av Universitetsrådet og distriktshøgskolene. I følge rammekonsesjonene skal søknad om konsesjon for hvert enkelt forskningsregister sendes til Datatilsynet via Datafaglig sekretariat.

Forskere og studenter som oppretter konsesjonspliktige personregistre må fylle ut et meldeskjema som fås ved henvendelse til Datafaglig sekretariat. Datafaglig sekretariat vurderer, på grunnlag av opplysningene i meldeskjemaet, om forslag til innsamling, tilrettelegging, publisering og oppbevaring av persondata tilfredsstillende krav til personvern som er nedfelt i personregisterloven og den gitte rammekonsesjonen. Sekretariatet skriver sin innstilling/prosjektvurdering som oversendes Datatilsynet for endelig godkjenning. Etter hva utvalget har fått opplyst er det ytterst sjelden at Datatilsynet nekter konsesjon til et forskningsprosjekt som er godkjent av Datafaglig sekretariat.

Når et prosjekt er avsluttet, vil det ofte være ønskelig å oppbevare opplysningene i personidentifiserbar form, for eksempel i påvente av en oppfølgingsundersøkelse. I følge vilkårene for rammekonsesjonene, kan personopplysningene arkiveres ved en godkjent arkivinstitusjon. Norsk samfunnsvitenskapelig datatjeneste er godkjent av Datatilsynet som arkivinstitusjon for persondata. Dersom en forsker ønsker å arkivere opplysningene i personidentifiserbar form, må saken legges frem for Rådet for persondataarkivering. Rådet for persondataarkivering er oppnevnt av Norges forskningsråd i henhold til rammekonsesjonene. Rådet er ledet av en jurist og består av representanter fra ulike fagområder. Datatilsynet møter som observatør. Datafaglig sekretariat utfører sekretærfunksjonen for Rådet.

Rådet skal sikre at den interesse som knytter seg til det aktuelle forskningsprosjektet blir veid mot personverninteressene. Rådet skal også ta standpunkt til eventuell gjenbruk av personopplysninger. Rådets anbefaling oversendes Datatilsynet som har endelig beslutningsmyndighet i arkiverings- og gjenbrukssaker.

Datatilsynet har ikke kompetanse til å dispensere fra taushetsplikten. Dersom opplysningene som ønskes brukt i et forskningsprosjekt er taushetsbelagte, kan imidlertid departementet på visse vilkår bestemme at et forvaltningsorgan kan eller skal gi opplysninger til bruk for forskning uavhengig av organets taushetsplikt etter § 13,

jf forvaltningsloven § 13 d. Søknad om dispensasjon fra taushetsplikten skal som hovedregel sendes det fagdepartement som forvaltningsorganet er underlagt. Når det gjelder helseopplysninger, er imidlertid dispensasjonsadgangen delegert til Statens helsetilsyn.

Forvaltningsloven § 13 e inneholde bestemmelser om forskeres taushetsplikt.

Det er også etablert forskningsetiske komiteer for henholdsvis medisinsk forskning (Nasjonal etisk komité for medisin; NEM) og samfunnsfag og humaniora (Nasjonal etisk komité for samfunnsfag og humaniora; NESH). Komiteene skal veilede og gi råd om forskningsetiske spørsmål, og forskerne skal gi innberetning til komiteene før de starter et forskningsprosjekt. Datatilsynet samarbeider også med de forskningsetiske komiteene, men samarbeidet er ikke formalisert på samme måte som med Datafaglig sekretariat.

12.5.5.3.3 Noen hovedproblemstillinger ved igangsettelse av forskningsprosjekter

Generelt sett finnes det to hovedtyper forskningsprosjekter; prosjekter som forutsetter aktiv deltagelse fra personer og prosjekter som baserer seg på registerforskning. Ulike problemstillinger reises ved disse to hovedtypene forskningsprosjekter.

Ved registerforskning vil en aktuell problemstilling ofte være spørsmål om kobling (samkjøring) av to eller flere registre. Datatilsynet kan gi tillatelse til slike koblinger. Normalt vil en slik tillatelse bli gitt med strenge vilkår om sikkerhet, tidsfrister med mer. Datatilsynet krever vanligvis ikke samtykke fra de registrerte i slike sammenhenger.

I prosjekter hvor det skal være direkte kontakt med personer reises ulike spørsmål knyttet til samtykkeproblematikk. Det kan være uenighet om hva et samtykke bør inneholde og hvordan en samtykkeerklæring bør utformes. Datafaglig sekretariat har utarbeidet en standard taushets- og samtykkeerklæring som er godkjent av Datatilsynet.

12.5.5.3.4 Utvalgets vurderinger

I henhold til kriteriene for konsesjonsplikt angitt ovenfor vil de fleste forskningsprosjekter som innebærer behandling av personopplysninger være meldepliktige (og ikke konsesjonspliktige som i dag). Dette gjelder selv om det forskes på sensitive opplysninger. Ulike forskningsprosjekter reiser imidlertid ofte vanskelige personvernmessige avveininger som bør foretas av andre enn forskeren selv. Datatilsynet vil også for disse persondatabehandlingene ha kompetanse til å gi ulike pålegg som skal sikre personvernet, men dette vil som for de øvrige meldepliktige behandlingene først skje ved en vurdering av prosjektet i etterkant. I noen tilfeller kan det være behov for en vurdering av prosjektet også *før* det igangsettes fordi avveiningen bl a kan gå på om det skal stilles krav til samtykke fra de personer det skal forskes på og eventuelt hvilke krav det skal stilles til samtykkeerklæringen. I og med at forskningen selv har etablert rutiner for at slik forhåndsvurdering skjer (i Datafaglig sekretariat, Nasjonal etisk komité for samfunnsfag og humaniora og Nasjonal etisk komité for medisin), reises ikke det samme behovet for at Datatilsynet i tillegg vurderer de samme spørsmålene. Det er imidlertid svært viktig at Datatilsynet har jevnlig kontakt med disse miljøene og gir råd og veiledning om hvilke krav som bør stilles av hensyn til personvernet. Tilsynet har dessuten kompetanse til å stoppe prosjekter som ikke skjer i samsvar med loven, eller kan knytte vilkår til gjennomføringen av slike prosjekter slik at de på denne måten blir i samsvar med loven.

12.5.5.4 Særskilt om offentlige registre opprettet med hjemmel i lov

Personregisterloven § 41 unntar fra konsesjonsplikt personregistre i organ for stat eller kommune som er opprettet ved egen lov. Begrunnelsen er at når det i lov er bestemt at det skal opprettes et personregister, har Stortinget tatt stilling til spørsmålet, og det er ikke behov for tillatelse fra Datatilsynet i tillegg. Unntaket medfører at en rekke registre ikke krever konsesjon, som for eksempel folkeregisteret og strafferegisteret. Paragraf 41 reiser spørsmål om hvor klar lovhjemmelen må være for at bestemmelsen skal få anvendelse, jf kommentarutgaven til personregisterloven side 91:

«Det er viktig å være oppmerksom på at det ikke er tilstrekkelig at en særlov hjemler en opplysningsplikt, eller en form for saksbehandling, som innebærer at opprettelse av registre er nødvendig. Det skal eksplisitt framgå at det skal eller kan føres et register, men det stilles ikke krav om at det skal være angitt opplysningstyper eller klart definert formål.»

Utvalget foreslår at registrene som nevnt i § 41 ikke undergis noen særregulering i den nye loven. Konsesjon- eller meldeplikt (eventuelt forenklet meldeplikt, se merknadene til § 31) vil gi Datatilsynet den ønskelige oversikt over hvilke handlinger som foretas innen offentlig forvaltning, slik at de kan utøve sin kontroll også her. Dette kan dessuten bidra til å høyne bevissthetsnivået om personvernspørsmål hos den meldepliktige ved at man må vurdere og redegjøre for den hjemmelen man har til å registrere personopplysninger. Videre etableres det en kontakt mellom den registeransvarlige og Datatilsynet og man sikrer offentlighet med hensyn til de personregistrene som opprettes med hjemmel i lov.

Utvalget understreker at konsesjonsvurderingen som regel er mer enn et «ja» eller et «nei», og peker på viktigheten av at også de forvaltningsorganene som ikke behøver konsesjon er i god dialog med Datatilsynet om hvilke løsninger som best fremmer personvernet, samtidig som de oppfyller andre krav til brukervennlighet og effektivitet m v.

12.5.5.5 Vurderingen av om konsesjon bør gis

Bruken av konsesjon reiser ikke bare spørsmål om når det skal være konsesjonsplikt, men også om hva som skal til for at konsesjon skal gis. Som det fremgår av 12.2.1, avgjøres konsesjonsspørsmålet i dag etter en avveining av personverninteresser mot de interesser som begrunner opprettelsen av registeret (jf personregisterloven § 10). Dette gir Datatilsynet en meget vid skjønnsmyndighet.

Det kan imidlertid stilles spørsmålstegn ved om det er formålstjenlig i større grad å klargjøre i lov eller forskrift når søkeren har krav på konsesjon. Stor grad av skjønnsfrihet gir best mulighet til å finne frem til konkret rimelige og riktige avgjørelser, samtidig som forutberegnelighet og likhetshensyn tilsier at avgjørelsesgrunnlaget i størst mulig grad fremgår av lov eller forskrift.

Utvalget vil først understreke at Datatilsynet ikke står fullt så fritt som loven i dag indikerer. For det første vil Datatilsynets egen praksis legge visse føringer på fremtidige avgjørelser, jf forvaltningsprinsippet om lik behandling av like saker. Dernest vil avgjørelser som treffes i klagesaker, og ikke minst de synspunkter som kommer til uttrykk i forbindelse med Stortingsbehandlingen av årsmeldingene, danne retningslinjer for Datatilsynets fremtidige avgjørelser. Spørsmålet blir så om det likevel er grunn til å presisere nærmere i lov eller forskrift når konsesjon kan gis.

Som det fremgår ovenfor foreslår utvalget at konsesjonsordningen skal reserveres for de tilfelle der vanskelige avveininger er påkrevet. Dette innebærer for det første at færre virksomheter enn tidligere må søke konsesjon, hvilket igjen betyr at

færre enn tidligere har behov for å bedømme på forhånd hvor stor sjansen er for å få konsesjon. Utvalget finner imidlertid ikke at dette taler for å unnlate å gi mer presise regler for når konsesjon skal tildeles – selv om antallet avgjørelser blir færre, vil det ofte være av stor betydning for de berørte rettssubjektene å kunne forutberegne sin rettsstilling så godt som mulig. Justeringen av området for konsesjonsplikt har imidlertid en annen og mer relevant konsekvens. Ettersom konsesjon i henhold til utvalgets forslag skal reserveres for tvilsomme og særlig viktige tilfellene, vil avgjørelsen av om konsesjon skal tildeles jevnt over by på vanskeligere og mer kompliserte avgjørelser enn i dag. Dette gjør det meget vanskelig å utforme tilfredsstillende detaljerte generelle regler for hvordan konsesjonsspørsmålet skal bedømmes. Utvalget foreslår at bestemmelsen i personregisterloven § 10 videreføres slik at vurderingen av om konsesjon skal gis fortsatt baseres på en bred interesseavveining.

12.5.6 Rådgivning og kontroll

Utvalget foreslår at dagens regler om rådgivning og kontroll videreføres i den nye loven. Som følge av at mindre ressurser vil benyttes til konsesjonsbehandling, kan disse oppgavene vies enda større oppmerksomhet enn i dag, jf "*Økonomiske og administrative konsekvenser av utvalgets forslag*" i kapittel 20 nedenfor. Dessuten foreslår utvalget regler om internkontroll som også vil lette Datatilsynets kontrollvirksomhet, se 12.5.8.

I og med at utvalget legger opp til en økt kontrollvirksomhet fra Datatilsynets side, kan det stilles spørsmål ved om dette nødvendiggjør granskingsregler utover hva som er fastsatt i forvaltningsloven § 15 for å ivareta rettssikkerheten til dem som blir utsatt for kontroll. Slike regler kan eventuelt fastsettes i forskrift.

12.5.7 Materielle regler

12.5.7.1 Innledning

Med materielle regler menes som tidligere nevnt lovbestemmelser eller forskrifter som direkte gir uttrykk for hvordan personopplysninger kan eller ikke kan brukes. Materielle regler vil også i tiden fremover være et sentralt virkemiddel for å regulere behandling av personopplysninger.

Utvalget foreslår at man i større grad lovfester materielle regler for hvordan behandling av personopplysninger bør skje. Eksempler på slike regler er at behandling av personopplysninger skal være saklig begrunnet, at personopplysninger innsamlet til ett formål ikke uten videre skal benyttes til et annet og at personopplysninger skal slettes når det ikke lenger er saklig grunn for oppbevaring.

12.5.7.2 Begrunnelse for innføring av flere materielle regler

Det er en fare for at materielle regler på personvernlovgivningens område kan bli for vage og generelle, og at det kan være vanskelig å finne regler som passer for alle typer virksomheter, jf 12.4 ovenfor om høringsinstansenes syn på forslagene i Føyenutredningen.

Utvalget har likevel kommet til at loven bør ha flere materielle regler. Begrunnelsen for dette er flerdelt. Dels kan materielle regler være nyttige hjelpemidler ved fortolkningen av lovens øvrige bestemmelser og dels kan de i større grad enn detaljfokuserte regler påvirke holdninger blant regelbrukerne. I tillegg er det etter utvalgets syn hensiktsmessig å på denne måten synliggjøre internasjonale retningslinjer (som for eksempel FNs og OECDs retningslinjer, se "*Oversikt over andre internas-*

jonale reguleringer og andre lands rett" i kapittel 9) som ikke på annen måte eksplisitt nedfeller seg i loven. Datatilsynets erfaring gjennom bruk av konsesjoner kan dessuten på denne måten komme til nytte ved at tidligere konsesjonsvilkår i noen grad kan nedfelles i materielle regler i loven.

Enkelte slike bestemmelser vil måtte utformes såvidt skjønnsmessig at overtredelse ikke egner seg for straffeforfølgning, se nærmere "*Sanksjoner*" i kapittel 19 nedenfor. Datatilsynet gis imidlertid kompetanse til å gi pålegg om at behandling i strid med disse reglene skal opphøre eller stille vilkår for at behandlingen kan fortsette.

I tillegg til disse mer skjønnsmessige reglene foreslår utvalget flere nye bestemmelser som også mer direkte gir uttrykk for hvordan personopplysninger kan eller ikke kan brukes. Disse er ment som vanlige pliktregler hvor brudd på bestemmelsene vil være straffesanksjonert (f eks informasjonsplikt ved innsamling av personopplysninger m v).

12.5.7.3 Noen nye materielle regler

I det følgende gis noen eksempler på noen nye materielle regler som utvalget foreslår. Forøvrig vises det til "*Individuelle personverngarantier*" i kapittel 11 og "*Merknader til de enkelte bestemmelsene*" i 21 hvor flere materielle regler omtales.

12.5.7.3.1 Anvendelse av personopplysninger til et annet formål enn det opprinnelige

Sett fra et personvernsynspunkt er det viktig at behandling av personopplysninger skjer ut fra et definert formål. Jo mer sensitive opplysningene er, og jo mer kvalifisert bruken av opplysningene skal være, desto viktigere er en klar avgrensning av formålet. Når den hvis opplysningene gjelder kjenner formålet, kan vedkommende bistå med korrekte opplysninger i den konkrete sammenhengen og lettere hevde sin interesse i personvern (for eksempel kreve opplysninger rettet eller slettet). Det er dessuten først når man kjenner formålet med behandlingen at det er mulig å vurdere hvilke opplysninger som er relevante (jf relevanskravet i personregisterloven § 6 første ledd som utvalget foreslår videreføres til den nye loven).

Det vil ofte være et ønske fra behandlingsansvarlige eller andre å anvende personopplysninger til andre formål enn det de opprinnelig er innsamlet for. Etersom det registreres stadig flere opplysninger, vil presset mot å bruke disse opplysningene også øke. I teorien har det vært forsøkt å forankre personvernet i ett enkelt overordnet synspunkt; ingen personopplysning må brukes til andre formål enn de som den er innhentet for. Etter utvalgets syn er dette åpenbart en standard som vanskelig vil holde når en kommer til den praktiske anvendelse. Den offentlige administrasjon kan vanskelig funksjonere etter allment godkjente prinsipper uten at det gis tilgang også på personopplysninger den enkelte helst så ble holdt skjult. Det kan også tenkes situasjoner hvor det er i den enkeltes interesse at opplysningene utleveres og brukes. I praksis vil man ofte ha behov for en konkret, individuell vurdering. Etter utvalgets syn bør det fastsettes noen rammer for denne vurderingen slik at fordelene med den nye behandlingen må være klart større enn ulempene som den volder for den enkelte og at den nye behandlingen ikke kan være uforenlig med det opprinnelige formålet, se lovforslaget § 8.

12.5.7.3.2 *Behandling av sensitive personopplysninger*

Det er grunn til å vise ekstra varsomhet ved behandling av sensitive personopplysninger. Etter personregisterloven § 6 annet ledd kan slike opplysninger ikke registreres uten at det er nødvendig (loven har en uttømmende oppregning av hvilke opplysninger dette gjelder). Etter utvalgets syn bør det fortsatt være begrensninger på bruk av sensitive personopplysninger. Loven bør imidlertid regulere adgangen til å benytte sensitive opplysninger mer uttrykkelig enn i dag. Dette vil bedre forutberegneligheten for de behandlingsansvarlige. En slik regulering kan dessuten bidra til å skape og spre holdninger om at det skal vises ekstra varsomhet ved behandling av visse typer opplysninger. Lovforslaget § 9 lister opp 9 ulike situasjoner hvor behandling av sensitive opplysninger er tillatt, se merknadene til § 9 hvor det redegjøres nærmere for disse situasjonene. I tillegg kan Datatilsynet etter annet ledd bestemme at sensitive personopplysninger også i andre tilfeller kan behandles dersom viktige samfunnsinteresser tilsier det og det settes i verk tiltak for å sikre de registrertes interesser.

12.5.7.3.3 *Bruk av fødselsnummer*

Fødselsnummer har vært i bruk siden 1964. Fødselsnummeret gir en stor grad av sikkerhet for at personer ikke forveksles. Det er av betydning for en effektiv saksbehandling som bygger på korrekte personopplysninger. På den annen side er fødselsnummeret en nøkkel til de personopplysninger som er samlet i et register, og det er en enkel nøkkel til kobling /samkjøring av opplysninger fra forskjellige registre.

Hovedbegrunnelsen for å innføre fødselsnummeret var et ønske om en enkel og entydig identifikasjon for å lette samordning/sammenstilling og utveksling av informasjon om enkeltpersoner når dette var nødvendig eller ønskelig ut fra oppgavene institusjonen/bedriften var pålagt.

I debatten om fødselsnummer så langt har det vært en betydelig sammenblanding av begrepene identifikasjon og legitimasjon. Med identifikasjon menes at fødselsnummeret på en relativt entydig måte peker ut en bestemt person. Dette er den funksjonen fødselsnummer primært bør ha. I visse sammenhenger har imidlertid fødselsnummeret blitt sett på som legitimasjon, dvs sannsynliggjøring av at en enkeltperson er den han utgir seg for å være. Fødselsnummer er imidlertid ikke egnet til å tillegges slike legitimasjonsvirkninger, noe som blant annet har ført til en rekke brudd på taushetsplikt fordi taushetsbelagte opplysninger er blitt gitt ut når et fødselsnummer er blitt oppgitt. Dersom det innskjerpes at fødselsnummer skal tjene som identifikasjon og ikke legitimasjon, kan personvernet være tjent med at fødselsnummer brukes i større utstrekning og i tilfeller der andre teknikker gir for usikker identifikasjon. Dette er bakgrunnen for utvalgets forslag om bruk av fødselsnummer, jf lovforslaget § 10.

12.5.8 Internkontroll

For å understreke den enkelte behandlingsansvarliges ansvar for å følge personvernreglene i lov og forskrift ved behandling av personopplysninger, foreslår utvalget at det innføres regler om internkontroll. Etter utvalgets syn vil et slikt system sannsynligvis bidra til å bevisstgjøre de behandlingsansvarlige (de må dokumentere hvilke tiltak som gjennomføres) mht de reglene som gjelder for behandling av personopplysninger. Det vil dessuten gjøre det enklere for Datatilsynet å sile ut de virksomhetene som bør utsettes for ytterligere kontroll, og man vil på den måten oppnå mer effektiv kontroll ved bruk av mindre ressurser.

Den tradisjonelle tilsynsformen som kun går ut på at tilsynsmyndigheten oppsøker en virksomhet og foretar kontroll av om regelverket respekteres, har visse svakheter. Det er meget ressurskrevende for myndigheten å kontrollere alle typer virksomheter. Det kan dessuten være vanskelig å avdekke en del type feil og mangler under en enkeltinspeksjon, og kontrollen kan ofte ha beskjeden forebyggende effekt fordi den bare sier noe om situasjonen der og da og i liten grad bidrar til en bredere forståelse av området.

Med bakgrunn i slike erfaringer er det både i Norge og internasjonalt skjedd en utvikling der det i stadig større grad legges vekt på at virksomhetene *selv* skal kunne dokumentere at det er etablert systemer som gir tilstrekkelig sikkerhet for at myndighetenes regelverk respekteres (internkontroll). Internkontroll vil med andre ord innebære at både offentlige og private virksomheter har plikt til å påse at ulike typer krav som Datatilsynet retter mot virksomheten overholdes. Krav om internkontrollsystem innebærer at virksomhetene må etablere *systematiske* tiltak for å påse at kravene fra denne myndigheten overholdes og at virksomheten må kunne *dokumentere* at slike systematiske tiltak er etablert og følges.

Ved enkelte andre tilsynsformer kan det oppstå uklarhet i ansvarsforholdet mellom myndighet og virksomhet, for eksempel slik at Datatilsynets kontroll tas som en garanti for at «alt er i orden». Ved internkontroll understrekes imidlertid at ansvaret for å følge vedkommende lov eller forskrift er plassert hos virksomhetene uavhengig av den kontroll tilsynet utfører.

EF-direktivet artikkel 19 nr 2, jf artikkel 21 nr 3 krever at det etableres en viss form for internkontroll for de behandlingene som ikke er underlagt meldeplikt. Direktivet bestemmer at det skal utpekes en person i virksomheten som skal ha ansvar for å påse at lover og regler på området følges, og vedkommende skal føre et register over de behandlingene som skjer. Registeret skal inneholde de samme opplysningene (med ett unntak) som direktivet krever skal fremgå av meldingen for de meldepliktige behandlingene. Opplysningene skal være offentlig tilgjengelig. Utvalget foreslår på bakgrunn av dette at det innføres krav om internkontroll for virksomheter og enkeltpersoner som behandler personopplysninger. Det bør i forskrift fastsettes nærmere regler om hvilke krav som stilles til den dokumentasjonen som skal finnes i virksomheten. Utvalget vil understreke at dette ikke på noen måte er ment å erstatte den kontrollvirksomheten Datatilsynet på eget initiativ skal utføre.

12.5.9 Bransjevisse atferdsnormer

12.5.9.1 EF-direktivet artikkel 27

EF-direktivet artikkel 27 åpner for at det kan utformes bransjevisse atferdsnormer (jf også fortalen nr 61):

«1. Medlemsstaterne og Kommissionen tilskynder til udarbejdelsen af atferdskodekser, der afhængigt af de særlige forhold i de forskellige sektorer skal bidrage til en korrekt anvendelse af de nationale bestemmelser, medlemsstaterne vedtager til gennemførelse av dette direktiv.

2. Medlemsstaterne fastsætter bestemmelser om, at de branche-foreninger eller andre organer, som repræsenterer andre kategorier af registransvarlige, som har utarbejdet udkast til nationale atferdskodekser, eller som agter at ændre eller forlænge gældende nationale kodekser, skal kunne forelægge dem for den nationale myndighed til udtalelse.

Medlemsstaterne fastsætter bestemmelser om, at denne myndighed bl. a skal kontrollere, at de udkast, den får forelagt, er i overensstemmelse med de nationale bestemmelser, der vedtages til gennemførelse av dette direktiv.

Hvis myndigheten finder det hensiktsmessig, kan den indhente bemærkninger fra de registrerede eller disses repræsentanter.

3. Udkast til EF-kodeks og forslag til ændring eller forlængelse af eksisterende EF-kodekser kan forelægges den i artikel 29 omhandlede gruppe. Denne udtaler sig bl. a. om, hvorvidt de udkast, den har fått forelagt, er i overensstemmelse med de nationale bestemmelser til gennemførelse af dette direktiv. Hvis den finder det nødvendigt, indhenter den bemærkninger fra de registrerede eller disses repræsentanter. Kommisionen kan tilse, at de kodekser, som gruppen har godkent, offentliggøres på passende vis.»

Som det fremgår av artikkel 27, mener man med «atfærdskodekser» bransjevisse atferdsnormer for behandling av personopplysninger. Normene utformes av andre enn myndighetene, f eks av bransjerepresentanter eller de behandlingsansvarlige selv. For å sikre at normene er forenlige med lover og forskrifter, skal det være mulig å forelegge forslagene til bransjenormer for Datatilsynet til vurdering.

Direktivet medfører ikke noen rettslig forpliktelse til å sørge for at det utarbeides bransjevisse atferdsnormer, og vi står i Norge fritt til å avgjøre om slike normer bør tas i bruk. Bruk av atferdsnormer anbefales i OECDs retningslinjer, og er nevnt i en rekke av Europarådets rekommandasjoner.

12.5.9.2 Bør bransjevisse atferdsnormer tas i bruk i Norge?

Utvalget vil først presisere at atferdsnormer ikke er noe entydig begrep. Normene kan utformes på en rekke ulike måter, og gis forskjellig rettslig status. Utvalget vil for sin del presiserer begrepet slik at det dreier seg om retningslinjer som virksomheter eller bransjerepresentanter selv utarbeider på frivillig basis. Retningslinjene sidestilles ikke med lover, forskrifter eller annen myndighetsutøvelse, og overtredelse resulterer ikke i sanksjoner fra myndighetenes side. Atferdsnormene kan sies å være et internt reglement.

Erfaring fra andre land som f eks Nederland, Storbritannia og New Zealand viser at utarbeidelsen av atferdsnormer har mange positive sider. En slik form for «selvregulering» kan vekke fornyet interesse og føre til større forståelse for personvern blant dem som behandler personopplysninger. Dette kan igjen underbygge legitimiteten til lovgivningen på området, og føre til mer frivillig kontakt og mindre polarisering mellom tilsynsmyndigheten og de det føres tilsyn med. Dessuten viser erfaringer fra andre rettsområder at normer som bygger på frivillighet og enighet kan være et nyttig supplement til formelle lover og forskrifter. Et eksempel på dette er varetakelse av forbrukerinteresser ved at Forbrukerombudet i samarbeid med bransjerepresentanter har forhandlet frem avtalevilkår for ulike tjenester.

Fordelen med slike retningslinjer fra bedriftenes side er at de kan avklare tvil, og bidra til klar og rasjonell håndtering av spørsmål som behandlingen av personopplysninger reiser. Atferdsnormene kan utformes mye mer detaljert, nyansert og smidig enn det er mulig å gjøre i en generell lov eller forskrift.

Som argument mot innføring av atferdsnormer kan anføres at ikke alle vil føle seg forpliktet til å følge normene og at det kan være vanskelig for bransjen å kontrollere at de blir fulgt. Dette er imidlertid problemer som i alle fall i noen grad også må sies å gjelde for lovfestede regler. Uansett kan man anta at det vil bli sett på som et konkurransefortrinn dersom man følger de fastsatte normene (ved at publikum foretrekker dem som følger atferdsnormene), og dette kan påvirke flere til å følge dem.

En annen ulempe med å innføre atferdsnormer kan være at det oppstår tvil om klarhet med hensyn til hvilken rettslig status atferdsnormene har. Det kan også

være fare for at retningslinjene kan stride mot lov eller forskrifter. Slike problemer kan imidlertid langt på vei unngås ved tilstrekkelig informasjon fra og dialog med Datatilsynet, og utvalget ser ikke disse argumentene som avgjørende innvendinger mot bruk av atferdsnormer.

I utarbeidelsen av atferdsnormene kan det blant annet bygges på ulike internasjonale retningslinjer. I Canada har således ulike handelsorganisasjoner og private virksomheter laget egne retningslinjer blant annet på grunnlag av OECDs retningslinjer (se 9.5.12).

KAPITTEL13

Særlige regler for visse virksomheter**13.1 GJELDENE RETT****13.1.1 Innledning**

Det er fire virksomhetstyper som er underlagt særskilt regulering etter personregisterloven; kredittopplysningsvirksomhet, databehandlingsvirksomhet for andre, adresserings- og distribusjonsvirksomhet og markeds- og opinionsundersøkelser. Det er fastsatt regler om den enkelte virksomhetstype i loven kapittel 5, 6, 7 og 8. Personregisterlovens alminnelige regler gjelder imidlertid for de registrene som føres innenfor de forskjellige virksomhetene. For eksempel når det gjelder kredittopplysningsvirksomhet, må foretaket ha konsesjon etter § 14 for å drive slik virksomhet, samt konsesjon etter § 9 til å føre elektronisk personregister.

Reglene om de særlige virksomhetene kom inn i loven etter forslag fra Sandvik-utvalget (NOU 1974:22 Persondata og personvern). Bakgrunnen for oppnevningen av utvalget var at «de muligheter elektronisk databehandling skaper for utvidet innsamling og bruk av persondata, ville kunne reise nye problemer...», se NOU 1974:22, side 6. Sandvik-utvalget foreslo flere generelle regler om innsamling og bruk av personopplysninger, men foreslo også særlige regler for visse virksomheter hvor dette hensynet gjorde seg spesielt gjeldende.

13.1.2 Kredittopplysningsvirksomhet

Virksomhet som driver kredittopplysning er underlagt reglene i loven kapittel 5. Inntil personregisterloven trådte i kraft i 1980, var det ingen særskilt regulering av denne virksomheten. Personregisterloven § 13 definerer kredittopplysningsvirksomhet til å være «virksomhet som består i å gi meddelelser som belyser kredittverdighet eller økonomisk vederheftighet (kredittopplysning)». Det er gjort visse unntak fra dette utgangspunktet.

I Sverige er det gitt en egen kredittopplysningslov, som håndheves av Datainspektionen sammen med dataloven og inkassoloven. I Danmark er kredittopplysningsvirksomhet regulert av loven om private registre.

Personregisterloven § 14 fastslår konsesjonsplikt for å drive denne type virksomhet. Det er også fastsatt visse rettigheter og plikter i materielle regler i loven (f eks bestemmelsen om gjenpartsplikt i § 19) og dessuten gitt adgang til å fastsette vilkår i forskrifter og enkeltvedtak. Den vesentlige delen av reguleringen følger av vilkårene i konsesjonene fra Datatilsynet. Her fastsettes bestemmelser om hvilke opplysninger som kan registreres, om sletting av eldre opplysninger og om tillatt bruk av de innsamlede opplysningene.

Etter § 21 kan Kongen (Justisdepartementet, jf kgl res av 21 desember 1979) bestemme at regler av samme karakter skal anvendes også på annen personopplysningsvirksomhet. Det er ikke gitt noen slik forskrift.

13.1.3 Databehandlingsvirksomhet

Databehandlingsvirksomhet er regulert i loven kapittel 6. Etter § 22 må virksomhet som består i å bearbeide personopplysninger for andre ved elektroniske hjelpemidler, ikke settes i gang uten konsesjon. Som begrunnelse for innføring av

særskilte regler for denne typen virksomhet anfører Sandvik-utvalget bl a på side 39:

«Det er utviklingen av moderne datateknikk som i særlig grad har gitt støtet til at integritetsvernet ved personopplysninger har blitt tatt opp til utredning. Men i vidt omfang er i dag situasjonen at brukerne av persondata ikke selv forestår selve den automatiserte databehandling, men at denne settes bort til særlige foretak, 'datasentraler', som disponerer den datatekniske ekspertise og det nødvendige databehandlingsutstyr. Og det er ikke minst i disse foretak en står overfor muligheten for krenkelser av personintegriteten ved kopleing og sammenkjøring av data fra flere forskjellige kilder.»

I tillegg til en regel om konsesjonsplikt er det noen materielle regler om behandlingen av opplysningene hos databehandlingsforetaket. Opplysningene må ikke brukes til andre formål enn det oppdraget gjelder, og kan heller ikke utleveres til andre uten at dette er avtalt med registreier. Datatilsynet kan etter § 24 sette vilkår om sikringstiltak som skal gjennomføres.

13.1.4 Adresserings- og distribusjonsvirksomhet

"Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse" i Kapittel 7 gir bestemmelser om adresserings- og distribusjonsvirksomhet. Det er virksomhet som består i å selge eller på annen måte tilby adresser for grupper av personer, eller i å utføre oppdrag for utsending av reklame og andre meddelelser til slike grupper, jf personregisterloven § 25. De fleste virksomheter driver med begge typer virksomhet. Til nå er det gitt ca 100 konsesjoner for adresserings- og distribusjonsvirksomhet.

Virksomheten kan ikke settes i gang uten konsesjon, jf § 25 første ledd. Det er i loven og i personregisterforskriften gitt enkelte materielle regler for virksomheten, men også på dette området følger den vesentlige delen av reguleringen av vilkårene i konsesjonene fra Datatilsynet.

Opplysningene i adresseringsforetakenes registre hentes fra mange forskjellige kilder. Det finnes en rekke offentlig tilgjengelige kilder der navn og adresse og kanskje andre opplysninger om enkeltpersoner er tilgjengelig. I tillegg kan foretaket benytte oppdragsgivers egne registre så sant dette ikke strider mot dette registerets formål. For de forskriftsregulerte personregistrene følger dette av personregisterforskriften § 3-1. For eventuelle andre registre vil dette følge av konsesjonsbestemmelsene. En siste mulighet er å drive adressemekling (listbroking). Det innebærer at en registreier stiller sitt register til disposisjon for adresserings- og distribusjonsforetaket som benytter det til utsending for en annen. Dette skjer for eksempel ved at et foretak tar kontakt med et A/D-foretak og forespør om det finnes et adresseregister som inneholder den aktuelle målgruppe. A/D-foretaket formidler kontakt til en registreier som eventuelt gir sitt samtykke til at registeret nyttes til utsending for den som hadde forespørselen (forutsatt at dette ikke er i strid med formålet). Etter personregisterforskriften § 3-4 tredje ledd (som bl a regulerer utlevering av opplysninger fra kunderegistre), regnes ikke oppbevaring eller behandling av personopplysninger i adresserings- eller distribusjonsforetak som utlevering når dette skjer etter oppdrag fra registerets eier.

13.1.5 Opinions- og markedsundersøkelser

Virksomhet som driver med opinions- og markedsundersøkelser er den siste virksomhetstypen som er underlagt særskilt regulering. Også for denne virksomheten

gjelder konsesjonsplikt, jf personregisterloven § 31. Etter loven § 31 omfatter reglene virksomhet som består i å utføre opinions- eller markedsundersøkelser *for andre*. Etter personregisterforskriften § 7-4 gjelder loven tilsvarende for «foretak som i enkeltstående tilfeller påtar seg slike oppdrag som nevnt i loven § 31 første ledd, og for foretak som setter i verk slike undersøkelser for sin egen administrasjon og virksomhet». Det er gjort visse unntak for forvaltningsorganer i forskriften §§ 7-1 og 7-2.

Virksomheten består i å spørre ut et visst antall personer om hva de mener om forskjellige spørsmål, og deretter beregne seg fram til hva hele befolkningen mener om de samme spørsmålene. Dette innebærer en omfattende innsamling av personopplysninger, og foretakene *kan* dermed ha store registre med personopplysninger. Ofte er imidlertid virksomheten ordnet slik at opplysningene blir anonymisert så fort som mulig etter at de er innhentet.

Loven har, foruten bestemmelsen om konsesjonsplikt, bestemmelser om utlevering, bruk og sletting av personopplysningene.

13.2 FORSLAG OM ENDRINGER I DAGENS REGLER – MANDATETS PUNKT G)

Etter mandatets punkt g) er utvalget bedt særskilt om å vurdere «[s]pørsmål om personregisterloven bør gis anvendelse på virksomhet som driver salg, vedlikehold av edb-utstyr og gjennom denne virksomheten får tilgang til personopplysninger, samt informasjonsformidlingsvirksomhet, se Datatilsynets rapport: Databehandlingsvirksomhet – hvor går vi? 26 januar 1994 (ref: 94/190-1)».

Datatilsynet forslår i sin rapport at definisjonen av databehandlingsvirksomhet endres slik at loven kapittel 6 får anvendelse på «virksomheter som får *rådighet* over andres personopplysninger». I dag er databehandlingsforetak definert som «[v]irksomhet som består i å *bearbeide* (vår utheving) personopplysninger for andre ved elektroniske hjelpemidler». Det foreslås samtidig å unnta flere av disse virksomhetene fra konsesjonsplikt, men i stedet pålegge taushetsplikt. Det er med andre ord først og fremst diskresjonshensynet som søkes ivaretatt.

Hensikten med en slik lovendring skal være å regulere nye typer virksomheter som på forskjellig måter får tilgang til andres personopplysninger gjennom de tjenestene virksomheten tilbyr. Som et eksempel nevner Datatilsynet informasjonformidlingsvirksomhet; «[det] vil si at selskapene selv ikke er ansvarlig for drift av personregistre for andre, men bare sørger for sammenstilling av informasjon fra flere forskjellige registre for kunden som etterspør opplysninger», jf Datatilsynets rapport side 2-3. En annen virksomhet som ønskes bedre dekket av ordlyden i § 22 er virksomhet som driver service- og vedlikehold på maskin eller programvare. Datatilsynet gir databehandlingskonsesjoner til foretak som driver slik virksomhet i dag selv om ikke virksomheten alltid kan sies å «bearbeide personopplysninger», som er lovens krav.

13.3 EF-DIREKTIVET

EF-direktivet har ingen særregler for visse virksomhetstyper slik personregisterloven har, men disse virksomhetene omfattes av direktivets generelle virkeområde; «behandling av personopplysninger». EF-direktivet er ikke til hinder for at det enkelte land fastsetter ulike regler for ulike virksomheter.

Direktivet har videre visse bestemmelser som skal sikre en forsvarlig behandling av personopplysninger også i de tilfeller behandlingen foretas av en annen enn den behandlingsansvarlige, jf artikkel 17 nr 2 og 3.

Medlemsstatene skal etter artikkel 17 nr 2 pålegge den behandlingsansvarlige å velge en databehandler som kan tilby den nødvendige garanti med hensyn til tekniske og organisatoriske sikkerhetsforanstaltninger, og det er den behandlingsansvarliges ansvar å påse at disse foranstaltninger overholdes.

Art 17 nr 3 bestemmer at gjennomføringen av en behandling hos en databehandler («registerfører») skal skje i henhold til kontrakt eller annet rettslig bindende dokument mellom den behandlingsansvarlige og behandleren. I kontrakten skal det fastsettes at behandleren ikke kan anvende opplysningene til andre formål enn det oppdraget gjelder («alene handler etter instruks fra den registeransvarlige») og at de sikkerhetsbestemmelser som gjelder for den behandlingsansvarlige også gjelder for behandleren.

Innholdet i reglene er nesten sammenfallende med innholdet i bestemmelser i personregisterloven om databehandlingsforetak (personregisterloven §§ 23 og 24). Databehandleren er i direktivet definert som «den fysiske eller juridiske person, offentlig myndighet, institusjon eller ethvert annet organ, der behandler personopplysninger på den registeransvarliges vegne», jf direktivet artikkel 2 e). Definisjonen er langt videre enn definisjonen av databehandlingsforetak i personregisterloven; det er ikke krav om det drives en *virksomhet*, heller ikke er det krav om at databehandleren *bearbeider* opplysningene.

13.4 UTVALGETS VURDERINGER

13.4.1 Generelt

Utvalget anser det som lite heldig å videreføre særskilt regulering av visse virksomheter slik personregisterloven gjør i dag. Begrunnelsen for innføring av disse reglene i 1978 kan ikke overføres til dagens situasjon. Det er ikke nødvendigvis innenfor disse virksomhetene det reises flest spørsmål knyttet til innsamling og bruk av personopplysninger (se om kredittopplysningsvirksomhet nedenfor under 13.4.3). Elektronisk behandling av personopplysninger skjer i dag innenfor de fleste typer virksomheter.

Utvalget foreslår dessuten en rekke nye materielle regler som vil få anvendelse på alle typer elektronisk behandling av personopplysninger (samt visse manuelle behandlinger, se lovforslaget § 3). For eksempel foreslås det regler om adgangen til å bruke opplysninger til andre formål, varslingsplikt ved innsamling av personopplysninger, sikring og sletting av personopplysninger. Flere generelle materielle regler minsker behovet for særlige regler for visse utvalgte virksomheter. Det kan likevel vise seg å være særskilte behov innenfor visse virksomheter og bransjer som behandler personopplysninger som ikke dekkes av lovens materielle regler (se om kredittopplysningsvirksomhet nedenfor), og utvalget foreslår at dette reguleres gjennom forskrift, jf lovforslaget § 45.

13.4.2 Den behandlingsansvarliges bruk av databehandler

Sandvik-utvalget beskriver en virkelighet hvor behandling av personopplysninger ofte settes bort til andre «som disponerer den datatekniske ekspertise og det nødvendige databehandlingsutstyr» (se ovenfor under 13.1.3). Dette er ikke blitt mindre aktuelt i 1997, og nye tjenester som innebærer behandling av personopplysninger på vegne av andre dukker stadig opp, se 13.2 ovenfor.

Det er derfor behov for i noen grad å regulere den situasjonen at en behandlingsansvarlig gir en annen i oppdrag å behandle personopplysninger på vegne av seg. Den behandlingsansvarlige er pålagt en rekke plikter etter loven som selvsagt fortsatt vil gjelde selv om vedkommende benytter en databehandler. En databehandler

bør imidlertid ikke kunne råde over personopplysningene på noen annen måte enn det som er avtalt mellom den behandlingsansvarlige og databehandleren. Datatilsynet bør dessuten kunne gi pålegg som anses nødvendig for å oppnå forsvarlig sikring. Slike pålegg bør gjelde både for den behandlingsansvarlige og databehandleren. Se merknadene til lovforslaget § 13.

13.4.3 Særskilt om kredittopplysningsvirksomhet

Kredittopplysningsvirksomhet skiller seg ut fra de andre virksomhetstypene i personregisterloven ved at opplysningene som behandles som regel ikke er sensitive etter loven, men at de av de registrerte ofte oppfattes som nettopp det. De kredittanmerkningene og vurderingene som foretas kan dessuten få store konsekvenser for de registrerte i mange sammenhenger. Det er derfor et særskilt behov for å sikre at opplysningene er korrekte, at det bare registreres opplysninger som det er saklig grunn for og at opplysningene ikke utleveres og brukes av andre enn de som kan sies å ha et saklig behov for dette.

Utvalgets forslag om flere materielle regler vil også gjelde for de foretak som driver kredittopplysningsvirksomhet, for eksempel adgangen til å bruke opplysninger til annet formål (lovforslaget § 8) og varslingsplikt ved innsamling av personopplysninger (lovforslaget §§ 20 og 21). Videre vil virksomheten være underlagt meldeplikt etter utvalgets forslag. Likevel antar utvalget at det vil være behov for ytterligere regler om kredittopplysningsvirksomhet. Dette kunne tenkes regulert i egen lov eller i forskrifter gitt i medhold av personregisterloven. Utvalget har foreslått en forskriftsbestemmelse (lovforslaget § 45). Bestemmelsen tar først og fremst sikte på nærmere regulering av kredittopplysningsvirksomhet, men åpner også for å forskriftsregulere andre typer virksomheter som behandler personopplysninger dersom dette skulle vise seg nødvendig.

Kredittopplysningsvirksomhet er i relativt liten grad i dag regulert av materielle bestemmelser i loven, men først og fremst gjennom konsesjonsvilkår fastsatt av Datatilsynet. Det skjer imidlertid i svært liten grad noen individuell vurdering av den enkelte virksomheten i forbindelse med konsesjonsbehandlingen. I løpet av de årene som er gått siden personregisterloven trådte i kraft har det utviklet seg en fast praksis i form av konsesjonsvilkår fastsatt i standardkonsesjon for kredittopplysningsvirksomhet. Etter utvalgets syn bør slik regulering gis i forskrifts form.

Utvalget har ikke vurdert konkret hvilke regler som bør gjelde for kredittopplysningsvirksomheten, men antar at følgende punkter bør med i en forskrift:

- definisjon av kredittopplysningsvirksomhet
- angivelse av formålet med kredittopplysningsvirksomhet
- angivelse av hvilke opplysninger (eventuelt hvilke type opplysninger) som er tillatt registrert
- angivelse av hvilke kilder som er tillatt brukt ved innhenting av personopplysninger
- angivelse av hvilke opplysninger som skal kunne inngå i eller danne grunnlag for ulike beregninger som for eksempel scoring/risikoprofil
- angivelse av hvem kredittopplysninger kan utleveres til
- angivelse av hvordan personopplysninger kan utleveres (enkeltopplysninger, masseopplysninger i papirversjon, masseopplysninger i edb-basert versjon)
- angivelse av slettingsregler (hvor lenge kan kredittanmerkninger benyttes?)
- omfanget av og innholdet i informasjon til den registrerte (for eksempel ved en gjenpartsplikt)
- taushetsplikt for de ansatte i kredittopplysningsbyrået.

KAPITTEL14

Fjernsynsovervåkning og annen elektronisk overvåkning**14.1 INNLEDNING**

Lyd- og billedopptak som er elektronisk behandling av personopplysninger (f eks fordi opptakene er lagret i digitalisert (maskinlesbar) form) omfattes av de alminnelige reglene i utvalgets lovforslag, se 10.1.2.3 og merknadene til §§ 3 og 4 i utvalgets lovforslag. Slike opptak diskuteres ikke nærmere her. Temaet i dette kapitlet er om og i hvilken grad loven eller deler av loven skal gis tilsvarende anvendelse på annen overvåkning som ikke omfattes av loven f eks når personopplysninger lagres analogt på videobånd eller annet, eller overvåkning der lyd eller bilde ikke lagres, men bare overføres til en høytaler eller en skjerm (jf personregisterlovens regler i dag om fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning (personregisterloven kapittel 9 a)).

Utvalget foreslår i 14.4 at dagens regler om fjernsynsovervåkning videreføres, samt suppleres på to punkter; for det første foreslår utvalget at fjernsynsovervåkning som resulterer i billedopptak blir underlagt meldeplikt. For det andre foreslår utvalget at Datatilsynet gis kompetanse til å gripe inn og stoppe fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning når slik overvåkning blir igangsatt ulovlig, f eks fordi overvåkningen ikke kan sies å være saklig begrunnet. Endelig foreslås at straffeloven § 390 b om varslingsplikt ved fjernsynsovervåkning av offentlig sted og arbeidssted flyttes fra straffeloven til den nye loven om behandling av personopplysninger.

14.2 GJELDENDE RETT**14.2.1 Personregisterloven, straffeloven § 390 b, åndsverkloven mm**

Det finnes ulike bestemmelser i lovgivningen som direkte eller indirekte regulerer fjernsynsovervåkning. I det følgende gis en kort oversikt over reglene.

For det første er fjernsynsovervåkning regulert gjennom personregisterloven §§ 37 a og 37 b. Bestemmelsene ble vedtatt ved lov 11 juni 1993 nr 78, og trådte i kraft 1 januar 1994. Bestemmelsene regulerer fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning i de tilfeller billedopptaket ikke utgjør et personregister i h t personregisterloven § 1 annet ledd. Dersom opptaket utgjør et personregister gjelder de alminnelige bestemmelsene i personregisterloven (om konsesjonsplikt etc). Se nærmere om reglene i personregisterloven nedenfor (14.2.2).

Fjernsynsovervåkning er dessuten regulert gjennom straffeloven § 390 b. Denne bestemmelsen har imidlertid et begrenset virkeområde. For det første gjelder den bare for «vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller liknende apparat». Overvåkning, fotografering, filming osv som gjøres manuelt (med en person bak kameraet) reguleres ikke. For det andre er fjernsynsovervåkning etter denne bestemmelsen ikke forbudt dersom «det ved skilting eller på annen måte er gjort tydelig oppmerksom på at stedet blir overvåket». Om innholdet i opplysningsplikten heter det i Ot prp nr 56 (1989-90) side 57:

«For at opplysningsplikten skal anses oppfylt, må informasjonen formidle noe mer enn det som direkte følger av fjernsynsovervåkningen selv. Informasjonen må på en effektiv måte kunne nå fram til personer som blir berørt

av overvåkningen. Derimot kan det ikke kreves at hver enkelt som kan bli berørt av overvåkningen faktisk er blitt informert. Avgjørende må være om informasjonen er egnet til å underrette vedkommende om overvåkningen».

Justisdepartementet kommenterer dette nærmere i St meld nr 15 (1996-97) side 6:

«Det er [...] ikke nødvendig at kameraene er synlige for at informasjonsp-likten skal anses oppfylt. Dersom et kamera er bevegelig, f eks ved fjernstyring, vil dette få konsekvenser for kravet til hvor omfattende skiltingen/merkingen må være. Hvis et område – f eks på grunn av størrelsen eller utformingen – er slik at det ikke lar seg gjøre å informere dem som kommer til området om overvåkningen, vil overvåkning være forbudt etter straffeloven § 390 b».

Bestemmelsen regulerer bare fjernsynsovervåkning «på offentlig sted eller av arbeidssted». Hva som skal regnes som offentlig sted, fremgår av straffeloven § 7 nr 1. Fjernsynsovervåkning som gjøres andre steder enn på offentlig sted eller arbeidssted, omfattes ikke av denne lovbestemmelsen.

Straffeloven § 390 b gjelder såvel private som for offentlige myndigheter. I straffeprosessloven § 202 a er det imidlertid åpnet for at politiet i visse tilfeller skal kunne foreta skjult fjernsynsovervåkning på offentlig sted.

Fjernsynsovervåkning av arbeidssted kan også være regulert i avtaler mellom partene i arbeidslivet. I hovedavtalen av 1994 mellom Næringslivets Hovedorganisasjon og Landsorganisasjonen i Norge er det for eksempel i § 9-13 nr 2 bestemt:

«Behov, utforming og innføring av interne kontrolltiltak skal drøftes på bedriften. Hvis direkte og kontinuerlig TV-overvåkning av den enkelte ansatte i arbeidssituasjonen er aktuell, skal hensikt og behov klarlegges. Slik overvåkning bør i størst mulig utstrekning unngås. Krav til saklighet i Lov om personregistre m.m. må håndheves.»

Det finnes også enkelte andre bestemmelser som ut fra personvern hensyn retter seg mot fotografering og filming. For eksempel er det forbudt å fotograferer siktede/tiltalte under forhandlingene i en straffesak, eller på vei til eller fra disse forhandlingene, jf domstolloven § 131 a og § 198 tredje ledd. Også straffeloven § 390 a om forbud mot krenkelse av privatlivets fred vil kunne sette skranker for fjernsynsovervåkningen. Bestemmelsen setter forbud mot handlinger som kan karakteriseres som «skremmende eller plagsom opptreden eller annen hensynsløs atferd».

Videre er det en bestemmelse i åndsverkloven § 45 c som regulerer adgangen til offentliggjøring av bilder. Utgangspunktet etter denne bestemmelsen er at offentliggjøring bare kan skje dersom den registrerte samtykker. Bestemmelsen gjelder uavhengig av hvordan bildene er tatt – om det er resultat av opptak gjort ved fjernsynsovervåkning eller om de er tatt ved ordinær fotografering, filming osv, er uten betydning.

Endelig kan arbeidsmiljøloven § 12 ha innvirkning på etableringen av overvåkningstiltak på arbeidsplassen. Og i den grad elektronisk overvåkning ikke reguleres av gjeldende lovgivning, kan ulovfestede personvernregler komme til anvendelse. Et eksempel på anvendelse av slike ulovfestede regler er Høyesteretts avgjørelse inntatt i Rt 1991 s 616 hvor et fjernsynsopptak som var gjort av innehaveren av et gatekjøkken og rettet mot en av de ansatte, ikke ble tillatt ført som bevis i straffesak mot den ansatte.

14.2.2 Nærmere om reglene i personregisterloven

I Ot prp nr 56 (1992-93) antar Justisdepartementet at løpende fjernsynsoptak som lagres på ordinære videobånd eller film ikke er å anse som personregistre, jf personregisterloven § 1 annet ledd annet punktum. Departementet antar videre at de fleste typer opptak som gjøres på bensinstasjoner, i banker, forretninger osv foregår på denne måten (løpende opptak som lagres på ordinære videobånd eller film). Justisdepartementet antar at de fleste fjernsynsoptak reguleres av de særskilte reglene om fjernsynsovervåking i personregisterloven kapittel 9a, og ikke av de alminnelige reglene om konsesjonsplikt m v.

Etter § 37 a er *fjernsynsovervåking og billedopptak* i forbindelse med slik overvåking bare tillatt dersom det er saklig begrunnet ut fra hensynet til virksomheten i det organ eller foretak som foretar overvåkingen. Ved overvåking av steder hvor en begrenset krets av personer jevnlig ferdes, er det stilt strengere vilkår for fjernsynsovervåking. På slike steder er fjernsynsovervåking (og billedopptak i den forbindelse) bare tillatt dersom det ut fra hensynet til virksomheten er et særskilt behov for overvåkingen.

Paragraf 37 b inneholder nærmere regler om lagring (sikring) og etterbruk av *billedopptak* gjort ved fjernsynsovervåking. Billedopptak skal bare kunne utleveres til noen utenfor det foretak eller organ som har foretatt opptaket, dersom den som er avbildet samtykker eller utleveringsadgangen følger av lov. Hvis ikke lovbestemt taushetsplikt er til hinder for utlevering, skal billedopptak likevel kunne utleveres til politiet i forbindelse med etterforskning av straffbare handlinger og ulykker. Billedopptak gjort ved fjernsynsovervåking skal slettes når det ikke lenger er saklig grunn for oppbevaring (§ 37 a andre ledd). Bestemmelsen er fulgt opp med mer detaljerte regler i forskrift.

14.3 INTERNASJONALE REGLER

EF-direktivet har ingen særskilte regler om fjernsynsovervåking, men slik overvåking omfattes av direktivets anvendelsesområde når overvåkingen representerer en elektronisk behandling, f eks ved at personopplysninger blir lagret i digitalisert form. Utvalget legger til grunn at elektronisk overvåking der bilde eller lyd ikke lagres, men bare vises på en monitor ikke omfattes av direktivet. Det samme gjelder overføring av opplysninger om personers utseende eller stemme til et vanlig (analogt) lyd- eller videoopptak, se utvalgets merknader under 10.1.2.3 og merknadene til §§ 3 og 4 i utvalgets lovforslag.

Europarådskonvensjonen om personvern i forbindelse med elektronisk databehandling av personopplysninger antas ikke å gjelde for fjernsynsovervåking. Ordlyden («elektronisk databehandling») tilsier at det er mer den tradisjonelle databehandling som er omfattet.

14.4 UTVALGETS VURDERINGER

Fjernsynsovervåking slik vi kjenner det fra banklokaler, forretninger osv, har etterhvert fått et betydelig omfang. Ofte innebærer denne typen overvåking at det også gjøres billedopptak. Dette betyr at de som foretar overvåking vil kunne sitte med store mengder billedmateriale av personer fra ulike steder og situasjoner. Normalt vil ikke den omstendighet at enkelte foretak eller organer sitter med slike billedopptak innebære noen fare eller trussel mot dem som er registrert. Formålet med fjernsynsovervåkingen er for eksempel å forebygge straffbare handlinger, eller å være et hjelpemiddel ved etterforskningen. En fare eller trussel mot den enkelte vil billedopptakene særlig være overfor den som har forgått seg (for eksempel ved en

straffbar handling), slik at materiale av den grunn blir interessant for overvåkeren og eventuelt politiet. I slike tilfeller vil den avbildede ofte ikke ha en like berettiget interesse i å få være beskyttet mot at opptakene benyttes.

Selv om man ikke gjør noe galt vil mange føle et ubehag ved det å vite (eller ha mistanke om) at andre overvåker dem og sitter inne med billedopptak av dem. Videre vil det være en fare for at billedopptak kan bli brukt på en måte som ut fra en alminnelig oppfatning ikke er akseptabel – eller til og med rettsstridig, for eksempel at billedopptakene nyttes som pressmiddel mot den avbildede hvis det viser vedkommende i situasjoner eller på steder han eller hun ikke ønsker skal bli kjent for andre.

Utvalget foreslår enkelte viktige endringer i dagens regler om fjernsynsovervåkning. Prinsipielt bør reglene gjelde for all elektronisk overvåkning, uavhengig av om overvåkingen skjer ved billedopptak, lydopptak eller ved f.eks. sensorer som registrerer bevegelser (når disse registreringene representerer personopplysninger). Utvalget har imidlertid ikke, innen den fastsatte tidsrammen, hatt anledning til å utrede konsekvensene av en slik utvidelse av reglens anvendelsesområde. I lovforslaget er det derfor bare foreslått regler om fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning.

Det kan være uheldig at overvåkeren selv er tillagt et så vidt skjønn når det gjelder vurderingen av om det er saklig behov for å igangsette overvåkning. Slik reglene er utformet skal han eller hun vurdere om fjernsynsovervåkingen er «saklig begrunnet» eller ikke, eventuelt hvorvidt han eller hun har et «særskilt behov», jf. personregisterloven § 37 a. Datatilsynet har i sin årsmelding for 1994 (St. meld. nr. 27 1995-96) påpekt at reglene på denne bakgrunn kan bli vanskelig å håndheve. Utvalget er enig i denne vurderingen. Datatilsynet bør derfor ha kompetanse til å gripe inn og stoppe overvåking som skjer i strid med loven, for eksempel fordi overvåkingen ikke kan sies å være saklig begrunnet. Ved at Datatilsynet gis kompetanse til å gripe inn vil det være Datatilsynet – og ikke overvåkeren – som avgjør om det foreligger et «saklig behov» i lovens forstand. Datatilsynets vedtak om å stoppe overvåking kan påklages. Dersom Datatilsynet skal ha en reell mulighet til å gripe inn og stoppe fjernsynsovervåking i strid med loven, bør slik overvåking etter utvalgets syn være meldepliktig. En slik meldeplikt vil også synliggjøre omfanget av slik overvåking i samfunnet, og det kan dessuten medføre økt bevissthet hos den behandlingsansvarlige som da uttrykkelig må angi hvilket saklig behov han eller hun har for overvåkingen.

Straffeloven § 390 b om at fjernsynsovervåking på offentlig sted eller arbeidssted er forbudt dersom det ikke ved skilting eller på annen måte er gjort tydelig oppmerksom på at stedet blir overvåket, bør flyttes fra straffeloven til ny lov om behandling av personopplysninger. Bestemmelsen hører naturlig sammen med de øvrige reglene om fjernsynsovervåking og varslingsplikten bør ses i sammenheng med de øvrige varslingsreglene i lovforslaget, se merknadene til § 24.

KAPITTEL15

Sikring av personopplysninger**15.1 INNLEDENDE FORKLARING OG OVERSIKT OVER FREMSTILLINGEN**

Med «sikring» av personopplysninger sikter utvalget til tiltak som er egnet til å forhindre at personopplysninger blir behandlet på måter som er ulovlige eller som av andre grunner ikke er ønsket. Sikringstiltakene skal bidra til at lovens bestemmelser etterleves og at opplysningene ellers behandles på måter som er i overensstemmelse med rettspraksis, adferdskodekser m v. I toneangivende utredningsarbeider er sikringsarbeidet primært knyttet til varetakelse av opplysningenes «kvalitet», «konfidensialitet» og «tilgjengelighet». Disse tre begrepene fungerer primært som fellesbetegnelse på en rekke mer detaljerte krav til opplysningene. Det er videre vanlig å fokusere særlig på tiltak av teknisk og organisatorisk art. Sikring av personopplysninger gjelder med andre ord tiltak av teknisk og organisatorisk art som er egnet til å sikre gjennomføringen av normative krav til kvalitet, konfidensialitet og tilgjengelighet. De normative kravene følger primært av rettssystemet (særlig lovgivning, avtaler og rettsavgjørelser), men kan også følge av bransjevise atferdsnormer (se 12.5.9) og rene moralske/etiske regler.

Når området beskrives som «sikring av personopplysninger» er dette upresist. Sikringstiltakene kan knyttes til tre nivåer ved behandlingen: Før det første gjelder det sikring av «persondata», dvs av de tegn, symboler m v som, når de fortolkes og anvendes i bestemte sammenhenger, har et innhold som kan beskrive en person. I datamaskinsystemet og ved maskinelle overføringer mellom datamaskinsystemer er det f eks data som behandles og transporteres. Når dataene fortolkes og forstås av et menneske eller et datamaskinprogram er dataene bærer av *informasjon*. Data behandles, fortolkes og blir til informasjon og informasjon formaliseres og blir til data innenfor rammene av et persondata/informasjonsystem, dvs det komplekset av regler og rutiner som til sammen bestemmer behandlingen av data og informasjon. Systemet kan dels være automatisert og dels manuelt. Sikringskravene kan og bør stilles til alle tre nivåer; data, informasjon og system. I innværende kapittel og i merknadene til lovforslaget § 11 har utvalget anvendt disse tre begrepene på den omtalte måten. For øvrig er det i utredningen ikke skilt strengt mellom «informasjon» og «data». «Data» er for enkelthets skyld anvendt fast i flere ordsammensetninger, f eks «persondata» og «persondatabehandling».

Nedenfor redegjør utvalget for tidligere utredninger og initiativ (15.2), de mest sentrale reglene på området (ikke uttømmende) (15.3), internasjonale regler (EF-direktiv og Europarådskonvensjon) (15.4) og til slutt utvalgets vurderinger (15.5).

15.2 TIDLIGERE UTREDNINGER OG INITIATIV

I 1981 nedsatte Justisdepartementet en arbeidsgruppe som skulle legge frem forslag til sikkerhetsforskrifter i medhold av personregisterloven. I høringsrunden møtte forslaget motbør blant annet fordi reglene ble ansett som for detaljerte og fordi en fryktet for at forslaget ville bli kostbart å gjennomføre. Forslaget ble ikke fulgt opp av Justisdepartementet. I 1984 ble det i samarbeid mellom Datatilsynet og Institutt for rettsinformatikk ved Universitetet i Oslo etablert en arbeidsgruppe med sikte på å utforme prinsipper for «sikring av personvern interesser». Rapport med forslag til sikringsforskrifter ble sendt på høring i 1988. Også dette forslaget møtte motbør,

spesielt fordi det foreslåtte regelverket ble ansett å være for komplisert, og fordi det var stor usikkerhet med hensyn til kostnadsmessige konsekvenser. I 1990 nedsatte regjeringen en ny arbeidsgruppe som skulle legge fram forslag til generelle og samordnede regler for beskyttelse av informasjon, herunder personopplysninger. Dette arbeidet resulterte i et nytt utkast til forskrifter. I tillegg ble det lagt fram et forslag til lov om informasjonssikkerhet som inneholdt overordnede regler og hjemmel for en samordnet forskrift. Mange høringsinstanser har uttalt seg skeptisk til forslaget. Regjeringen har ikke lagt forslaget fram for Stortinget. Det er etter høringsrunden enighet mellom de berørte departementer om at samordningsbehovet ikke skal varetas gjennom et felles regelverk (jf St meld nr 27 1995-96 side 7). I 1996 oppnevnte regjeringen et råd for IT-sikkerhet, med oppgave å utrede virkemidler som kan fremme IT-sikkerhet. Dette rådet er også ment å ivareta samordningsbehovet. Så vidt utvalget er kjent med, er det ikke tatt initiativ for å etablere sikringsregler etter personregisterloven.

15.3 GJELDENDE RETT

Regler som setter krav til sikring av personopplysninger omfatter både lover, forskrifter og instruksjoner for statsforvaltningen. Fremstillingen nedenfor er ment å gi en oversikt over de mest sentrale reglene på området. Fremstillingen er på ingen måte ment å gi en uttømmende oversikt.

15.3.1 Personregisterloven §§ 8 b og 24

I henhold til personregisterloven § 8 b kan Kongen ved forskrift eller enkeltvedtak gi regler for sikring av personopplysninger. Kongens myndighet til å gi bestemmelser om sikring av personopplysninger ved enkeltvedtak er delegert til Datatilsynet, mens forskriftsmyndigheten er delegert til Justisdepartementet ved kgl res 30 september 1988. Det er gitt to forskrifter med hjemmel i denne bestemmelsen (se 15.3.2 og 15.3.3 nedenfor). Datatilsynet setter imidlertid krav til sikkerheten i forbindelse med at de gir konsesjoner for opprettelse av personregistre etter personregisterloven § 9. Datatilsynet har også gitt ut generelle veiledninger som gir råd om hvilke krav Datatilsynet stiller ved utforming av konsesjoner. Disse veiledningene er utgitt i egne brosjyrer, f eks:

- «Sikkerhetsregulering av delte edb-systemer» (utgitt 23.9.1992)
- «Krav til sikring av medisinsk informasjon» (utgitt 20.2.1992)
- «Elektronisk overføring av sensitive personopplysninger» (utgitt 20.1.1993)

Paragraf 8 b gjelder både for konsesjonspliktige og ikke-konsesjonspliktige personregistre. Bestemmelsen kom inn i loven ved en lovendring i 1987 (lov 12 juni 1987 nr 55) til erstatning av noen mer spesielle hjemler i dagjeldende lov. Unnlattelse av å etterkomme pålegg om sikring etter prgl § 8 b rammes ikke av straffebestemmelsen i § 38. Det er heller ikke knyttet andre sanksjoner til bestemmelsen. Det antas at dette er en ren forglemmelse. Tidligere (før lovendringen i 1987) ble pålegg om sikring gitt med hjemmel i § 11 og overtredelse av vilkårene var straffesanksjonert i § 38. Under lovendringen i 1987 (da § 8 b ble tilføyd) ble ikke straffebestemmelsen endret tilsvarende.

Etter § 24 kan Kongen «ved forskrift eller for det enkelte foretak gi bestemmelser om de sikringstiltak som skal gjennomføres». Bestemmelsen gjelder for databehandlingsforetak. Kongens myndighet er delegert til Justisdepartementet ved kgl res 21 desember 1979. Det er ikke gitt slike bestemmelser.

15.3.2 Forskrift i medhold av lov om personregistre m m av 21 desember 1979

Forskriften er fastsatt av Justisdepartementet med hjemmel i personregisterloven §§ 9 annet ledd og 8 b, jf kgl res 21 desember 1979 og kgl res 30 september 1988. Etter forskriften "*Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte*" i kapittel 2 fritas en rekke personregistre for konsesjonsplikt under forutsetning av at «kravene til registerets innhold mm i kapitlet her følges, og at bestemmelsene i "*Hva er personvern?*" i kapittel 3 overholdes» jf forskriften § 2-1.

I "*Hva er personvern?*" i kapittel 3 er det gitt følgende bestemmelse om sikring:

«§ 3–3 Sikring

Den registeransvarlige må sørge for nødvendig sikring av konfidensialitet, kvalitet og tilgjengelighet for personopplysninger og registre.

Den registeransvarlige skal godkjenne alle brukere av registeret, samt drifts- og vedlikeholdspersonale. Enhver bruker av et elektronisk register skal entydig identifiseres og autentiseres av registersystemet før tilgang til registeret.

Datatilsynet kan gi pålegg som ansees nødvendige for å oppnå forsvarlig sikring.

For organ i staten vises for øvrig til Beskyttelsesinstruksjonen, Sikkerhetsinstruksjonen med utfyllende bestemmelser og Datasikkerhetsdirektivet.

Denne paragrafen gjelder ikke for registre som nevnt i § 2-15.»

15.3.3 Forskrift om unntak fra konsesjonsplikt i saker om hvitvasking

Forskriften er fastsatt av Justisdepartementet 23 mars 1995 med hjemmel i personregisterloven §§ 9 annet ledd, 8 b og 7 femte ledd, jf kgl res 21 desember 1979 og kgl res 30 september 1988. Forskriften har relativt detaljerte regler om sikring som omfatter krav om:

- kun autorisert tilgang med spesifiserte rettigheter
- at autorisasjon kan gis kun etter bestemte vilkår
- at den registeransvarlige skal etablere og følge opp sikringsregler om tilgangskontroll, datakvalitet og tilgjengelighet.

15.3.4 Sikkerhetsinstruksjonen

Instruksjonen anvendes «ved behandling av dokumenter som inneholder opplysninger som er av betydning for rikets sikkerhet, eller det internasjonale forsvarspolitiske samarbeid, eller som er av særlig betydning for forholdet til fremmede makter. Instruksjonen skal [...] også [...] anvendes under behandling av NATO-graderte opplysninger», jf § 1. Instruksjonen korresponderer således med straffeloven §§ 90-93. Anvendelsesområde er derfor langt videre enn personregisterloven som kun omfatter personopplysninger.

Instruksjonens primære formål er å ivareta hensynet til konfidensialitet og har ulike tiltakskrav knyttet til ulike graderinger, som er: begrenset, konfidensielt, hemmelig og strengt hemmelig, jf § 2.

Instruksjonen forvaltes av Forsvarsdepartementet med Forsvarets overkommando som utøvende myndighet.

15.3.5 Beskyttelsesinstruksjonen

Instruksjonen «kommer til anvendelse ved behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i Sikkerhetsinstruksjonen», jf § 1.

Beskyttelsesgradene er fortrolig og strengt fortrolig, jf § 2. Et dokument skal bare graderes når det «kan unntas fra offentlighet i medhold av offentlighetsloven og skadevirkninger som nevnt i § 4 kan inntreffe.» Instruksjonen presiserer ikke hva som ligger i «skade». Instruksjonen er fastsatt for å ivareta hensynet til konfidensialitet (hindre at graderte dokumenter blir gjort kjent for uvedkommende). Instruksjonen har flere likelydende behandlingsregler med Sikkerhetsinstruksjonen, men er langt mindre detaljert.

Instruksjonen forvaltes av Statsministerens kontor. Det er ikke etablert tilsyn.

15.3.6 Datasikkerhetsdirektivet

Formålet med Datasikkerhetsdirektivet er å sikre at informasjon gradet etter sikkerhetsinstruksjonen eller Beskyttelsesinstruksjonen, blir behandlet på en betryggende måte ved elektronisk databehandling. Direktivet med vedlegg skal sikre at informasjon ikke blir kjent for uvedkommende (sikring av konfidensialet), informasjon ikke endres uautorisert (sikring av integritet) og at informasjon og dataressurser er tilgjengelig for autoriserte brukere (Sikring av tilgjengelighet). Direktivet er gitt i medhold av Sikkerhetsinstruksjonens § 16. I samråd med Statsministerens kontor skal direktivet også gjelde for elektronisk behandling av informasjon gradert iht Beskyttelsesinstruksjonen, jf Beskyttelsesinstruksjonen § 12.

Datasikkerhetsdirektivet omhandler planlegging, godkjenning, anskaffelse, implementering, drift, vedlikehold og kontroll av datautstyr og programvare,

15.4 INTERNASJONALE REGLER

15.4.1 EF-direktivet artikkel 17

Art 17 nr 1 og 2 gjelder informasjonssikkerhet, og i nr 1 pålegges medlemsstatene å gi regler om registeransvarliges plikt til iverksettelse av tekniske og organisatoriske foranstaltninger til beskyttelse av personopplysninger. Sikkerhetsforanstaltningene skal sikre et *tilstrekkelig* sikkerhetsnivå i forhold til den risiko behandlingen innebærer og arten av de opplysningene som behandles. Det er opp til medlemsstatene å fastsette hva som er et tilstrekkelig sikkerhetsnivå. Etter nr 2 plikter den behandlingsansvarlige å velge en persondatabehandler som kan tilby tilstrekkelig garanti for at de tekniske og organisatoriske sikkerhetsforanstaltninger treffes og skal påse at disse overholdes. Art 17 nr 4 bestemmer at sikkerhetsforanstaltningene etter nr 1, av bevisshensyn, skal foreligge i skriftlig form.

15.4.2 Europarådskonvensjonen

Europarådskonvensjonen artikkel 7 lyder:

Formålstjenlige sikringstiltak skal treffes for å verne personopplysninger lagret i elektroniske dataregistre mot tilfeldig eller ikke-autorisert adgang, forandring eller spredning.

Det er ikke ytterligere definert hva som er å anse som «formålstjenlige tiltak».

15.5 UTVALGETS VURDERINGER

Utvalget vil peke på at det i 15 år er arbeidet med sikkerhetsforskrifter til personregisterloven uten at dette arbeidet har ført fram til noen forskrifts- eller lovregulering. Personvernet er én av flere begrunnelser for å sikre opplysninger. Tiltak for å sikre konfidensialitet kan f.eks. både begrunnes i personvern og ivaretagelse av forretningsmessige og/eller politiske interesser. Det kan derfor åpenbart være grunn til

å ønske en samordning av feltet. Samtidig er det på det rene at det er et stort behov for tiltak som på en systematisk måte kan bedre etterlevelsen av lovgivning vedrørende behandling av personopplysninger. Sikringskrav vil kunne føre til et høyere bevissthetsnivå hos de behandlingsansvarlige, fordi kravene fordrer en gjennomgang av viktige organisatoriske og praktiske forhold ved virksomheten. I medhold av Kredittilsynsloven § 4 er det gitt regler om sikkerhet for kredittinstitusjoner, forsikringsselskaper m v. Utvalget mener at informasjons- og datasikkerhet også er en nødvendig del av en fremtidig regulering på personvernområdet. Utvalget foreslår å knytte en plikt til å etablere og anvende alminnelig anerkjente metoder for informasjons-/datasikkerhet for persondatabelandlinger. Utvalget avstår imidlertid fra å fastsette noe spesifikt sikkerhetsnivå. Den løsning som her er valgt er dessuten teknologi- og metodeuavhengig.

De regler som foreslås innebærer at eventuelle pålegg om sikringstiltak må skje i form av enkeltvedtak fra Datatilsynet med hjemmel i lovforslaget § 40. Spørsmålet om hva som er tilstrekkelige sikkerhetsnivå må således vurderes konkret av Datatilsynet i en dialog med den behandlingsansvarlige. Tilsynets avgjørelse vil være gjenstand for klage. Se forøvrig merknadene til § 11 i lovforslaget.

KAPITTEL16

Overføring av personopplysninger til utlandet**16.1 OVERSIKT**

Overføring av personopplysninger over landegrensene er i mange tilfelle et viktig ledd i offentlig og privat virksomhet. Samtidig er det på det rene at overføring av personopplysninger fra ett land til et annet kan representere en betydelig trussel mot personvernet. Særlig gjelder dette når regelverket i landet som opplysningene overføres til ikke varetar personvern på en tilfredsstillende måte.

Nedenfor gis det først en oversikt over gjeldende rett (16.2). Blant annet pekes det på at ny teknologi reiser tolkningsspørsmål som dagens regler ikke gir noe klart og/eller hensiktsmessig svar på. Deretter omtales internasjonale forpliktelser av betydning for utformingen av regler om overføring av personopplysninger til utlandet (16.3). Til slutt presenteres utvalgets vurderinger som ligger til grunn for lovforslaget (16.4). I tråd med direktivet sondres det mellom overføring av personopplysninger innenfor og utenfor EØS-området.

16.2 GJELDENDE RETT**16.2.1 Hovedtrekk**

I personregisterloven § 36 heter det at:

«Register som omfattes av § 9 første ledd må ikke overføres til utlandet uten samtykke av Kongen.

Personopplysninger som er innsamlet her i riket, må ikke overføres til utlandet uten samtykke av Kongen når formålet er å innføre opplysningene i et register som nevnt i § 9 første ledd. Kongen kan ved forskrift gjøre unntak fra første og annet ledd. Det kan fastsettes at disse bestemmelser ikke skal gjelde i forhold til enkelte andre land.»

Som det fremgår av første ledd er utgangspunktet at Kongen (delegert til Datatilsynet med Justisdepartementet som klageinstans) må gi sitt *samtykke* før overføring finner sted. Tredje ledd gir hjemmel til å fravike samtykkekravet ved forskrift. Denne hjemmelen er benyttet, og forskriften § 8-1 bestemmer at overføringen må *meldes* til Datatilsynet i god tid før overføringen skal finne sted:

«Dersom register eller opplysning som nevnt i lovens § 36 første og annet ledd overføres til utlandet, behøves ikke noe slikt samtykke som nevnt i § 36. Overføringen må meldes til Datatilsynet på fastsatt skjema i god tid før overføringen finner sted. Datatilsynet kan nekte overføring eller sette vilkår for overføringen.

Overføring behøves ikke meldes når Norge har plikt til å foreta slik overføring etter folkerettslig overenskomst eller som følge av medlemskap i internasjonal organisasjon.»

Tilsynet kan altså velge å nekte overføring, eller sette vilkår for hvordan overføringen kan finne sted. På denne måten kan Datatilsynet kontrollere overføringer ut av Norge og gripe inn der det anses nødvendig, samtidig som reguleringen blir mindre arbeidskrevende enn dersom samtykke måtte vurderes for hver eneste overføring.

I forskriften § 8-1 er det gjort unntak fra meldeplikten når Norge har plikt til å foreta slik overføring etter folkerettslig overenskomst eller som følge av

medlemsskap i internasjonal organisasjon. Begrunnelsen for bestemmelsen var at det neppe er behov for melding til Datatilsynet når overføringen var vedtatt gjennom internasjonale forpliktelser (jf Eirik Djønne m fl, Personregisterloven med kommentarer s 158 TANO 1987). I praksis har bestemmelsen blitt tolket snevrere enn ordlyden skulle tilsi.

Regelverket får anvendelse både på *manuell* og på *elektronisk* overføring av personregistre/opplysninger til utlandet. Eksempler på manuell overføring er at opplysningene sendes med kurer eller med post.

16.2.2 Særskilte tolkningsspørsmål

Elektronisk overføring – f eks via nettverk eller satellitt – reiser særskilte tolkningsspørsmål. Eva I E Jarbekk drøfter flere slike problemstillinger i avhandlingen «Personvern og overføring av personopplysninger til utlandet» (Complex 4/96) s 57 flg. Utvalget vil for sin del nøye seg med å peke på noen tolkningsspørsmål hvor løsningen i henhold til gjeldende rett er tvilsom eller gir lite formålstjenlige løsninger, og hvor det er ønskelig med en avklaring i den nye loven.

Et særtrekk ved elektronisk overføring er at avsenderen kan bestemme hvem mottakeren skal være, men ikke ad hvilke veier opplysningene skal overføres. Selv når personopplysninger overføres fra ett sted i Norge til et annet sted i Norge kan det være at opplysningene sendes via telelinjer eller satellitter i utlandet. I en del tilfeller vil opplysningene også mellomlagres i utlandet som ledd i overføringen. Strengt tatt dreier det seg også her om overføring av personopplysninger til utlandet, men ettersom avsenderen som regel ikke er klar over at opplysningene tar veien om utlandet, sendes ikke melding til Datatilsynet. Det er mulig at loven på dette punkt må tolkes innskrenkende (jf Jarbekk s 58), slik at det ikke er overføring til utlandet i lovens forstand dersom avsender bare har til hensikt å overføre opplysningene til mottakere i Norge.

Et annet tolkningsspørsmål knytter seg til bruk av internasjonale nettverk (som f eks Internett). Kan personopplysninger som gjøres tilgjengelige på slike nettverk – og som dermed kan lastes ned i utlandet av et stort antall personer – sies å være overført til utlandet i lovens forstand? Spørsmålet er bl a aktuelt for såkalte «hjemmesider», hvor informasjonen gjøres tilgjengelig i utlandet, men hvor den som gjør opplysningene tilgjengelig ikke selv har spesifisert mottaker. Teoretisk er det mulig at ingen besøker hjemmesiden og gjør seg kjent med opplysningene. Praktisk sett vil noen i utlandet lagre og bearbeide informasjonen. Hvorvidt bruk av hjemmesider er overføring av personopplysninger til utlandet slik loven nytter uttrykket er i dag usikkert. Datatilsynet har i noen tilfeller sett det slik at å gjøre personregistre tilgjengelig på en hjemmeside som er kontrollert fra Norge er *utlevering* av opplysningene, og ikke overføring til utlandet. Praksis er imidlertid ikke entydig. Hvordan dette spørsmålet bør reguleres i den nye loven er drøftet under 16.4.2.1.

16.3 INTERNASJONALE REGLER

16.3.1 Europarådskonvensjonen

Europarådskonvensjonen kapittel III artikkel 12 regulerer overføringer av personopplysninger til land som har ratifisert konvensjonen. Utgangspunktet etter konvensjonen er at man ikke kan forby eller kreve særlig tillatelse for overføring av personopplysninger som går til en annen parts territorium utelukkende med det formål å verne privatlivets fred (artikkel 12 nr 2). Det er likevel etter samme artikkel nr 3 adgang til å gjøre unntak fra dette utgangspunktet dersom ikke den annen parts regler gir tilsvarende beskyttelse:

- «3. Likevel skal hver part ha rett til å avvike fra bestemmelsene i punkt 2:
- a) I den grad dens lovgivning inneholder særskilte regler for visse kategorier av personopplysninger eller av elektroniske dataregistre, på grunn av disse opplysningers eller registres karakter, dersom ikke den annen parts regler gir tilsvarende beskyttelse;
 - b) når overføringen blir foretatt fra partens territorium ved hjelp av mellomledd på en annen parts territorium, for å unngå at slike overføringer fører til omgåelse av lovgivningen som er nevnt i begynnelsen av dette punkt.»

16.3.2 EF-direktivet

Direktivet skiller skarpt mellom overføring av personopplysninger til EØS-land og tredjeland. Artikkel 1 nr 2 bestemmer at det skal være *fri utveksling av personopplysninger mellom medlemslandene*:

- «1. Medlemsstatene sikrer i overensstemmelse med dette direktiv beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personopplysninger.
2. Medlemsstatene må ikke af grunde, der har forbindelse med den i stk. 1 foreskrevne beskyttelse, innskærpe eller forbyde fri utveksling af personopplysninger mellem medlemsstatene.»

Direktivet går lenger i å kreve fri overføring av personopplysninger enn Europarådskonvensjonen. (Europarådskonvensjonen tillater at medlemslandene innskrenker retten til overføring dersom «den annen parts regler [ikke] gir tilsvarende beskyttelse» som ens eget land, jf ovenfor). Nærmere presiseringer av hvordan direktivet må forstås er flettet inn i utvalgets vurderinger, se 16.4.1 nedenfor.

Når det gjelder overføring av personopplysninger til *tredjeland* (andre land enn EØS-land), gir direktivet utførlige regler i kapittel IV artiklene 25 og 26).

I *artikkel 25* oppstilles en rekke grunnprinsipper som skal sikre at videregivelse av opplysninger bare skjer til land som har et *tilstrekkelig beskyttelsesnivå* når det gjelder personvern. Hva som er «tilstrekkelig» i denne sammenheng, må vurderes konkret fra sak til sak på bakgrunn av bl a opplysningenes art, behandlingen(e)s formål og varighet, gjeldende rett i det aktuelle tredjeland, osv.

Medlemsstatene og Kommisjonen har gjensidig underrettelsesplikt overfor hverandre hvis de mener at bestemte tredjeland ikke har et tilstrekkelig beskyttelsesnivå.

Dersom Kommisjonen, etter å ha rådført seg med det utvalget som etter artikkel 31 opprettes med medlemmer fra alle medlemslandenes regjeringer, konstaterer at et tredjeland ikke sikrer et tilstrekkelig beskyttelsesnivå i forhold til videregivelse av visse typer opplysninger, plikter medlemslandene å sette i verk nødvendige tiltak for å hindre fremtidig videregivelse av personopplysninger av samme art til vedkommende tredjeland.

Kommisjonen kan etter artikkel 25 nr 5 gå inn i forhandlinger med tredjeland i et forsøk på å avhjelpe den situasjon som har oppstått etter at Kommisjonen har konstatert at beskyttelsesnivået i vedkommende land ikke er tilstrekkelig. Dersom resultatet av disse forhandlingene er positive, kan Kommisjonen i neste omgang, etter på nytt å ha rådført seg med ovennevnte utvalg, fastslå at vedkommende lands beskyttelsesnivå *er* tilfredsstillende, jf artikkel 25 nr 6. I så fall må også medlemslandene legge det til grunn deretter.

Det er overlatt til det enkelte medlemsland å utforme nærmere regler om anvendelsen av de prinsippene for videregivelse som oppstilles i artikkel 25. Det vil bli å være opp til det enkelte land å bestemme hvilke prosedyrer som skal følges på nas-

jonalt plan når det gjelder overførsel av opplysninger til tredjeland, og det vil også være landenes oppgave å bestemme hvilken myndighet som skal ta stilling til om et bestemt tredjeland har et tilstrekkelig beskyttelsesnivå.

Artikkel 26 pålegger medlemsstatene å tillate overføring av personopplysninger til tredjeland *uavhengig av* om vedkommende tredjeland har et tilstrekkelig beskyttelsesnivå når det gjelder personvern eller ikke.

Artikkel 26 inneholder til dels vide unntak fra hovedreglene om videregivelse i artikkel 25. Unntakene medfører altså at overføring i visse tilfelle kan skje selv om det aktuelle tredjeland ikke har et tilstrekkelig beskyttelsesnivå.

I artikkel 26 nr 1 bokstav a-f oppstilles en rekke alternative vilkår som kan berette overførsel av personopplysninger til tredjeland.

Etter nr 1 bokstav b kan overførsel foregå der det er nødvendig av hensyn til *gjennomføring* av en kontrakt eller en *kontraktsinngåelse* der den registrerte er part. Bestemmelsen må ses i sammenheng med artikkel 7 bokstav b (som tillater behandling av personopplysninger for kontraktsformål).

Etter nr 1 bokstav d kan overføring skje der det er nødvendig – eller er fastsatt i lov – for å beskytte viktige *samfunnsinteresser*, eller for at et *rettskrav* skal kunne fastlegges, gjøres gjeldende eller forsvares. Sistnevnte må ses i sammenheng med artikkel 8 nr 2 bokstav e (som tillater behandling av sensitive personopplysninger dersom dette er nødvendig for å forsvare et rettskrav).

Hva som er viktige samfunnsinteresser må vurderes konkret, men videregivelse kan f eks være påkrevet i forbindelse med internasjonal utveksling av opplysninger mellom skatte- og tollforvaltninger, eller mellom nasjonale sosial- og helsemyndigheter (se fortalen pkt 58).

Etter nr 1 bokstav e kan videregivelse skje der det er påkrevet av hensyn til den registrertes «*vitale interesser*». Denne bestemmelsen er parallell til – og må ses i sammenheng med – artikkel 7 bokstav d.

Overføring av personopplysninger til tredjeland er også omhandlet i fortalen punkt 56 – 60.

16.4 UTVALGETS VURDERINGER

På bakgrunn av direktivets regler er det nødvendig å skille mellom overføring av opplysninger til EØS-land og overføring av opplysninger til tredjeland.

16.4.1 Overføring av opplysninger til EØS-land

Som det fremgår foran krever direktivet at personopplysninger skal kunne utveksles fritt mellom medlemslandene (og EØS-landene), og utvalget legger dette til grunn. Fri utveksling antas å ha klare økonomiske og sosiale fordeler, se fortalen punkt 3) – 6).

Det er på det rene at implementeringen av direktivet fører til at det blir noe lettere enn før å overføre personopplysninger til EØS-land. Rettslig sett skal det være like lett å overføre opplysninger til andre EØS-land som å overføre opplysningene innenfor landets grenser. Overføringen av opplysningene over landegrenser skal ikke støte an mot større rettslige hindre enn innenlands overføring – overføring av opplysninger fra Oslo til Bergen skal rettslig sett likestilles med overføring av opplysninger fra Oslo til f eks Athen eller London.

Uttrykket «fri utveksling» av personopplysninger kan imidlertid lett gi opphav til misforståelser, og bør derfor presiseres. For det første vil utvalget for ordens skyld understreke at norske *taushetspliktregler* fremdeles er til hinder for at opplysninger gis videre – uansett om mottakeren befinner seg innenfor Norges grenser

eller i et annet EØS-land. For det andre gjelder direktivets krav om fri utveksling av personopplysninger bare *innenfor direktivets anvendelsesområde*, jf artikkel 3 og "*Lovens saklige og geografiske virkeområde*" i kapittel 10 foran. I dette ligger at vi står fritt til å bestemme hvilke regler som skal gjelde for overføring av personopplysninger på områder *som direktivet ikke regulerer* – f eks politiets og påtalemyndighetens registre (regler om overføring av opplysninger på slike områder er ofte undergitt særskilt regulering). For det tredje må direktivet forstås slik at overføring til et annet EØS-land kan nektes dersom det aktuelle landet *ikke har gjennomført EF-direktivet*, jf forutsetningsvis artikkel 1 nr 1. Endelig står det enkelte land fritt til å stille krav til *overføringsmåten*, så langt kravene er de samme for innenlands overføringer. Begrepet «fri utveksling» må forstås med disse begrensningene når det brukes i det følgende.

Selv med de presiseringene som er nevnt i forrige avsnitt kan en ikke se bort fra at personopplysninger som overføres fra Norge til andre EØS-land blir behandlet annerledes enn de ville blitt i henhold til det norske regelverket. Dette skyldes at direktivet gir medlemslandene en viss frihet til selv å velge hvordan reglene skal være. Og det er ikke bare ulikt regelverk som gjør at overføringer utgjør en fare for personvernet. Opplysninger som overføres plasseres dermed i en ny sosial og kulturell virkelighet – i en annen sammenheng – som gjør at opplysningene kan tillegges et annet innhold enn det de ble tillagt i avsenderlandet. Et stykke på vei kan disse farene avhjelpes ved at det stilles krav til måten opplysningene overføres på. Utvalget viser til de generelle materielle reglene (f eks om krav til sikkerhet) som også gjelder ved videregivelse av opplysninger til utlandet.

Det synes klart at regelen i personregisterloven § 36 første ledd (plikt til å innhente samtykke fra Datatilsynet) ikke er forenlig med direktivets krav om uhindret flyt av personopplysninger innenfor EØS-området. Noe mer tvilsomt kan det være om dagens ordning med meldeplikt (forskriften § 8-1) kan opprettholdes. Ordlyden i direktivet (eller fortalen) oppstiller ikke noe uttrykkelig forbud mot at det enkelte land holder seg orientert om hvilke opplysninger som sendes ut. En meldeplikt som utløses av en (planlagt) overføring vil heller ikke legge materielle hindringer i veien for overføringen. Muligens kan en slik meldeplikt likevel hevdes å stride mot prinsippet om fri flyt av personopplysninger, fordi det på den måten knyttes plikter til overføringen. Uansett foreslår ikke utvalget at overføring av personopplysninger i seg selv utløser meldeplikt. Meldeplikten vil avhenge av om overføringen er en type behandling som etter loven (og forskriften) er meldepliktig.

Datatilsynet vil i de fleste tilfeller være informert om overføringene i samband med den alminnelige konsesjons- eller meldepliktsordningen. Dette skyldes at opplysningene gjerne vil ha vært gjenstand for en eller annen form for behandling før de blir sendt ut av landet, og den forutgående behandlingen vil – ihvertfall der den representerer en personverntrussel – ha vært gjenstand for meldeplikt eller konsesjonsplikt. I så fall vil meldingen eller konsesjonssøknaden fortelle om opplysningene senere skal overføres til et annet land, og eventuelt til hvilke(t) land det er snakk om. Dersom den opprinnelige meldingen ikke inneholdt opplysninger om overførsel av opplysningene til utlandet, må ny melding sendes hvor de nye opplysningene fremgår. I de tilfeller hvor det ikke på forhånd er foretatt noen behandling som utløser meldeplikt i Norge, og overføringen representerer en meldepliktig behandling, vil overføringen måtte meldes til Datatilsynet etter de vanlige reglene. Enkelte overføringer vil ikke utløse meldeplikt, for eksempel når opplysningene som overføres er allment tilgjengelig, jf lovforslaget § 31 tredje ledd.

16.4.2 Overføring av opplysninger til tredjeland

For overføring av personopplysninger til tredjeland, dvs land utenfor EØS-området, gir direktivet det enkelte land større frihet til å utforme reglene selv. Riktignok oppstilles det som hovedregel at det ikke må overføres personopplysninger til land som ikke har et tilfredsstillende beskyttelsesnivå (jf artikkel 25, gjengitt ovenfor), men direktivet åpner som nevnt for en rekke unntak fra denne hovedregelen (jf artikkel 26).

Overføring av personopplysninger til tredjeland krever et mer nyansert regelverk enn overføring av opplysninger innenfor EØS-området. Dette aktualiserer noen problemstillinger som ikke gjør seg gjeldende for overføring innen EØS området, se oversikten i de tre neste avsnittene.

For det første må det trekkes en *nedre grense* for hva som skal omfattes av reglene – hvor mye skal til før det dreier seg om en overføring som loven bør regulere? (se 16.4.2.1).

For det andre oppstår spørsmålet om den norske loven bør gå lenger i å avskjære overføring enn det direktivet gjør. Hvilke overføringsmuligheter bør vi gjennomføre i norsk lov? (se 16.4.2.2).

For det tredje må utvalget ta stilling til hvilke vilkår som skal stilles for overføring av personopplysninger til tredjeland (16.4.2.3), og endelig må det vurderes hvilket behov det er for tilsyn med slik overføring. Bør det kreves samtykke (konsesjon), eller er det tilstrekkelig med meldeplikt? (se 16.4.2.4).

16.4.2.1 Grensen mot frie overføringer til tredjeland

Verken direktivet eller utvalgets lovforslag regulerer enhver form for overføring av personopplysninger til tredjeland, se grensedragningen bokstav a) – e) nedenfor. Det betyr at overføringer som ikke reguleres av direktivet kan skje selv om rettstilstanden i tredjelandet ikke har et tilstrekkelig beskyttelsesnivå.

16.4.2.1.1 Private aktiviteter

Utvalget presiserer at verken direktivet eller den norske loven får anvendelse på rent personlige aktiviteter (jf 10.1.3.4). Dette medfører at overføring av personopplysninger som ledd i slik aktivitet ikke omfattes av reglene nedenfor. Verken direktivet eller loven er f eks til hinder for å sende personlig e-post til en venn i Afrika, og dette skal heller ikke meldes til tilsynsmyndigheten.

16.4.2.1.2 Skal opplysningene videregis?

I tråd med direktivet regulerer utvalgets lovforslag kun *videregivelse* av opplysninger til tredjeland. Dette fører bl a til at mange former for midlertidig overføring ikke reguleres. Et eksempel kan være at en forretningsmann tar med sin bærbare PC til USA. Dersom forretningsmannen beholder opplysningene for seg selv, finner det ikke sted noen videregivelse.

16.4.2.1.3 Overføring innen EØS-området via tredjeland

I redegjørelsen for gjeldende rett ble det pekt på at den som overfører elektronisk bare kan bestemme mottaker, og ikke hvilken «rute» opplysningene skal ta. Dette kan som nevnt f eks føre til at opplysninger som skal overføres til en adressat innenfor Norges grenser overføres via utlandet. Lovforslaget omfatter bare overføring av opplysninger som skal *videregis til tredjelandet*. Ved en ren transport via tredjelan-

det finner det åpenbart ikke sted noen videregivelse, og dette reguleres ikke av utvalgets lovforslag. Mer tvil knytter seg til tilfellene der opplysningene *mellomlagres i utlandet* som ledd i transitt. Det kan hevdes at mellomlagringen er videregivelse. På den andre siden ville en slik bokstavelig tolkning føre til uholdbare tilstander – dette understrekes allerede av at avsenderen normalt ikke har noen anelse om det skjer mellomlagring eller ei.

16.4.2.1.4 *Bruk av internasjonale kommunikasjonskanaler*

Bruk av internasjonale kommunikasjonskanaler som for eksempel Internett blir stadig mer utbredt, og nye overføringsmåter reiser spørsmål om bruken skal anses som overføring av personopplysninger. Noe generelt svar kan neppe gis – her som ellers må hver kommunikasjonsform vurderes for seg. Nedenfor gis noen nærmere vurderinger knyttet til et par eksempler på kommunikasjonsmuligheter som Internett gir.

Overføring av opplysninger via *e-post* må i utgangspunktet likestilles med bruk av andre kommunikasjonskanaler. Det forhold at oversendelsen skjer via Internett bør ikke i seg selv føre til at e-post undergis egne regler. Dersom e-post skal reguleres på annen måte enn andre kommunikasjonskanaler, må begrunnelsen være at særlige grunner tilsier dette. Det betyr at kommunikasjon via e-post til en mottager i Norge ikke er å anse som overføring (selv om posten går via utlandet). Det motsatte vil være tilfelle dersom mottageren befinner seg i utlandet. Den beste måten å vareta diskresjonsinteressen er formentlig å gjøre brukerne oppmerksomme på at man tar visse risiki ved å benytte ubeskyttet e-post. På denne måten er det opp til brukerne selv å avgjøre i hvilke tilfelle e-post er en hensiktsmessig kommunikasjonskanal.

Ved bruk av *hjemmesider* gjøres informasjon tilgjengelig også i utlandet. Mange hjemmesider vil allerede i utgangspunktet være unntatt fra direktivets og lovens anvendelsesområde: Rent personlige (private) hjemmesider omfattes ikke, jf 10.1.3.4. Virksomheters hjemmesider omfattes bare når de inneholder personopplysninger, jf 10.1.1.3 (f eks ren produktinformasjon omfattes ikke).

Hjemmesidene man etter dette står igjen med, kan reguleres på to forskjellige måter. For det første kan man videreføre dagens praksis, slik at å legge ut personopplysninger på en hjemmeside som kontrolleres fra Norge anses som *utlevering* av opplysningene. I så fall sondres det ikke mellom å gjøre opplysningene tilgjengelige innenfor eller utenfor landets grenser. Velges denne løsningen, reguleres bruk av hjemmesider på Internett av de vanlige reglene for utlevering av personopplysninger (f eks taushetspliktlovgivning) – grenseoverskridelsen fører ikke til særregulering.

En innvending mot å se på slik publisering som et spørsmål om utlevering (og ikke overføring til utlandet) er at det kan være mer betenkelig å gjøre opplysningene tilgjengelig i tredjeland enn innenfor landets grenser. Når opplysningene først gjøres tilgjengelige, er sjansen stor for at de også vil bli lastet ned og brukt i et land der norsk lov ikke gjelder, og hvor Datatilsynet ikke har jurisdiksjon. *Alternativet* til å se på bruk av hjemmesider som utlevering, er derfor å se på slik bruk som *overføring av personopplysninger til utlandet*, og la slik bruk (i utgangspunktet) følge reglene som foreslås senere i dette kapitlet.

Utvalget går inn for at publisering på Internett (f eks ved bruk av hjemmeside) er å anse som overføring av personopplysninger til utlandet. Se forøvrig "[Forholdet til yttringsfriheten](#)" i kapittel 17 om forholdet til yttringsfriheten.

16.4.2.2 Hvilke overføringsmuligheter bør gjennomføres i norsk lov?

Direktivet artikkel 26 går langt i å tillate overføring av personopplysninger til tredjeland selv om beskyttelsesnivået ikke er tilstrekkelig. Det er opp til det enkelte land å bestemme om alle mulighetene skal benyttes. For utvalget har det vært avgjørende å se hen til *om personvern hensyn varetas på en tilstrekkelig god måte* dersom unntakene gjennomføres i norsk rett. Enkelte av unntaksmulighetene i artikkel 26 har i så måte voldt noe tvil. Dette gjelder unntaket i artikkel 26 nr 2 om at overføring kan finne sted dersom det gis avtalegarantier for hvordan opplysningene skal behandles i tredjelandet – den opplysningene gjelder vil normalt ikke være part i avtalen og av den grunn ikke ha noe innflytelse på innholdet.

Utvalget har likevel kommet til at adgangen som direktivet gir til å overføre opplysninger til tredjeland bør benyttes fullt ut. Begrunnelsen for dette er flerdelt. For det første er det vanskelig å ha oversikt over når det kan oppstå legitime behov for å overføre personopplysninger. Følgende eksempel kan illustrere poenget: De færreste U-land lovregulerer personvernsspørsmål på en tilfredsstillende måte. Samtidig kan det tenkes situasjoner – for eksempel i forbindelse med et bistandsprosjekt – som kan forsvare at det overføres personopplysninger. Hvilke behov for overføring som kan oppstå i fremtiden er det vanskelig å ha noen kvalifisert oppfatning av i dag, og det er formålstjenlig at loven gir anledning til å løse slike lite forutsigbare behov på en smidig måte. For det andre har det liten betydning å lage strenge regler dersom et annet EØS-land går lenger i å tillate overføring til tredjeland. Det mer restriktive norske regelverket kan lett omgås ved først å overføre opplysningene til det mer liberale EØS-landet, for deretter å overføre det til den endelige destinasjonen. Dette siste forholdet tilsier nært samarbeid mellom EØS-landene både på lovgiverplan og mellom tilsynsmyndighetene.

Under enhver omstendighet er det på det rene at det må etableres rutiner for kontroll av overføring av personopplysninger til tredjeland. Formålet med tilsynet er å sikre at overføringen er forsvarlig ut fra personvern hensyn, se nedenfor 16.4.2.4.

16.4.2.3 Vilkår for overføring til tredjeland

Som det fremgår ovenfor mener utvalget det må legges avgjørende vekt på en vurdering av hvor god personvernbeskyttelse det aktuelle tredjelandet har. Som en følge av at EØS-landene og Kommisjonen må vurdere de ulike tredjelandenes personvernregler vil det raskt etableres en (også for Norge) veiledende praksis.

I tråd med direktivet foreslår utvalget at overføring av personopplysninger kan finne sted dersom beskyttelsesnivået i det aktuelle tredjelandet er *tilstrekkelig*. Hvorvidt beskyttelsesnivået er tilstrekkelig, skal vurderes ut fra alle reguleringsmetodene som det aktuelle tredjelandet anvender. Viktige momenter i vurderingen av beskyttelsesnivået gis i artikkel 25 nr 2. For eksempel skal det blant annet legges vekt på opplysningenes art og formålet med behandlingen av personopplysningene. Momentene er omtalt i merknadene til lovforslaget § 29. Utvalget vil her nøye seg med å peke på at direktivets oppregning av momenter ikke er uttømmende. Dette betyr at Datatilsynet kan se hen til ytterligere momenter i vurderingen av om beskyttelsesnivået er tilstrekkelig. Et moment som direktivet ikke nevner, men som det er naturlig å tillegge betydelig vekt, er om det aktuelle tredjelandet har forpliktet seg til å oppfylle Europarådets konvensjon (se "[Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse](#)" i kapittel 7).

I tillegg til at overføring av personopplysninger kan skje til tredjeland med et tilstrekkelig beskyttelsesnivå, foreslår utvalget at man i tråd med direktivet i visse tilfelle tillater overføring selv om beskyttelsesnivået i det aktuelle tredjelandets lov-

giving ikke er tilstrekkelig. Artikkel 26 gir i alt 6 muligheter til eksport til land som ikke har lovgivning med et tilfredsstillende beskyttelsesnivå (se nr 1 bokstav a) – f). Vilkårene er nærmere behandlet i spesialmotivene (se merknadene til lovforslaget § 30). I tillegg kan overføring finne sted dersom mottakeren av personopplysningene gir tilstrekkelige garantier for at privatlivets fred og personenes grunnleggende rettigheter og friheter beskyttes. Garantiene kan fortrinnsvis hjemles i kontraktsbestemmelser, herunder standardkontrakter (jf artikkel 26 nr 4).

Utvalget foreslår også at bestemmelsen i forskriften § 8-1 siste ledd videreføres, slik at overføring kan skje når internasjonale forpliktelser krever dette.

16.4.2.4 Behov for tilsyn med overføringen?

Overføring av personopplysninger til tredjeland kan bare finne sted dersom nærmere bestemte vilkår er oppfylt. Vilkårene vil være nedfelt i loven, og må i utgangspunktet som for all annen lovgivning tolkes av borgerne selv. Det synes imidlertid klart at Datatilsynet – ihvertfall på noen områder – må føre kontroll med at vilkårene for overføringen er oppfylt. Det vil fremgå av meldingsskjemaene, eventuelt konsesjonssøknadene, hvorvidt en har til hensikt å videregi personopplysningene til et tredjeland (se 16.4.1). Dersom den opprinnelige meldingen ikke inneholdt opplysninger om overførsel av opplysningene til utlandet, må ny melding sendes hvor de nye opplysningene fremgår.

Datatilsynet må ha kompetanse til å nekte eller sette vilkår for fortsatt overføring.

Loven bør suppleres med forskriftshjemmel slik at justeringer kan foretas uten å måtte gå veien om lovendring.

KAPITTEL17

Forholdet til ytringsfriheten**17.1 INNLEDNING****17.1.1 Oversikt over problemstillingen og utvalgets forslag**

Personregisterlovens regler om krav til saklighet og regler om innsyn, retting og sletting m m gjelder også for f eks pressens personregistre. I forhold til personregisterloven har likevel ytringsfrihetsspørsmål vært lite påaktet. At problemstillingen nå har kommet på dagsordenen, skyldes flere forhold som stikkordsmessig kan oppsummeres som nye teknologiske muligheter til å behandle personopplysninger, et mer omfattende saklig virkeområde for loven og flere lovregler om behandling av personopplysninger. Utvalget drøfter i dette kapitlet i hvilken grad det er nødvendig å gjøre unntak fra lovens regler for å finne en rimelig balanse mellom hensynene til personvern og ytringsfrihet. Direktivet artikkel 9 åpner for at slike unntak kan gjøres (se nærmere om artikkel 9 nedenfor).

Utvalget foreslår at det gjøres unntak fra loven der dette er nødvendig for å forene hensynet til ytringsfrihet med personvern. Hvor langt unntaket rekker, beror bl a på tolkningen av Grunnlovens og andre overordnede rettsnormers vern av ytringsfriheten. Dette innebærer at unntak må gjøres der det ville stride mot Grunnloven og internasjonale forpliktelser å la personopplysningsloven få anvendelse. Unntaket åpner imidlertid for at unntak også kan gjøres selv om den aktuelle interessen i ytringsfrihet ikke har grunnlovsværn. Om slike unntak skal gjøres beror på en avveining av personverninteresser mot hensynet til ytringsfrihet. Utvalget gir flere eksempler på hvordan slike avveininger kan gjøres.

17.1.2 Ytringsfrihetskommisjonens arbeid

Regjeringen har ved kongelig resolusjon 23 august 1996 nedsatt en ytringsfrihetskommisjon som vil se nærmere på avgrensningen av grunnlovsværnet for ytringsfrihet mot andre grunnleggende rettigheter og verdier. I kommisjonens mandat (jf pkt 5) heter det blant annet at et sentralt punkt i kommisjonens arbeid vil være å foreta en prinsipiell drøftelse av de interesser som kan komme i strid med denne friheten, og foreta en avveining av disse interessene i forhold til ytrings- og informasjonsfriheten. Utvalget legger til grunn at personvern hensyn er en interesse som ytringsfrihetskommisjonen kommer til å avveie i forhold til ytrings- og informasjonsfriheten. Kommisjonen skal avgi sin innstilling senest 1 juli 1999.

17.1.3 Oversikt over resten av kapitlet

Kapitlet er bygget opp slik at det først gjøres nærmere rede for bakgrunnen til og innholdet i artikkel 9 (17.3). Deretter forklares innholdet i de norske og internasjonale reglene som har betydning for unntaksvurderingene (17.4), før utvalget kommer med sine vurderinger (17.5). Men aller først er det av interesse å undersøke hvordan noen europeiske land (herunder Norge) i dag regulerer forholdet mellom personregisterlovgivning og ytringsfrihet.

17.2 GJELDENE RETT I NORGE OG NOEN ANDRE EUROPEISKE LAND

Personregisterloven inneholder ikke særregler eller unntak for personregistre som benyttes til de aktivitetene som direktivet nevner i artikkel 9 (jf 17.3). Lovens regler om f eks den enkeltes rett til innsyn i registrerte opplysninger om en selv og reglene om plikt til å rette eller slette uriktige personopplysninger gjelder også for personregistre som f eks benyttes til journalistiske formål. Det eneste unntaket for denne type virksomhet finnes i personregisterforskriften § 2-14 som unntar dags- og ukepressens personregistre til bruk i journalistisk virksomhet fra konsesjonsplikten i personregisterloven § 9.

Andre europeiske stater synes pr i dag å ha regulert forholdet til personregisterlovgivningen på tre forskjellige måter. I enkelte stater inneholder ikke personregisterlovgivningen noe uttrykkelig unntak for media. Dette er situasjonen i bl a Belgia, Spania, Portugal, Sverige og Storbritannia. Andre stater – herunder bl a Norge, Tyskland, Frankrike, Nederland, Østerrike, Finland og i noen grad Italia – har valgt å gjør unntak for media fra deler av personregisterlovgivningen. Endelig har noen stater som f eks Danmark valgt å unnta media fra anvendelsesområdet til den generelle personregisterlovgivningen, og i stedet gi særregler for slik virksomhet.

Oversikten i avsnittet ovenfor illustrerer ulike lovtekniske løsninger, men gir ikke sikre holdepunkter for hvordan de nevnte statene har avveid hensynet til ytringsfrihet mot personvern hensyn. For å vurdere dette, må man bl a også ta hensyn til konstitusjonelle regler, ulovfestede regler og tilsynsmyndighetenes praksis i det enkelte land.

17.3 NÆRMERE OM DIREKTIVET ARTIKKEL 9

I følge direktivet artikkel 9 skal medlemstatene gjøre unntak fra de fleste av de alminnelige reglene for behandling av personopplysninger som utelukkende finner sted i journalistisk øyemed eller i kunstnerisk eller litterær virksomhet i den grad det er nødvendig for å forene retten til privatlivets fred med reglene for ytringsfrihet. Unntak kan gjøres fra de alminnelige reglene om behandling av personopplysninger (direktivet kapittel II), videregivelse av opplysninger til tredjeland (direktivet kapittel IV) og reglene om tilsynsmyndighetens kompetanse m v (direktivet kapittel VI). Derimot kan det ikke gjøres unntak for media fra reglene i direktivet kapittel I (alminnelige bestemmelser), kapittel III (rettsmidler, ansvar og sanksjoner), kapittel V (atferdskodekser) og kapittel VII (gjennomføringsbestemmelser). I det britiske høringsnotatet (Consultation Paper on the EC Data Protection Directive pkt 4.19 – Home Office 1996) og i Kommisjonens rekommandasjon 1/97 pkt 3 er det uttrykkelig sagt at et *generelt* unntak for enkelte bransjer, f eks pressens virksomhet, ikke er forenlig med direktivet. Utvalget forstår dette slik at unntak kun kan gjøres der dette er nødvendig av hensynet til ytringsfriheten.

I Kommisjonens rekommandasjon 1/97 oppstilles flere retningslinjer for hvordan artikkel 9 bør gjennomføres i den enkelte stats interne rett. Blant annet understrekes det at unntak må bygge på *proporsjonalitetsprinsipper* i den forstand at det bare kan gjøres unntak fra direktivbestemmelser som kan true ytringsfriheten, og bare så langt det er nødvendig for å oppnå en tilfredsstillende balanse mellom hensynet til personvern og ytringsfriheten.

Videre fremheves det at unntak ikke er nødvendig dersom direktivbestemmelsene (og forutsetningsvis de enkelte lands forslag til lovbestemmelser) er formulert på en så smidig måte at hensynet til media m v kan varetas på en tilstrekkelig måte innenfor de rammene bestemmelsens ordlyd setter.

For det tredje fremgår det at unntak ikke kan gis utelukkende til utvalgte yrkesgrupper som f eks journalister. Unntakene må gjelde for enhver som behandler personopplysninger for et *journalistisk formål*. Det er således hensikten med og arten av behandlingen som er avgjørende, og ikke den formelle yrkesmessige statusen til den som forestår behandlingen.

Rekommandasjonen tydeliggjør også at direktivet forutsetter en avveining av to grunnleggende interesser, og at et viktig moment i denne interesseavveiningen er om og eventuelt i hvilken grad den registrerte gis rettigheter i forhold til media – som f eks rett til å komme med replikk eller få rettet uriktige opplysninger. Mer generelt er det av interesse om det foreligger atferdsnormer (som f eks «Vær varsom-plakaten») som tar hensyn til den registrertes interesser.

17.4 OMRISS AV GRL § 100 OG EMK ARTIKKEL 8 OG 10 SOM SKRANKER FOR NY LOV OM BEHANDLING AV PERSONOPPLYSNINGER

Ytringsfriheten beskyttes i norsk rett av Grl § 100. Første punktum slår fast at «Trykkefrihed bør finde Sted». Ordet «bør» må leses som «skal». Grunnloven oppstiller med andre ord et absolutt forbud mot at det innføres et system med forhåndssensur av bøker eller andre trykte skrifter. Også ordet «Trykkefrihed» må fortolkes på sin historiske bakgrunn. Bestemmelsen ble gitt som en reaksjon mot det gamle sensursystemet. Det Grunnlovens forfattere først og fremst ville forby var en administrativ og endelig avgjørende forhåndssensur, hvor en skriftlig ytring kunne forbys uten at ytringens lovlighet ble prøvet av domstolene (jf Bredo Morgenstjerne, Lærebog i Den norske statsforfatningsret, 2 utg Kristiania 1909 s 638). Juridiske forfattere har imidlertid vært enige om at bestemmelsen også beskytter mot et sensursystem som er underlagt domstolenes judisielle prøvelse. Grunnloven § 100 første punktum må derfor sies å beskytte friheten til å trykke et hvilken som helst skrift uten at dette betinges av en forutgående prøvelse av skriftets lovlighet. Det er verdt å merke seg at Grunnloven på dette punkt ikke sonderer mellom skriftlige ytringers innholdsmessige karakter. Bestemmelsen beskytter ikke bare tradisjonell journalistisk virksomhet, men enhver som tar sikte på publisering i et trykt skrift (f eks historikere, forfattere etc). Videre ville friheten til å trykke vært meningsløs uten friheten til å *utgi* trykte skrifter. Grunnloven § 100 første punktum sikter derfor ikke bare mot den tekniske trykkeprosessen. Bestemmelsens siktemål er å forby at det legges hindringer i veien for publikasjonen av trykte skrifter (Slik også Eggen i uttrykt vedlegg side 4).

Ytringsfriheten beskyttes også av artikkel 10 i den europeiske menneskerettighetskonvensjonen (EMK) og artikkel 19 i FN's konvensjon om sivile og politiske rettigheter (SP). Ordlyden i EMK artikkel 10 er nokså lik ordlyden i SP artikkel 19. Sett hen til at Den europeiske menneskerettighetskommisjonen og – domstolen har tolket artikkel 10 på en måte som gjør at den har fått omfattende rekkevidde, kan det vanskelig tenkes at SP artikkel 19 setter mer omfattende skranker for lovgivningsmakten (jf Eggen side 1). Utvalget har derfor i hovedsak lagt vekten på EMK artikkel 10, jf direktivets fortale pkt 37. EMK artikkel 8 beskytter privatlivet, og Menneskerettighetsdomstolen har i sin praksis utviklet bestemmelsen slik at den også setter skranker for elektronisk behandling av personopplysninger, jf 9.3.

17.5 UTVALGETS VURDERINGER

17.5.1 Innledning

Utvalget har tidligere pekt på at direktivet nytter uttrykket «behandling av personopplysninger» på en måte som gjør at direktivets saklige anvendelsesområde blir meget omfattende. Meget av det som ligger innenfor arbeidsområdet til f eks en journalist – f eks arkivundersøkelser, intervjuer, reportasjearbeid m v – vil kunne omfattes (i den grad dette representerer elektronisk behandling eller det opprettes manuelle personregistre).

Hensynet til personvern vil et stykke på vei være varetatt gjennom annen lovgivning som har særlig stor betydning for medias behandling av personopplysninger, som f eks injurielovgivningen og taushetspliktbestemmelser (som begrenser tilgangen til f eks opplysninger om personlige forhold), og brudd på denne lovgivningen kan forfølges rettslig. I tillegg har f eks pressen tradisjonelt lagt vekt på atferdsnormer (som f eks «Vær Varsom-plakaten og Redaktørplakaten») og selvdømmeordninger (som f eks Pressens Faglige Utvalg, Fagpressens Faglig-etiske utvalg og NRKs klagenemnd). Det må også tillegges vekt at pressen skal fylle funksjonen som «den fjerde statsmakt» og uavhengig samfunnsrefser, noe som kan gjøre det nødvendig og ønskelig at myndighetene viser en viss tilbakeholdenhet med myndighetsinngrep og regulering.

På den annen side må det også tas i betraktning at ny teknologi øker mulighetene både for organisasjoner, virksomheter og enkeltpersoner til å behandle personopplysninger med tanke på publisering, og de færreste av disse vil ta hensyn til massemedias egne regler og selvdømmeordninger. Å lage differensierte regler ut fra i hvilken grad den som benytter seg av ytringsfriheten respekterer slike bransjevise atferdsnormer er praktisk vanskelig og av hensyn til ytringsfriheten prinsipielt betenkelig.

Vurderingen av hvilke unntak og modifikasjoner som bør gjøres fra de alminnelige regler av hensyn til ytringsfriheten må skje bl a på grunnlag av Grl § 100 og EMK artikkel 10. Utvalget har på denne bakgrunn valgt å gi en generell regel som gjennomfører direktivet artikkel 9 (se lovforslaget § 5). En slik generell regel tar hensyn til at de overordnede reglene om ytringsfrihet ikke er statiske, men i stadig utvikling (særlig gjelder dette EMK artikkel 10). Nedenfor gis noen eksempler på hvordan unntaksbestemmelsen vil virke. Det sondres i den forbindelse mellom unntak fra materielle regler (dvs regler som direkte sier noe om hvordan personopplysninger kan eller skal behandles), og regler om Datatilsynets kontroll.

17.5.2 Eksempler på unntak fra lovens materielle regler

Enkelte av lovens materielle bestemmelser vil det meget sjelden være behov for å gjøre unntak fra for å finne frem til en rimelig balanse mellom personvern og hensynet til ytringsfriheten. Dette gjelder f eks de generelle bestemmelsen om at personopplysninger bare kan samles inn til lovlige og uttrykkelig angitte formål og bestemmelsen om sikring av personopplysninger. I forhold til andre lovbestemmelser vil derimot slike unntak som den store hovedregelen være påkrevet. Dette gjelder f eks bestemmelsene om bruk av sensitive personopplysninger (lovforslaget § 9), og om bruk av personopplysninger til andre formål enn de opprinnelig er innsamlet for (lovforslaget § 8).

I forhold til en del bestemmelser kan unntaksvurderingen føre til at bestemmelsen delvis får anvendelse så langt dette er forenlig med en rimelig balanse mellom personvern og ytringsfrihet. Dette gjelder f eks bestemmelsen som pålegger den behandlingsansvarlige plikt til å varsle den registrerte når det samles inn

opplysninger fra andre kilder enn den registrerte selv (lovforslaget § 21). I en del tilfelle kan hensynet til ytringsfriheten varetas innenfor den rammen bestemmelsens ordlyd setter – for eksempel slik at det ikke er påkrevet med varsel fordi dette ville være «uforholdsmessig vanskelig» (jf lovforslaget § 21 annet ledd). Dette er imidlertid ikke alltid tilstrekkelig for å finne frem til en tilfredsstillende balanse mellom personvern og hensynet til ytringsfriheten. Plikt til å varsle på et tidlig stadium i journalistiske undersøkelser kan f.eks. undergrave muligheten til å hemmeligholde reportasjeideer, hvilket igjen kan redusere f.eks. journalisters og forfatters mulighet til å sette dagsorden for den offentlige debatt. Varslingsplikten må derfor under enhver omstendighet modifieres slik at det ikke er å nødvendig å varsle før opplysningene publiseres. Og dersom varslingsplikten da ville være «uforholdsmessig vanskelig», faller plikten helt bort.

For de ulike innsynsreglene blir spørsmålet om slike regler kan komme i strid med prinsippet om journalisters *kildevern* (jf Eggen side 2 og 16 flg.). Med kildevern menes i vår sammenheng en rett til å nekte å oppgi hvem som har gitt fra seg personopplysningene som er eller som vil bli behandlet. Kildevernet er ikke direkte beskyttet av Grunnloven § 100, og det oppstår neppe noen problemer i forhold til den konstitusjonelle beskyttelsen av ytringsfriheten. EMK artikkel 10 verner imidlertid behovet for kildebeskyttelse. Ethvert inngrep i denne friheten må kunne forsvares som nødvendig i et demokratisk samfunn. I en kjent sak (EMD case of Goodwin vs the UK, judgement of 27 mars 1996, § 39 annet avsnitt) uttalte Menneskerettighetsdomstolen bl.a. at beskyttelse av kilder er en grunnleggende forutsetning for pressefrihet, og at inngrep i dette vernet krever sterke grunner («overriding requirement in the public interest»). I den utstrekning innsyn vil krenke kildevernet må altså Datatilsynets eller den registrertes innsynsrett kunne begrunnes i tungtveiende grunner for at innsynsretten skal være forenlig med EMK artikkel 10, og nødvendighetsvurderingen må prinsipielt sett foretas i konkrete enkeltsaker. På bakgrunn av den vekt Den europeiske menneskerettighetsdomstolen tillegger kildevernet vil inngrep i dette vernet i form av innsynsrett bare helt unntaksvis kunne forsvares.

Plikten til å gi den som ber om det generell informasjon om behandling av personopplysninger (lovforslaget § 16) er imidlertid så generell og har et så begrenset omfang at det ikke skaper problemer i forhold til kildevernet, se merknadene til denne bestemmelsen.

Videregivelse av personopplysninger til utlandet kan for eksempel skje ved at opplysningene gjøres tilgjengelige på Internett eller via andre internasjonale informasjonskanaler (se nærmere "*Overføring av personopplysninger til utlandet*" i kapittel 16), eller ved at personopplysninger som er publisert i f.eks. en biografi eller i en avis kjøpes i Norge og tas med til utlandet. Felles for disse overføringsmåtene er at de gjerne er utslag av behandling av personopplysninger i journalistisk øyemed, eller foretatt som ledd i kunstnerisk eller litterær virksomhet. I slike tilfeller må det gjøres unntak fra reglene om videregivelse av opplysningene til utlandet.

17.5.3 Unntak fra Datatilsynets kontroll

Et krav om konsesjon for å behandle personopplysninger som ledd i f.eks. journalistisk virksomhet ville reist spørsmål i forhold til Grunnloven § 100 første punktum. Selv om formålet med en konsesjonsordning ikke er å etablere noe sensurssystem, vil konsesjonsordningen innebære at et administrativt organ (Datatilsynet) har kompetanse til å utøve et betydelig skjønn ved sin konsesjonsbehandling, både mht om konsesjon skal gis og eventuelt på hvilke vilkår. Det kan hevdes å være en teoretisk mulighet for at det i konsesjonsvurderingen kan komme til å bli tatt hensyn til

søkerens politiske profil, forholdet til offentlige myndigheter, avisens innhold etc. At det finnes en slik teoretisk mulighet kan tale for å anse konsesjonsplikt som brudd på Grunnlovens forbud mot forhåndssensur, se om en lignende problemstilling Eivind Smith: Konstitusjonelle sider av lovgivning om eierbegrensninger m v i media (Vedlegg VI til NOU 1995: 3 s 143). Lovforslaget legger imidlertid opp til at det bare skal være konsesjonsplikt for behandling av sensitive personopplysninger der opplysningene benyttes til å treffe enkeltvedtak eller andre enkeltavgjørelser som direkte får rettsvirkninger for enkeltpersoner, jf lovforslaget § 33 og § 2 nr 9. Virksomhet som nevnt i artikkel 9 fyller ikke disse vilkårene og vil derfor uansett ikke være konsesjonspliktig. Det vil derfor ikke være nødvendig å gjøre unntak fra konsesjonsplikten av hensyn til ytringsfriheten (slik også Eggen side 4).

Lovforslagets bestemmelser om meldeplikt (se lovforslaget §§ 31 og 32) vil i utgangspunktet få anvendelse på all elektronisk behandling av personopplysninger, herunder behandling av personopplysninger i journalistisk øyemed og kunstnerisk eller litterær virksomhet. Meldeplikten innebærer ikke noe krav om forhåndsgodkjenning av et administrativt organ, men krever at det sendes inn et skjema som på generelt grunnlag beskriver behandlingen av personopplysningene.

Utvalget kan ikke se at Grl § 100 skulle være til hinder for at også behandling av personopplysninger i bl a journalistisk øyemed omfattes av meldeplikten (slik også Eggen side 8 flg). Meldeplikten gjelder bare generelle opplysninger og ikke opplysninger om den enkelte sak. Det er bare et spørsmål om å gi slik generell informasjon til Datatilsynet, og ikke tale om å etablere grunnlag for noen form for sensur. Det vil derfor ikke være nødvendig å gjøre unntak fra reglene om meldeplikt av hensyn til ytringsfriheten. Spørsmål om å gjøre et slikt unntak blir derfor et spørsmål om hensiktsmessighet.

Det vil variere i hvilken grad Datatilsynet vil kunne gjøre seg nytte av informasjonen som følger av meldingen. For f eks etablert pressevirksomhet er det usikkert om meldingen vil bringe frem opplysninger som ikke allerede er kjent. For andre grupper, f eks virksomheter, organer og enkeltpersoner som benytter seg av ny teknologi til å publisere ytringer, kan meldingene gi informasjon som ikke tidligere var kjent, og som anses som verdifull av hensynet til varetakelse av personvernet. Når utvalget ikke velger å gå inn for et generelt unntak fra meldeplikt for f eks behandling av personopplysninger i journalistisk øyemed, skyldes dette blant annet at artikkel 9 er utformet så vidt at den omfatter mer enn tradisjonell journalistikk, og at det av hensynet til ytringsfriheten neppe bør finne sted noen forskjellsbehandling (se nærmere om dette foran 17.3). Den behandlingsansvarlige ville dessuten uansett ha plikt til å ha visse opplysninger tilgjengelige, jf lovforslaget § 16. Meldeplikten bør derfor gjelde generelt (en annen ting er at pressens behandling av personopplysninger i mange tilfeller vil være unntatt fra meldeplikt etter lovforslaget § 31 tredje ledd).

Forsåvidt gjelder Datatilsynets tilgang på opplysninger (lovforslaget § 38) vises det til fremstillingen foran om unntak fra de materielle reglene, der det konkluderes med at Datatilsynets og den registrertes innsynsrett bør vike i den grad innsynet kommer i konflikt med hensynet til kildevern.

Datatilsynet kan med hjemmel i lovforslaget § 40 gi pålegg om at behandling i strid med loven skal opphøre eller stille vilkår som må oppfylles for at behandlingen skal være i samsvar med loven. Dersom pålegget ikke overholdes kan Datatilsynet ilegge den avgjørelsen retter seg mot en daglig løpende mulkt (lovforslaget § 41).

For virksomhet som omfattes av direktivet artikkel 9 vil Datatilsynets kompetanse til å gi pålegg være begrenset til de tilfellene hvor man ikke har funnet det nødvendig å gjøre unntak fra de materielle reglene av hensyn til ytringsfriheten.

Spørsmålet her blir om det av hensyn til ytringsfriheten er grunn til å gjøre ytterligere unntak fra Datatilsynets påleggskompetanse.

Utvalget har ikke funnet grunn til å unnta virksomhet som omfattes av direktivet artikkel 9 fra Datatilsynets kompetanse etter §§ 40 og 41 generelt. Utvalget vil imidlertid presisere at hensynet til ytringsfriheten tilsier at Datatilsynet viser stor tilbakeholdenhet med å bruke denne kompetansen. Grunnloven § 100 er overordnet loven om behandling av personopplysninger og legger føringer på Datatilsynet sin virksomhet. Kompetansen i §§ 40 og 41 må også utøves slik at den ikke kommer i konflikt med Norges internasjonale forpliktelser.

I de tilfellene hvor Datatilsynet ikke finner det mulig eller hensiktsmessig å bruke sin påleggskompetanse, kan det være aktuelt for Datatilsynet å utøve en ombudsfunksjon, hvilket innebærer å komme med kritikk og sette søkelyset på problemstillinger som er viktige ut fra personvern hensyn (dette kan f.eks. gjøres i årsmeldingen, jf direktivets fortale pkt 37 siste punktum).

Å sørge for at de av lovens regler som gjelder blir respektert, bør for øvrig på området for artikkel 9 først og fremst være en oppgave for de behandlingsansvarlige selv og de forbund og organisasjoner de er medlemmer av (se om pressens etiske regler og selvdømmeordninger i 17.5.1).

Direktivet gir ikke adgang til å unnta fra sanksjoner og domstolskontroll. Dette følger av at direktivet kapittel III som inneholder regler om rettsmidler, ansvar og sanksjoner ikke omfattes av unntakshjemmelen i artikkel 9. Også domstolene må imidlertid tolke lovens bestemmelser i lys av hensynet til ytringsfrihet.

17.5.4 Litt om hva som er journalistisk øyemed og kunstnerisk eller litterær virksomhet

Det er tidligere påpekt at unntak etter artikkel 9 ikke kan gis utelukkende til utvalgte yrkesgrupper, men at unntakene må gjelde for enhver som behandler personopplysninger i *journalistisk øyemed eller for kunstnerisk eller litterær virksomhet*.

Hvorvidt formålet med og arten av behandlingen faller inn under disse kategoriene må avgjøres konkret. Det er således ikke sikkert at enhver publisering fra en etablert pressevirksomhet skjer i journalistisk øyemed. Samtidig kan en rekke publiseringer fra andre typer virksomheter, enkeltpersoner og organisasjoner skje i slikt øyemed selv om dette ikke vanligvis omfattes av virksomhetens eller organisasjonens formål. En slik grensedragnings har også vært foretatt etter personregisterloven i dag. I vedtak 28 februar 1997 stadfestet Justisdepartementet Datatilsynets vedtak om avslag på søknad fra Økonomisk Rapport om tillatelse til å motta og lagre skattelister (opprette personregister som skal gjøre bruk av elektroniske hjelpemidler, jf personregisterloven § 9) for produksjon av skattebøker (Justisdepartementets ref 96/12128 A-AP ALS/kw). Vedtaket bygger på en forutsetning om at Økonomisk Rapports utgivelse av skattebøker ikke er «journalistisk virksomhet», jf personregisterforskriften § 2-14 som fritar «Dags- og ukepressens personregister til bruk i journalistisk virksomhet [...] fra konsesjonsplikten etter personregisterloven § 9 første ledd».

KAPITTEL18

Tilsynsmyndigheten**18.1 INNLEDNING – MANDATET OG OVERSIKT OVER KAPITLET**

I utvalgets mandat bokstav a heter det at utvalget skal vurdere hvilke oppgaver som bør ligge til Datatilsynet i fremtiden. Mandatet pålegger i tillegg utvalget å vurdere hvilken stilling Datatilsynet bør ha i forhold til regjeringen og Justisdepartementet, herunder regjeringen og departementets instruksjons- og kontrollmyndighet.

Når det gjelder spørsmålet om hvilke oppgaver Datatilsynet bør ha i fremtiden, er dette i stor grad allerede behandlet i "*Regulering og kontroll*" i kapittel 12 om reguleringsteknikker. Mange av reguleringsteknikkene, f.eks. konsesjons- og meldepikt, forutsetter et Datatilsyn, og gir således uttrykk for tilsynets fremtidige oppgaver. Under 18.2 vil utvalget komme med noen mer prinsipielle synspunkter på hvilke funksjoner tilsynet bør ha, og hvordan disse bør løses. Dessuten må det vurderes om tilsynet har fått slik kompetanse som direktivet krever at det skal ha.

Hoveddelen av "*Tilsynsmyndigheten*" i kapittel 18 dreier seg om hvordan tilsynsmyndigheten (Datatilsynet og Personvernemnda) bør organiseres og plasseres i forhold til forvaltningen for øvrig (18.3). Utvalget foreslår bl.a. at tilsynsmyndigheten får større uavhengighet av den utøvende makt enn tilfellet er i dag.

Til slutt i "*Tilsynsmyndigheten*" i kapittel 18 behandles domstolsprøving av tilsynsmyndighetens avgjørelser.

18.2 DATATILSYNETS OPPGAVER I FREMTIDEN**18.2.1 Oversikt**

Først presenteres noen prinsipielle synspunkter på tilsynets funksjoner i fremtiden (18.2.2). Deretter vurderes forholdet til direktivet (18.2.3).

18.2.2 Noen prinsipielle synspunkter

Datatilsynet bør videreutvikle sin kompetanse og sin kapasitet med tanke på å imøtekomme behov for et miljø som kan identifisere og formulere personverntrusler, og som kan være i stand til å anvisse hvorledes de kan unngås eller begrenses. Datatilsynet bør også ha som oppgave å kontrollere om lovbestemmelser og lovhjemlede vedtak faktisk etterleves.

For å nå disse målene vil tilsynet ha behov for informasjon om personopplysningsbrukerne; informasjon om hvem de er, hvor de er og hva de gjør. Innhenting av denne informasjonen kan skje på flere måter, som for eksempel gjennom meldinger, konsesjonsbehandling, kontrollvirksomhet og mer «ombuds»-preget virksomhet (for eksempel rådgiving).

En av Datatilsynets viktigste funksjoner vil være å bevisstgjøre folk om hvilken betydning deres aktivitet har for personvernet, og om hvilke tiltak som kan settes i verk for å sikre at hensynet til personvern varetas. Manglende kunnskap om personvern kan føre til at personvern ikke tas med i betraktningen, eller til at personvern tillegges mindre vekt enn ønskelig. Foran i utredningen har utvalget pekt på hvor viktig det er at personvern hensyn tas i betraktning ved utviklingen og anvendelsen av nye teknologiske løsninger (se "*Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet*" i kapittel 4). For at dette

skal være mulig må de teknologiske miljøene tilføres kunnskap om personvern. Datatilsynet har kompetanse som forener prinsipiell personverntenkning med teknologisk innsikt, og bør ha som oppgave å stimulere personvern fremmende teknologi i samarbeide med private og offentlige interessenter innen norske IT-miljøer og IT-forskning.

Også andre former for frivillig kontakt mellom Datatilsynet og personopplysningsbrukere er ønskelig. Datatilsynet bør for eksempel medvirke og stimulere til at personvern kan bli en «ombuds»-funksjon i bedrifter, etater, organisasjoner og interessegrupper. Datatilsynet bør dessuten bruke sin kompetanse til å bistå i utformingen av profesjonsetiske retningslinjer (se "*Bransjevise atferdsnormer*" i kapittel 12.5.9 om bransjevise atferdsnormer).

Mer generelt bør Datatilsynet settes i stand til å påta seg forholdsvis konkret rådgivning ved spørsmål om planlegging, gjennomføring og evaluering av virksomhet innenfor privat og offentlig sektor som har betydning for personvernet. Datatilsynet mottar i dag en rekke henvendelser om å delta i ulike prosjekt- og planleggingsgrupper, men kan av kapasitetshensyn bare imøtekomme et fåtall av henvendelsene (jf Årsmelding for Datatilsynet 1995 i St meld nr 15 1996-97 s 8 v sp).

Selv om utstrakt rådgivning kan føre til kunnskap om og respekt for personvernhensyn, er det grunn til å tro at ikke alle vil respektere personvernet i tilstrekkelig grad. Det er derfor nødvendig at Datatilsynet også har som oppgave å kontrollere at lovens bestemmelser faktisk blir fulgt i praksis. Kontrollen vil iht det nye lovforslaget i noen grad finne sted på forhånd gjennom vurdering av konsesjonsøknader, men fokus vil nå særlig bli satt på etterfølgende kontroll. Den etterfølgende kontrollen baserer seg dels på meldeplikten som gir informasjon til tilsynet om forhold det kan være grunn til å kontrollere, og dels på en kompetansebestemmelse som gir Datatilsynet mulighet til å gi pålegg der kontrollen avslører at loven ikke blir fulgt.

Utvalget ser det som sannsynlig at internasjonaliseringen av personvernsspørsmål og utviklingen av internasjonale forpliktende avtaler og institusjoner for varetakelse av personvernhensyn, vil prege arbeidet i Datatilsynet i fremtiden. Dette må få ressursmessige konsekvenser ikke bare for bemanningssituasjonen, men også når det gjelder medarbeidernes kvalifikasjoner.

Det er i denne sammenheng nødvendig å være oppmerksom på at det vil kunne oppstå situasjoner der en utvidelse av Datatilsynets ansvar knyttet til forvaltning av for eksempel internasjonale samarbeidsprosjekter vil kunne skape konflikt eller uklarheter. I særlige ugunstige tilfeller vil dette kunne berøre den tillit og integritet Datatilsynet også i fremtiden vil være avhengig av for å kunne løse sine forvaltningssoppgaver på en god måte.

18.2.3 Forholdet til direktivet artikkel 28

18.2.3.1 Innledning – problemstillingen

Etter artikkel 28 nr 1 skal hvert av medlemslandene utpeke minst én offentlig tilsynsmyndighet som skal påse at reglene som gis til gjennomførelse av direktivet, overholdes. I Norge er denne tilsynsmyndigheten Datatilsynet. Tilsynsmyndigheten(e) skal tillegges en rekke funksjoner, og det er forutsatt at de(n) skal utøve sine oppgaver «i full uavhengighet» (se nærmere om dette under 18.3). I artikkel 28 nr 2-7 gis utfyllende – men ikke uttømmende – oversikt over tilsynets kompetanse. I det følgende vurderes det om funksjonene som tillegges Datatilsynet i "*Regulering og kontroll*" i kapittel 12 er tilstrekkelig til å oppfylle direktivet.

18.2.3.2 Høringsarbeid

I henhold til artikkel 28 nr 2 skal Datatilsynet uttale seg bl a når det utarbeides lover og forskrifter av betydning for behandling av personopplysninger. Av personregisterloven § 3 nr 4 fremgår det at Datatilsynet etter henvendelse eller av eget tiltak skal gi uttalelse i generelle spørsmål som gjelder bruk av personopplysninger, men loven oppstiller ikke noen plikt til å høre Datatilsynet slik direktivet gjør. Rent faktisk er direktivet oppfylt, Datatilsynet bidrar allerede aktivt i forskjellig høringsarbeid og på et videre felt enn det direktivet krever. Deltagelse i høringsarbeid bør etter utvalgets syn fortsatt være en viktig oppgave for Datatilsynet. Det bør vurderes om det er hensiktsmessig å endre utredningsinstruksen slik at plikten til å høre Datatilsynet også fremgår av denne.

18.2.3.3 Tilgang til opplysninger m m

I henhold til artikkel 28 nr 3 første strekpunkt skal tilsynsmyndighetene ha kompetanse til å samle inn alle opplysninger som er nødvendige for å kunne utføre tilsynsoppgavene. Tilsynsmyndighetene skal også kunne iverksette undersøkelser og kreve tilgang til personopplysninger som behandles. Slik kompetanse har Datatilsynet i dag, jf personregisterloven § 5, som utvalget foreslår at videreføres i den nye loven (se lovforslaget § 38).

Særlige spørsmål oppstår der den som forklarer seg til Datatilsynet har brutt lovgivningen slik at det kan være aktuelt med strafforfølgning. Etter straffeprosessloven har den som er mistenkt for en forbrytelse rett til å nekte å bidra til sin egen domfellelse ved å forklare seg (jf straffeprosessloven § 90). Denne bestemmelsen gjelder imidlertid bare når strafforfølgning er iverksatt, Datatilsynets mistanker om straffbare forhold er ikke tilstrekkelig. I lys av praksis fra menneskerettighetsdomstolen kan det spørres om retten til å nekte å forklare seg bør utvides til også å gjelde granskingsstadiet i forvaltningssaker. Problemstillingen reiser vanskelige prinsipielle spørsmål av generell karakter som utvalget ikke har hatt anledning til å gå nærmere inn på (jf nærmere Morten Eriksens artikkel «Plikt til å uttale seg om egne og nærstående straffbare forhold i forvaltningssaker» i Juristkontakt nr 7 for 1996).

Artikkel 28 nr 3 andre strekpunkt inneholder en rekke beføyelser som skal tilkomme tilsynsmyndighetene. For det første skal de ha kompetanse til å gripe effektivt inn ved behandlinger som omtalt i artikkel 20 (behandlinger som medfører særlige risiki for personers rettigheter og friheter), for eksempel ved å uttale seg før behandlingene iverksettes. Dette kravet er oppfylt gjennom de foreslåtte reglene om konsesjonsbehandling, se 12.5.5 og lovforslaget § 33. I tillegg kreves det at tilsynsmyndighetene skal offentliggjøre uttalelsene på en passende måte. Hva som er «passende», sier ikke direktivet noe om. Utvalget mener for sin del at plikten til offentliggjøring er tilstrekkelig varetatt gjennom årsmeldingen, ulike informasjonstiltak for øvrig samt mulighet til innsyn i Datatilsynets dokumenter iht offentlighetsloven.

For det andre følger det av andre strekpunkt i artikkel 28 nr 3 at tilsynsmyndighetene skal ha kompetanse til å kreve at opplysninger blokkeres, slettes eller tilintetgjøres. Datatilsynet har i medhold av personregisterloven § 8 annet ledd kompetanse til å pålegge retting, sletting eller supplering av uriktige opplysninger, og utvalget foreslår at denne bestemmelsen videreføres og suppleres med en ny bestemmelse om sletting av personopplysninger, se nærmere 11.5 og lovforslaget §§ 25 og 26.

For det tredje følger det av andre strekpunkt i artikkel 28 nr 3 at tilsynsmyndighetene enten skal kunne

- forby en behandling av personopplysninger, eller

- utstede en advarsel til den behandlingsansvarlige, eller
- påtale en overtredelse overfor den behandlingsansvarlige, eller
- høre nasjonalforsamlingen eller andre nasjonale politiske institusjoner.

Det siste strekpunktet er oppfylt ved at Datatilsynet gjennom sin årsmelding (se nedenfor) «hører» Stortinget slik direktivet legger opp til. For øvrig gir utvalgets lovforslag § 40 Datatilsynet kompetanse til å gi pålegg om at behandling av personopplysninger i strid med loven skal opphøre eller stille vilkår som må oppfylles for at behandlingen skal være i samsvar med loven, se merknadene til lovforslaget § 40.

I artikkel 28 nr 3 tredje strekpunkt heter det at tilsynsmyndighetene skal kunne bringe overtredelser inn for domstolene, eller gjøre domstolene oppmerksomme på overtredelsene. Det siste alternativet passer best i land med en inkvisisjonsbasert straffeprosess, dvs land der domstolen selv tar initiativ til å forfølge straffbare forhold. Slik norsk straffeprosess er bygget opp, ville det ha liten mening å gjøre domstolene oppmerksomme på et straffbart forhold uten ytterligere oppfølging. Direktivet er på dette punkt tilstrekkelig gjennomført i norsk rett ved at Datatilsynet kan anmelde overtredelser av personregisterloven til politiet og påtalemyndighetene for strafferettslig forfølging ved domstolene. Direktivet kan ikke forstås slik at tilsynsmyndighetene selv skal ha påtalekompetanse.

18.2.3.4 Anmodning om kontroll

I henhold til artikkel 28 nr 4 første ledd skal enhver kunne henvende seg til tilsynsmyndighetene og be om beskyttelse av rettigheter og friheter i forbindelse med behandling av personopplysninger. Bestemmelsen omfatter for eksempel tilfeller der den registrerte ønsker å få kontrollert om loven er blitt eller vil bli fulgt. Direktivet pålegger ikke tilsynsmyndighetene å prioritere enhver slik henvendelse, men har plikt til å underrette datasubjektet om hvordan saken er fulgt opp. Bestemmelsen må anses å være gjennomført gjennom Datatilsynets praksis. Tilsynet mottar og behandler mange henvendelser fra enkeltpersoner, jf Årsmelding for Datatilsynet 1995 s 9 h sp:

«Mange av henvendelsene til Datatilsynet tar også opp saker som ikke er direkte knyttet til søknader om oppretting av registre eller å drive konsesjonspliktig virksomhet. Henvendelsene omfatter andre deler av personregisterloven og tar gjerne opp temaer som er aktuelle i samfunnsdebatten eller som knytter seg direkte til enkeltpersoners hverdagsliv. Dette gjelder spørsmål om overvåking, utlegging av skattelister, adressert reklame i posten, innsyn i registre, sletting av opplysninger, bruk av fødselsnummer med mer. Datatilsynet mottok for eksempel 102 skriftlige henvendelser om innsyn i ulike registre i 1995.»

Artikkel 28 nr 4 annet ledd bestemmer at enhver skal ha rett til å anmode om at tilsynsmyndighetene kontrollerer lovligheten av en behandling på områder hvor det i medhold av artikkel 13 er gjort innhogg i individuelle rettigheter. Direktivet må forstås slik at Datatilsynet har plikt til å følge opp denne type saker. Dette kan utledes av siste punktum i annet ledd, hvor det heter at den som har kommet med anmodningen skal underrettes om at det er foretatt en kontroll. Hvor grundig kontrollen skal være, må avgjøres av tilsynsmyndigheten. En slik plikt til å følge opp henvendelser fra borgerne følger av alminnelige forvaltningsrettslige prinsipper, og utvalget ser ikke behov for å lovfeste denne plikten.

18.2.3.5 Årsmelding

I artikkel 28 nr 5 heter det at hver tilsynsmyndighet med regelmessige mellomrom skal utarbeide og offentliggjøre en rapport om sin virksomhet. Dette har Datatilsynet gjort allerede fra starten av i form av sin årsmelding. Årsmeldingen oversendes til regjeringen, som utarbeider en Stortingsmelding om Datatilsynets virksomhet. Stortingsmeldingen inneholder regjeringens merknader til Datatilsynets årsmelding, og Datatilsynets årsmelding følger som trykt vedlegg. Årsmeldingen gir en fylldig oversikt over Datatilsynets virksomhet og over prinsipielt viktige eller nye saksområder.

Utvalget går inn for at det også i fremtiden bør utarbeides en årsmelding. Årsmeldingen vil som i dag ha flere viktige funksjoner – blant annet vil den gi informasjon om tilsynsvirksomhet og prinsipielle personvernspørsmål, og dermed stimulere til og gi grunnlag for debatt.

18.2.3.6 Datatilsynets stedlige kompetanse

Artikkel 28 nr 6 første ledd fastslår at norske tilsynsmyndigheter skal kunne utøve kompetansen som beskrevet i nr 3 (se 18.2.3.3) på norsk territorium og Svalbard uansett hvilken nasjonal lov som regulerer den aktuelle behandlingen av personopplysninger. Datatilsynet kan for eksempel pålegge et utenlandsk selskap som vil publisere personopplysninger i Norge å rette, slette eller supplere uriktige opplysninger i den grad dette er hjemlet i utenlandsk lovgivning (som regulerer virksomheten til det utenlandske selskapet).

Av annet ledd fremgår det at tilsynsmyndighetene skal samarbeide (f eks ved utveksling av opplysninger) i den grad det er nødvendig for å oppfylle tilsynsmyndighetenes plikter. Det er noe uklart om det siktes til samarbeid over landegrensene eller mellom flere tilsynsmyndigheter i ett land. Tolkningsspørsmålet kommer imidlertid ikke på spissen. I Norge vil all myndighetsutøvelse med unntak av regelgivning og klagebehandling foretas av Datatilsynet. Kravet til «samarbeid» mellom Datatilsynet og klageinstansen i forbindelse med klagebehandling reguleres av forvaltningsloven kapittel VI og alminnelige forvaltningsrettslige regler, og utvalget ser ikke behov for ytterligere regulering. Når det gjelder samarbeid med andre lands tilsynsmyndigheter, er det påkrevet med en lovhjemmel som gjør unntak fra lovbestemt taushetsplikt. Det vil være behov for et slikt samarbeid med andre lands tilsynsmyndigheter fordi tilsynsmyndighetenes kompetanse er begrenset til eget territorium.

18.2.3.7 Taushetsplikt

I artikkel 28 nr 7 heter det at tilsynsmyndighetens medlemmer og ansatte skal ha taushetsplikt om de fortrolige opplysningene de har tilgang til. Personregisterloven inneholder ikke egne regler om taushetsplikt, men ettersom både Datatilsynet (og Personvernemnda som foreslås opprettet) er forvaltningsorganer, gjelder taushetspliktbestemmelsen i forvaltningsloven § 13. Taushetsplikten etter forvaltningsloven § 13 vil imidlertid ikke alltid være tilstrekkelig omfattende, og det er av avgjørende betydning at den behandlingsansvarlige og databehandleren har tillit til at opplysninger om sikkerhstiltak m v ikke kommer på avveie. Utvalget foreslår derfor en bestemmelse om taushetsplikt for Datatilsynets ansatte for slike opplysninger, se lovforslaget § 11 tredje ledd.

18.3 ADMINISTRASJON AV LOVEN – ORGANISERING AV TILSYNSMYNDIGHETEN

18.3.1 Oversikt

I 18.3 drøftes hvorledes tilsynsmyndigheten bør organiseres, herunder hvorledes beslutningsprosessen skal være.

Først gis det en oversikt over dagens ordning (18.3.2) og forholdet til EF-direktivet (18.3.3). Deretter redegjøres det for overordnede målsettinger for organisering av denne form for statlig virksomhet (18.3.4). I 18.3.5 behandles den administrative forankringen av Datatilsynet. Utvalget kommer til at dagens ordning på dette punkt i hovedsak bør videreføres, slik at Datatilsynet fortsatt administrativt bør høre under Justisdepartementet. Utvalget vurderer deretter om og eventuelt i hvilken grad Justisdepartementet skal kunne instruere Datatilsynet (18.3.6). Utvalgets konklusjoner er bl a at departementet ikke bør kunne instruere tilsynet om utfallet i enkeltsaker, og ei heller generelt om hvordan loven skal forstås eller forvaltningsskjønnet skal utøves. Datatilsynets ledelse og organisering drøftes under 18.3.7 (herunder spørsmål om Datatilsynet fortsatt skal ledes av et styre). Til slutt vurderes det hvem som skal behandle klager over tilsynets avgjørelser (18.3.8). Utvalget foreslår at Justisdepartementet ikke lenger skal behandle klager, men at klager istedet skal behandles av en uavhengig klageinstans (Personvernemnda). Opprettelsen av Personvernemnda reiser en rekke ulike spørsmål (18.3.9). Stortingets kontroll kommenteres avslutningsvis under 18.3.10.

18.3.2 Hovedtrekkene i dagens ordning

I henhold til personregisterloven § 2 er Datatilsynet et «frittstående organ underordnet Kongen og det departement Kongen fastsetter». I kongelig resolusjon 8 november 1979 er det bestemt at Datatilsynet er underlagt Justisdepartementet. Uttrykket «frittstående» markerer bl a at Datatilsynet ikke er en del av departementet. Organiseringen av tilsynet bygger i liten grad på instruks fra departementet. Dette har gjort det mulig å møte nye utfordringer innenfor en organisatorisk ramme som er fleksibel og som raskt kan endres.

Datatilsynet ledes av et styre med syv medlemmer, jf personregisterloven § 2 annet ledd. Styret behandler i første rekke saker som aktualiserer nye eller endrede problemstillinger for personvernet og saker som berører sentrale samfunnsmessige spørsmål. Alle klagesaker behandles av styret. Styret fatter vedtak i de sakene som legges frem av administrasjonen. I forarbeidene til personregisterloven er det fremhevet at det ved sammensetningen av styret først og fremst skal legges vekt på den enkelte kandidatens personlige egnethet (i motsetning til direkte interessegrupprepresentasjon, jf Ot prp nr 2 (1977-78) s 49). I praksis har det blitt vanlig å oppnevne representanter fra NHO og LO i styret. Styret blir oppnevnt for fire-årsperioder og det er adgang til gjenoppnevning.

I 1996 hadde styret syv møter og behandlet 20 saker. I tillegg ble 25 saker lagt frem til orientering. Femten av sakene ble behandlet som klagesaker og 14 av disse ble sendt over til Justisdepartementet som klageinstans mens én ble omgjort av styret.

18.3.3 EF-direktivet

I direktivet artikkel 28 nr 1 heter det at tilsynsmyndigheten skal kunne utøve sine funksjoner i «full uavhengighet». I dette avsnittet drøftes direktivets krav til uavhengighet mer generelt. Den nærmere rekkevidden av direktivets uavhen-

gighetskrav vurderes konkret i tilknytning til spørsmålene om administrativ forankring, instruksjonsmyndighet og klagebehandling.

Utvalget vil først understreke at «uavhengighet» er et relativt begrep. Fullstendig uavhengighet fra alle andre samfunnsinstitusjoner er ikke mulig – dette følger allerede av at det må bevilges penger til driften av tilsynsvirksomheten. Spørsmålet blir derfor *hvor uavhengig* direktivet krevet at Tilsynsmyndigheten må være. Flere forhold har betydning for graden av uavhengighet, se nærmere 18.3.6 og 18.3.8 om bl a instruksjonsmyndighet og behandling av klagesaker.

Ettersom direktivet legger opp til at tilsynsmyndigheten skal være et forvaltningsorgan, er det videre naturlig å tolke direktivet slik at kravet til uavhengighet relaterer seg til *den utøvende statsmakt*, dvs regjeringen/departementet.

Når direktivets krav til uavhengighet skal presiseres videre, er det naturlig å feste seg ved at det er under *utøvelsen av sine tilsynsoppgaver* at tilsynsmyndigheten skal være uavhengig av regjeringen/departementene, se nærmere om dette nedenfor. Uavhengigheten skal være faglig (funksjonell). Noen skarp grense mot administrativ uavhengighet er det imidlertid ikke.

18.3.4 Overordnede målsettinger for organisering av denne formen for statlig virksomhet

I NOU 1989: 5 «En bedre organisert stat» (Hermansen-utvalget) drøftes hvorledes ulike former for statlig virksomhet bør organiseres. Følgende generelle hensyn og krav fremheves (jf s 149 – 150):

- Politisk styrbarhet
 - faglig og innholdsmessig
 - samordningsmessig
- Faglig kvalitet og verdiforankret selvstendighet
- Effektivitet
 - kostnadseffektivitet
 - formålseffektivitet
- Rettsstatsverdier
 - rettsikkerhet og likebehandling
 - offentlighet
- Interesserepresentasjon og de ansattes medbestemmelse
- Fornyelses- og omstillingsevne.

Med *politisk styrbarhet* menes at statsmakten for å kunne påvirke samfunnsutviklingen må kunne styre sine utførende virksomheter. Styring kan skje på flere måter, for eksempel gjennom regelverk og gjennom instruksjer. Om graden av selvstendighet heter det at (jf s 64 h sp):

«Institusjoner der den rent faglige virksomheten har stor betydning, vil ofte reelt sett kunne ha en stor grad av selvstendighet i den konkrete utforming av sin virkemåte. Styringsrelasjonene må derfor utformes konkret og tilpasses arten av virksomheten og fullmaktsforholdene. Dette er like mye et organisasjons- og administrasjonsfaglig som et forvaltningsrettslig spørsmål. Avveiningen mellom politisk styrbarhet og faglig selvstendighet må avgjøres konkret. Kravet til politisk styrbarhet vil derfor måtte oppfylles på noe ulike måter alt etter hva slags statlig engasjement virksomheten kanaliserer og hva formålet med engasjementet er.»

Utvalget har lagt stor vekt på en konkret tilpassing av politisk styrbarhet innenfor de rettslige og faktiske rammene utvalget er bundet av. Et særlig trekk ved organiseringen av Datatilsynet er at politisk styring slik utvalget ser det i stor grad bør skje gjennom lov- og forskriftsvedtak, og ikke gjennom instruks (dette utdypes nedenfor).

Faglig kvalitet og verdiforankret selvstendighet er spesielt viktig for et frittstående tilsynsorgan som Datatilsynet. Utøvelsen av virksomheten krever mye informasjon, nærhet til saksfeltet og høy faglig juridisk og teknologisk kompetanse. Dette er utdypet i 18.2.2 ovenfor.

Effektivitet kan presiseres nærmere til henholdsvis kostnadseffektivitet og formålseffektivitet. Med kostnadseffektivitet forstås forholdet mellom tilførte ressurser og den ytelsen organet frembringer. Datatilsynet har helt fra starten av hatt stor kostnadseffektivitet og ytet en imponerende innsats til tross for beskjedne ressurser. Den andre måten å måle effektivitet på er formålseffektivitet, dvs hvor godt forvaltningsorganet når de mål som er satt for virksomheten. En står her overfor vurderinger som er særdeles komplekse og vanskelige. Det er mulig at enda større formålseffektivitet kunne vært oppnådd dersom regelverket hadde vært utformet slik at Datatilsynet i mindre grad hadde måttet behandle trivielle konsesjonsøknader. Dette har utvalget foreslått endret ved å innsnevre området for konsesjonsplikt, se "*Konsesjonsplikt*" i kapittel 12.5.5. For øvrig kan ikke utvalget se at hensynet til formålseffektivitet tilsier en annen organisering av Datatilsynet enn i dag.

Hensynet til *interesserepresentasjon* har tradisjonelt ikke stått særlig sterkt når forvaltningsorganer skal organiseres. Datatilsynets styre er riktignok bredt sammensatt med blant annet representanter fra LO og NHO, men oppnevningen har hele tiden i tråd med lovgivers ønske vært basert på faglig og personlig egnethet og ikke på noe ønske om interesserepresentasjon. Utvalget har ikke sett det som ønskelig å vektlegge hensynet til interesserepresentasjon sterkere enn i dag.

I NOU 1989: 5 heter det om *rettsstatshensyn* bl a at (s 71 flg):

«I det norske samfunnet og i den norske forvaltningen har rettsstatsverdier og hensynet til rettssikkerhet en sentral plass. Den enkelte skal være beskyttet mot overgrep og vilkårlighet fra forvaltningen, og skal ha mulighet både til å skaffe seg oversikt over og innsikt i sin rettsstilling i forhold til myndighetene, og til å forsvare sine rettslige interesser. Rettsstillingen skal kunne forutberegnes, avgjørelser truffet av forvaltningsorganene skal kunne påklages til overordnet ledd med mindre klageadgangen er avskåret, og enhver har krav på å bli likebehandlet med andre som fremmer tilsvarende saker.»

Rettsstatshensyn vil som i dag varetas av bl a forvaltningsloven, offentlighetsloven og ulovfestet forvaltningsrett. Datatilsynet er et forvaltningsorgan, og saksbehandlingsreglene i forvaltningsloven – herunder regler om saksopplysning, varsel, innsyn, begrunnelse og klagebehandling – får anvendelse på vanlig måte. Dersom det begås formelle feil, og disse kan ha påvirket vedtakets innhold, kan vedtaket settes tilside som ugyldig, jf prinsippet i forvaltningsloven § 41.

Utvalget har vurdert om det er behov for å supplere de generelle reglene i forvaltningsloven med spesielle regler for Datatilsynets virksomhet. Generelt sett foreligger det ikke erfaringer som tilsier at det er behov for slike spesielle regler. Utvalget har lagt vekt på å videreføre norske rettssikkerhetstradisjoner, bl a ved å opprettholde den administrative klageadgangen til tross for at direktivet ikke krever dette. Rettssikkerhetshensyn danner også bakgrunnen for utvalgets forslag om en faglig uavhengig og bredt sammensatt klageinstans.

Lovforslaget vil for øvrig vareta rettsstatshensyn bedre enn i dag ved at loven selv i større grad gir uttrykk for hvordan personopplysninger skal eller bør behandles (se "*Individuelle personverngarantier*" i kapittel 11, "*Materielle regler*" i avsnitt 12.5.7 og "*Merknader til de enkelte bestemmelsene*" i kapittel 21). Når slike regler kan leses rett ut av loven, blir det lettere for den enkelte å vite hva han eller hun har å forholde seg til.

18.3.5 Datatilsynets administrative forankring

18.3.5.1 Dagens ordning

Det følger av underordningsforholdet til regjeringen/departementet at det i utgangspunktet tilligger departementet å fastsette nødvendige organisatoriske bestemmelser (jf Ot prp nr 2 (1977-78) s 70 h sp). Det samme gjelder ansettelsesmyndigheten, jf tjenestemannsloven § 5 nr 1. Regjeringen bestemmer videre innholdet i budsjettforslaget som fremmes for Stortinget.

18.3.5.2 Utvalgets vurderinger

Ettersom Datatilsynet også i fremtiden bør ha kompetanse til å treffe rettslig bindende avgjørelser (for eksempel konsesjonsvedtak og pålegg om sletting), taler mye for at det ikke ville være forenlig med konstitusjonelle regler å la tilsynet være direkte underlagt Stortinget (slik som f eks Sivilombudsmannen er). Dette ble lagt til grunn i Føyen-utredningen s 55 (vedlegg 6 til St meld nr 14 (1983-84), av departementet i den etterfølgende behandlingen av lovforslaget (jf Ot prp nr 34 (1986-87) s 10 og av Eivind Smith i utredning på oppdrag fra utvalget. Utvalget legger derfor til grunn at tilsynet fremdeles skal være administrativt underlagt regjeringen og et departement. Selv om administrative spørsmål kan være av betydning for hvordan tilsynsmyndigheten utfører sine oppgaver, er en slik løsning ikke i strid med direktivets krav til uavhengighet (se ovenfor hvor det legges til grunn at uavhengigheten gjelder faglige spørsmål).

I forbindelse med behandlingen av Føyen-utredningen ble det vurdert om tilsynet burde underordnes et annet departement enn Justisdepartementet. Alternativene var Statsministerens kontor og det daværende Forbruker- og administrasjonsdepartementet. Regjeringen la avgjørende vekt på bl a Justisdepartementets generelle ansvar for rettssikkerhets- og personvernspørsmål. Innordning under Statsministerens kontor ville kreve en styrking av kontoret for å administrere et spesielt felt, hvilket ikke var ønskelig (Ot prp nr 34 (1986-87) s 10 – 11). Justiskomiteen var enig i regjeringens vurderinger (jf Innst O nr 64 for 1986-87 s 2 – 3), og utvalget ser ikke grunn til å foreslå at Datatilsynet underordnes et annet departement enn Justisdepartementet.

18.3.6 Regjeringens/departementets instruksjonsmyndighet

18.3.6.1 Dagens ordning

Med instruksjonsmyndighet menes kompetanse til å bestemme hvordan Datatilsynet skal forholde seg til for eksempel lovtolkning og skjønnsutøvelse.

Uttrykket «frittstående» i personregisterloven § 2 tolkes gjerne slik at Datatilsynet er unntatt fra den alminnelige instruksjonsmyndighet som tilligger Justisdepartementet i egenskap av overordnet organ. Dette innebærer for det første at Justisdepartementet er avskåret fra å instruere Datatilsynet om utfallet i enkeltsaker. Det samme gjelder trolig generelle instruksjoner om lovtolkning og om hvordan for-

valtningsskjønnet (f.eks. interesseavveiningen i konsesjonsspørsmål) skal utøves (se nærmere om disse spørsmålene Selmer i «Samfunn – rett – rettferdighet, Festskrift til Torstein Eckhoff» TANO 1986). Departementets instruksjonsmyndighet innskrenker seg i så fall til rent organisatoriske- og arbeidsmessige forhold.

18.3.6.2 Utvalgets vurderinger

Spørsmålet om og eventuelt i hvilken grad regjeringen/departementet bør kunne instruere Datatilsynet er særskilt fremhevet i utvalgets mandat (se 18.1). Utvalget ser det som hensiktsmessig å avklare i loven hva departementet skal kunne instruere Datatilsynet om. I denne vurderingen står kravet til uavhengige tilsynsmyndigheter sentralt.

For en nærmere vurdering må det presiseres hva slags instruks det er snakk om. Instruksjonsmyndighet kan omfatte

- å bestemme utfallet (herunder skjønnsutøvelsen) i en bestemt sak (som er til behandling hos tilsynet)
- generelle instruksjoner om lovtolkning
- generelle instruksjoner om skjønnsutøvelse
- generelle instruksjoner om saksbehandling (rutiner)
- instruks om prioritering av saker/saksområder
- instruks om organisatoriske forhold.

Å gi departementet kompetanse til å instruere Datatilsynet om *utfallet i enkeltsaker* vil ikke være forenlig med direktivets krav til (faglig) uavhengighet (se ovenfor). Det samme gjelder generelle instruksjoner om *lovtolkning* og *skjønnsutøvelse*. Departementets mulighet til å direkte påvirke innholdet i Datatilsynets faglige avgjørelser vil derfor begrense seg til å gi materielle forskrifter til loven.

Når det derimot gjelder adgangen til å instruere om organisatoriske- og arbeidsmessige forhold, taler sammenhengen med budsjettansvaret for at departementet beholder sin instruksjonsmyndighet på dette punktet. Departementet skal i forbindelse med budsjettbehandlingen sette mål og veilede i tråd med gjeldende lover og regler og retningslinjer for oppfølging av underliggende virksomheter. Målene vil gjerne være av nokså generell karakter, mens den mer detaljpregete og fortløpende planleggingen og prioriteringen forestås av tilsynet selv. Departementets etatsstyring må ta hensyn til at tilsynsmyndigheten skal være faglig uavhengig.

18.3.7 Ledelse og organisering av Datatilsynet

18.3.7.1 Datatilsynets styre

Som nevnt i 18.3.2 ledes Datatilsynet i dag av et styre, jf personregisterloven § 2 annet ledd. I spørsmålet om Datatilsynet fortsatt bør ledes av et styre har utvalget delt seg i to.

Utvalgets leder og medlemmene Apenes, Kristiansen, Meinich og Schartum går inn for at når det opprettes en bredt sammensatt og faglig kompetent klageinstans (se 18.3.8 og 18.3.9), vil det ikke være behov for å videreføre dagens styreordning.

Medlemmene Bredengen, Gundersen, Hestnes, Håøy og Koch går inn for at dagens ordning med et bredt sammensatt og faglig kompetent styre bør videreføres fordi opprettelse av nytt klageorgan etter disse medlemmenes mening ikke har betydning for spørsmålet om hvorledes Datatilsynet bør organiseres.

Utvalget har lagt vekt på å gjøre omfattende rede for begge gruppens synspunkter for på den måten å legge til rette for senere overveielser hos høringsinstansene, i departementet og i Stortinget.

Utvalgets leder og medlemmene Apenes, Kristiansen, Meinich og Schartum mener at dagens ordning med et eget styre for Datatilsynet bør avvikles, når det opprettes en egen klageinstans (se 18.3.8 og 18.3.9).

Disse medlemmene mener en ordning med et faglig kompetent styre vil innebære en tre instans behandling av klagesaker. *Disse medlemmene* finner ingen grunn til å fravike en normal ordning med behandling i to instanser. Samtidig erkjenner *disse medlemmene* at det i vanskelige og prinsipielle enkeltsaker kan være behov for en grundigere saksbehandling enn i mer kurante saker. Slike behov kan imidlertid på tilstrekkelig måte dekkes gjennom interne tiltak i Datatilsynet. Dessuten kommer Datatilsynet til i enda større grad enn i dag å ha en bred kontaktflate utad og på den måten tilføres faglig kompetanse. I tillegg ligger det i kortene at samarbeidet med tilsynsmyndighetene i andre land, særlig med EU-land, vil øke betraktelig i tiden som kommer, med den erfaringsutveksling som dette innebærer. Det må også tas i betraktning at det gjerne er prinsipielle og tvilsomme saker som påklages, og i så fall vil klageinstansen (som forutsetningsvis er enda mer kompetent enn styret ville vært) behandle saken. Klageinstansen kan også gripe inn og omgjøre avgjørelser av eget tiltak dersom vilkårene i forvaltningsloven § 35 er oppfylt.

Disse medlemmene erkjenner at Datatilsynets styret gjennom sin aktive rolle i enkeltsaksbehandlingen i tiden siden personregisterloven trådte i kraft, har etablert seg som en instans med stor faglig autoritet. *Disse medlemmene* mener imidlertid at det er av vesentlig betydning at en lykkes med å etablere en ny og uavhengig klageinstans med tilstrekkelig kompetanse og autoritet (se 18.3.8 og 18.3.9). Dersom styreordningen opprettholdes, vil en lett kunne få to reelt konkurrerende klageinstanser. Dette vil vanskeliggjøre en tilfredsstillende etablering av en øverste klageinstans.

Disse medlemmene mener at det ikke er behov for et styre for Datatilsynet som behandler administrative saker. *Disse medlemmene* viser til at styrebehandling er gjennomført i bare en tredjedel av direktoratlignende organer, og er etter det *disse medlemmene* kjenner til helt ukjent i ombudsmannsmodellen (som det på mange måter er nærliggende å sammenlikne Datatilsynet med). Det er også av betydning at etatens størrelsesmessig er beskjedne med sine drøyt tyve medarbeidere – og at etaten neppe vil vokse vesentlig i årene fremover. Et «virksomhetsstyre» på 7 medlemmer utgjør ca 1/3 av det totale antall ansatte i Datatilsynet. *Disse medlemmene* mener at dette ikke vil representere en forsvarlig ressursbruk. En fortsatt styreordning i tillegg til klageinstansen vil dessuten medføre at saksbehandlingen blir unødvendig omstendelig. Disse forholdene tilsier at styrets administrative bistand ikke er så viktig at den er noe tungt argument for å opprettholde styret. Samtidig understreker *disse medlemmene* betydningen av at Datatilsynet disponerer tilstrekkelig administrative ressurser.

Medlemmene Bredengen, Gundersen, Hestnes, Håøy og Koch mener Datatilsynet fortsatt skal ledes av et styre. En viktig begrunnelse for dette er Datatilsynets uavhengighet, som innebærer at tilsynet ikke er underlagt direkte politisk styring fra Regjeringen. Det er lite hensiktsmessig å ha styre i etater og direktorater som kan instrueres direkte fra Regjeringen og departementene. For mer uavhengige forvaltningsorganer kan imidlertid et balansert sammensatt styre være en hensiktsmessig arena for avveining av ulike interesser og hensyn forut for at avgjørelser treffes. Styret kan gi det uavhengige Datatilsynet større legitimitet i samfunnet. Det forutsettes at styrets sammensetning ikke rokker ved tilsynets faglige uavhengighet. Kandidater til styre må velges ut fra egnethet, samfunnsmessig innsikt og evne til å være med på å ta i bruk og utvikle de nye virkemidler Datatilsynet får gjennom den nye

loven. Da et styre varetar bestemte roller i en virksomhet, er virksomhetens størrelse ikke avgjørende for om det er behov for styre eller ei, ei heller for styrets størrelse.

Disse medlemmene mener at den politiske styringen fra overordnet departement vil begrenses til fastsettelse av forskrifter og til signaler som gis i forbindelse med de årlige budsjettproposisjoner og tildelingsbrev, samt Stortingsbehandlingen av Datatilsynets årsmelding. Styret vil derfor ha den løpende etatstyringen og styringsdialogen med Datatilsynets administrasjon: vedta og følge opp strategi- og virksomhetsplaner, årsmelding og evaluering av tilsynets virksomhet og følge opp tilsynets budsjett og regnskap.

Disse medlemmene mener at styret skal behandle saker som aktualiserer nye eller endrede problemstillinger for personvernet og saker som berører sentrale samfunnsmessige spørsmål, herunder drøfte spørsmål knyttet til internasjonalt samarbeide på personvernområdet. Med det nye settet av virkemidler Datatilsynet får, må styret spille en aktiv rolle i prioritering, utforming og bruk av disse virkemidlene gjennom å utforme strategier og planer for Datatilsynets virksomhet. Den nye loven innebærer mindre vekt på konsesjoner og større vekt på virkemidler som etterfølgende kontroll, tilsyn, rådgivning og veiledning. Et aktivt styre kan, etter *disse medlemmenes* syn, sammen med Datatilsynets administrasjon bidra til å utvikle formålseffektive strategier for å vareta personvern hensynet i informasjonssamfunnet.

Disse medlemmene mener at styret vil tilføre Datatilsynet både faglig og administrativ kompetanse, som må sees i sammenheng og i forhold til tilsynets oppgaver slik de fremkommer i loven. Med sin brede sammensetning og høye faglige kompetanse har styret hittil bidratt vesentlig til opparbeidelsen av den sterke posisjon Datatilsynet har i dag og representerer i seg selv en verdifull ressurs for tilsynet. Med den endring i virkemiddelbruk, de videre fullmakter Datatilsynet får gjennom den nye loven og med et mer uavhengig Datatilsyn, mener *disse medlemmene* at et bredt sammensatt kollegialt organ vil gi tilsynet økt legitimitet, bedre samfunnsmessig forankring og bidra til aksept av de nye reguleringsmåtene.

Disse medlemmene mener at Datatilsynet trolig fortsatt vil ha en ressursituasjon som vil kreve jevnlig vurdering og prioritering av virkemiddelbruken, en prioritering som styret må medvirke aktivt til. Departementet er avskåret fra å delta i denne dialogen fordi Datatilsynet er faglig uavhengig. Tilsvarende vil klageinstituttet være en form for reaktiv tilbakemelding, mens et styre med sin rolle kan bidra til et mer proaktivt Datatilsyn som tidlig fanger opp signaler og eventuelt justerer strategi og virkemiddelbruk. Styret bør behandle og treffe avgjørelser i saker av prinsipiell karakter, fastsette forskrifter (dersom departementet delegerer slik kompetanse) og ta opp klagesaker før eventuell oversendelse til Personvernemnda. Klagesaker vil, selv om styret ikke er å betrakte som en egen behandlingsinstans, gi viktige signaler om forhold som kan tilsi revurdering av strategi og virkemiddelbruk. Styret har som administrasjonen, anledning til å omgjøre påklagede vedtak. Dersom styret fjernes, vil en også fjerne dagens ordning med at prinsipielle saker undergis bred behandling i styret og gå over til en ordning hvor bare klagesakene vil få en slik behandling og da i klageinstansen. *Disse medlemmene* ser en slik omlegging som uheldig.

Disse medlemmene mener at sammensetningen av styre bør baseres på samme kriterier som i dag. Kongen, etter innstilling fra Justisdepartementet, bør som i dag oppnevne styret og bestemme hvem som skal være leder og nestleder. Det bør utarbeides generelle retningslinjer for styret i Datatilsynet som klargjør styrets mandat, fullmakter, ansvar og roller. Det faller utenfor utvalgets mandat å utdype dette i detalj.

Disse medlemmene understreker at styret vil ha en helt annen rolle, vareta helt andre oppgaver og ha en helt annen nærhet og løpende oppfølging av Datatilsynets virksomhet enn det Personvernemnda vil og bør ha (se 18.3.9).

18.3.7.2 Datatilsynets direktør

Datatilsynets direktør bør fremdeles være uavsettelig embetsmann. Det stillingsværet og den uavhengighet dette gir, gjør det lettere å føre kritisk tilsyn med offentlig virksomhet. I en del andre ledende stillinger i offentlig forvaltning er det vanlig å ansette for en bestemt periode (åremål). Bruk av åremålsstilling er et virkemiddel som gjør det mulig å oppnå en best mulig balanse mellom hensynet til kontinuitet og behovet for fornyelse. Utvalget har kommet til at regjeringen bør ha anledning, men ikke plikt til å ansette Datatilsynets direktør på åremål.

Datatilsynets direktør er i dag utnevnt av Kongen i statsråd. Utvalget går inn for å videreføre denne ordningen. At regjeringen utnevner direktøren er naturlig fordi Datatilsynet driver utøvende myndighet, og i samsvar med utnevningen av lederne i andre direktorater og ombud (med unntak av Stortingets ombudsmann for forvaltningen). Det kunne komme i konflikt med Stortingets kontrollerende rolle dersom Stortinget skulle utnevne direktøren. Fordelen med å la Stortinget utnevne direktøren ville bli at utnevningprosessen trolig ville vekke bred debatt om hvem som burde ansettes i stillingen. Utvalget har imidlertid ikke ansett dette som tungtveiende nok til å kunne begrunne en endring av dagens ordning.

18.3.8 Klager over Datatilsynets avgjørelser

18.3.8.1 Dagens ordning

I dag behandles klager over Datatilsynets enkeltvedtak av Justisdepartementet. I saker som angår Justisdepartementet (f.eks. når Justisdepartementet er registereier) avgjøres klagesaken av Kongen i statsråd etter at Administrasjonsdepartementet (nå Planleggings- og samordningsdepartementet) har forberedt klagesaken. Nedenfor presenteres noen hovedtrekk i dagens ordning. Lee Bygrave gir i sin bok «Personvern i praksis» (Cappelen Akademisk Forlag, Oslo 1997) en gjennomgåelse av Justisdepartementets behandling av klager på Datatilsynets avgjørelser i perioden 1980 – 1996, og utvalget viser til denne fremstillingen for en mer inngående gjennomgåelse av dagens praksis.

Avgjørelsene som Datatilsynet treffer kan påklages dersom avgjørelsen er et enkeltvedtak og den som ønsker å klage enten er part i saken eller har rettslig klageinteresse (forvaltningsloven § 28). Datatilsynets og departementets praksis viser at ideelle organisasjoner har blitt ansett som klageberettigete, mens klager fra enkeltpersoner som er eller kan tenkes å bli registrert i et register som utgangspunkt ikke kan påklage vedtak om samtykke til å opprette registeret. Som regel kommer klagen fra den som ikke har fått konsesjon til å opprette et register, eller der det er satt konsesjonsvilkår som klageren synes er for strenge.

Fristen for klage er tre uker fra klageren er underrettet om Datatilsynets vedtak (jf forvaltningsloven § 29). Praksis viser at Datatilsynet og Justisdepartementet ofte har behandlet klager selv om de har kommet inn for sent og kunne vært avvist (jf oppreisningsregelen i forvaltningsloven § 31). Dersom det klages over Datatilsynets vedtak, vil Datatilsynets administrasjon oversende saken til styret, som etter samråd med administrasjonen vurderer om førsteinstansvedtaket bør omgjøres, eller om vedtaket bør opprettholdes slik at klagesaken oversendes klageinstansen (Justisdepartementet).

Justisdepartementet har full kompetanse i klagesaken. Det betyr at departementet kan overprøve alle tilsynets vurderinger, og selv avgjøre om f eks konsesjon skal gis. Som regel tar klagebehandlingen i departementet mellom tre og seks måneder. Departementets avgjørelse i klagesaken kan ikke påklages videre til Kongen i statsråd, men saken kan bringes inn for domstolene. Dette skjer svært sjelden (se nærmere om grunnene til dette i drøftelsen av om det er behov for klageadgang). Etter det utvalget kjenner til er det bare én klagesak som hittil er behandlet av domstolene (se Rt 1994 s 691 «Psykoseregisterdommen» hvor det ble reist krav om sletting og oppreisning).

18.3.8.2 Er det behov for klageadgang?

Det er naturlig å avklare innledningsvis om det er behov for å kunne kreve Datatilsynets enkeltvedtak overprøvet uten å måtte anlegge rettssak. I norsk forvaltningsrett er den store hovedregelen at enkeltvedtak kan påklages. Direktivet krever imidlertid ikke at det skal være adgang til administrativ klage (klage til et forvaltningssorgan), og det enkelte land står fritt på dette punktet. Klageordningen koster tid og ressurser, hvilket kan tilsi at adgangen til å kreve administrativ dobbelbehandling bør falle bort.

Flere grunner taler likevel for at det som i dag bør være klageadgang. Samfunnsmessige hensyn taler for klageadgang fordi behandlingen av klagesakene vekker debatt og interesse for saksfeltet. Like viktig er hensynet til klageren. Dersom det ikke skal være klageadgang, må den som ønsker å få overprøvd Datatilsynets vedtak bringe saken inn for domstolene. Klagebehandling vil ofte ta kortere tid enn domstolsbehandling. Dessuten er det billigere – ihvertfall sammenlignet med de tilfellene der saksøkeren selv må betale saksomkostningene som rettssaken fører med seg. I tillegg vil en domstolsprøving i tråd med læren om forvaltningens frie skjønn innskrenke seg til å være en prøving av Datatilsynets bevisbedømmelse, saksbehandling og lovtolkning. Forvaltningsskjønnet (f eks interesseavveiningen etter personregisterloven § 11) i den enkelte sak vil som den store hovedregelen ikke bli overprøvet av domstolene, og det er gjerne disse vurderingene som byr på tvil. Endelig vil domstolene i all hovedsak nøye seg med å prøve gyldigheten av tilsynets vedtak, og ikke selv avgjøre om f eks konsesjon skal gis. Det beste resultatet den private part kan håpe på ved domstolsbehandling er følgelig å få kjent tilsynsmyndighetens vedtak ugyldig, slik at saken må behandles på nytt av Datatilsynet. Erfaringene med personregisterloven viser at den private part så å si aldri bringer Datatilsynets avgjørelse inn for domstolene.

En klage over Datatilsynets vedtak vil dessuten ofte kunne starte en offentlig diskusjon om prinsipielle avveininger mellom personvern hensyn og andre hensyn. Slike diskusjoner kan være nyttig på flere måter; de kan bidra til en god opplysning av saken (alle hensyn kommer frem) og kan dessuten ha en folkeopplysende funksjon.

Utvalget vil på denne bakgrunnen gå inn for at det også i fremtiden bør være anledning til å få overprøvet Datatilsynets avgjørelser uten å måtte bringe saken inn for domstolene.

18.3.8.3 Skal Justisdepartementet fremdeles behandle klager over Datatilsynets vedtak?

Et neste grunnleggende spørsmål er om Justisdepartementet fremdeles skal behandle klager over Datatilsynets avgjørelser, eller om dette skal utføres at et forvaltningssorgan som er uavhengig av regjeringen og departementet.

Det er ikke noe konstitusjonelt i veien for å legge kompetanse til å behandle klager til et uavhengig forvaltningsorgan (jf Eivind Smiths utredning, vedlegg 5). Avgjørende er om det av ulike grunner er nødvendig eller ønskelig.

Den norske statsforvaltning er hierarkisk oppbygget. Øverst i hierarkiet står Kongen som etter den tradisjonelle hovedregel er politisk leder av og har politisk ansvar for statsadministrasjonen for øvrig. Under sin behandling av Ingvaldsenkomiteens innstilling (jf Tid S 1976 – 77 s 9 og Stort forh 1977 s 4077) sa Stortinget seg enig i at unntak fra å organisere forvaltningsapparatet i et hierarki under politisk ledelse må begrunnes i særlige hensyn. Stortinget har etter det utvalget kjenner til ikke gitt uttrykk for et annet syn senere.

Å legge klagebehandling til et organ som er uavhengig av regjeringen og departementet vil være et unntak fra den alminnelige forvaltningsstrukturen. Regjeringen er den nærmeste til å ha overordnet styring med og ansvar for utformingen av personvern- og IT-politikken, og å avgjøre klagesaker er et virkemiddel for å gjennomføre politiske målsettinger på området. Avgjørende blir om det likevel foreligger «særlige hensyn» som kan begrunne opprettelsen av en uavhengig klageinstans.

Sentralt i denne diskusjonen står direktivets krav til uavhengige tilsynsmyndigheter. Slik reglene er i dag, kan Justisdepartementet ved å behandle klagesaker bestemme hvordan Datatilsynet skal behandle liknende saker i fremtiden. Grunnen til dette er at departementets begrunnelse i en klagesak ofte er av prinsipiell eller generell karakter, slik at den sier noe om hvordan departementet vil avgjøre liknende klagesaker i fremtiden. Og hvis Datatilsynet vil unngå å få avgjørelsene omgjort av klageinstansen, må tilsynets praksis i førsteinstansbehandlingen være i samsvar med det syn departementet har gitt uttrykk for i tidligere klagesaker. Kompetanse til å behandle klager innebærer med andre ord en mulighet til å styre/instruere Datatilsynets praksis – en styringsmulighet som synes vanskelig å forene med direktivets krav til uavhengighet. Også en selvstendig klageinstans sine avgjørelser vil påvirke Datatilsynets praksis, men påvirkningen kommer da fra et organ som selv er tilsynsmyndighet i direktivets forstand, og ikke fra den utøvende statsmakt. Gjennomføringen av direktivets krav til uavhengighet er slik utvalget ser det et tungtveiende argument for å opprette en selvstendig klageinstans.

Det finnes enkelte andre argumenter som trekker i samme retning.

Opprettelsen av en uavhengig klageinstans kan føre til at avgjørelser i klagesaker oppfattes som uhildet og sterkere faglig begrunnet. Hensynet til effektivitet, særlig i form av rask saksbehandlingstid, kan også tale for at klagesakene bør behandles av en uavhengig klageinstans.

Endelig kan det være at klagesaksbehandling ikke bør være noen naturlig oppgave for departementene i fremtiden. St meld nr 35 (1991-92) om statens forvaltnings- og personalpolitikk kan tas til inntekt for at departementene i hovedsak skal være sekretariater for politisk ledelse og lede sektorpolitikken på departementets ansvarsområde. Faglige spesialfunksjoner og enkeltsaksbehandling skal primært håndteres av forvaltningsorganer utenfor departementene.

Utvalget legger til grunn at direktivets krav til uavhengige tilsynsmyndigheter gjør at dagens ordning med Justisdepartementet som klagebehandler ikke bør opprettholdes, og at det må opprettes en eget forvaltningsorgan til å behandle klager over Datatilsynets avgjørelser. Utvalget finner også en viss støtte for denne løsningen i andre hensyn, bl a i hensynet til effektiv behandling av klagesakene.

Spørsmålet blir så hvordan den nye klageinstansen (Personvernemnda) bør organiseres, noe som må ses i sammenheng med hvilke krav som bør stilles til Personvernemnda.

18.3.9 Organisering av Personvernemnda

18.3.9.1 Innledning og oversikt

Personvernemnda skal overta en funksjon som Justisdepartementet har i dag. Avgjørelsene i klagesaker legges til grunn i Datatilsynet, og har stor betydning for hvordan personvernet varetas. Det er således helt nødvendig at Personvernemnda organiseres og bemannes slik at den får tillit og legitimitet i samfunnet. Når Personvernemnda skal bygges opp er det også av betydning at lovtolkning i snever forstand sjelden blir avgjørende i klagesakene. Forvaltningsskjønnet – konkrete avveininger av personvern hensyn mot andre samfunnsmessige verdier – står derimot sentralt.

I det følgende drøftes den nærmere organiseringen av Personvernemnda. Det sies også noe om hvilke oppgaver Personvernemnda bør ha (18.3.9.5). Utvalget har delt seg i et flertall og et mindretall i synet på antall medlemmer i Personvernemnda og om Kongen bør oppnevne alle medlemmene, eller om oppnevningskompetansen bør være delt mellom Kongen og Stortinget, se 18.3.9.2. Utvalget er samstemmig i de øvrige spørsmålene som drøftes i 18.3.9.

18.3.9.2 Hvem bør oppnevne medlemmene i Personvernemnda?

Et *flertall* i utvalget bestående av medlemmene Bredengen, Gundersen, Hestnes, Håøy, Koch, Kristiansen og Meinich går inn for at Personvernemnda bør bestå av fem medlemmer. Samtlige av medlemmene og lederen bør oppnevnes av Kongen. På denne måten er det gode muligheter til å oppnå at Personvernemnda får en godt koordinert sammensetning, og det skapes klare linjer i forholdet mellom regjeringen og Stortinget. *Disse medlemmene* mener på prinsipielt grunnlag at det vil være uheldig å dele oppnevningen av medlemmene i klageinstansen mellom Kongen og Stortinget. Å bringe Stortinget inn i oppnevningen av et forvaltningsorgan som Personvernemnda vil være, ville innebære at Stortinget tildeles utøvende myndighet. Oppnevning dels av Kongen og dels av Stortinget vil dessuten kunne føre til at det vil være vanskeligere å sikre at Personvernemnda får en tilfredsstillende sammensetning kompetansemessig. *Flertallet* minner dessuten om at når Stortinget behandlet personregisterloven gikk komiteflertallet (de borgerlige partiene) inn for at styrets medlemmer skulle oppnevnes av Stortinget etter forslag av Kongen, som også skulle foreslå hvem som skulle være styrets formann og varaformann (Innst O nr 47 for 1977-78 s 5), men at forslaget ikke fikk tilstrekkelig tilslutning i den videre behandlingen av lovforslaget.

Et *mindretall* i utvalget, bestående av utvalgets leder og medlemmene Apenes og Schartum mener i likhet med flertallet at det er viktig å ta vare på den tradisjonelle og konstitusjonelle rollefordelingen mellom Stortinget og Kongen, og slutter seg til flertallets prinsipielle syn på at det normalt bør være Kongen som oppnevner medlemmene i forvaltningsorganer. *Disse medlemmene* mener imidlertid at det i dette konkrete tilfellet gjør seg gjeldende særskilte forhold som likevel kan begrunne en delt oppnevning myndighet. For det første vektlegger *disse medlemmene* at den nyopprettede Personvernemnda får et stort ansvar og en særlig viktig oppgave når den skal overta en oppgave som tidligere ble utført av et departement. For det andre berører personvern spørsmål hele befolkningen og gjelder et grunnleggende verdivalg i tilknytning til den videre utvikling og anvendelse av informasjonsteknologi i samfunnet. I slike spørsmål erkjenner *disse medlemmene* at Stortinget vil kunne representere en verdifull kanal med selvstendig betydning. For å sikre at Personvernemnda får en så bred og demokratisk forankring i befolkningen som mulig ser *disse medlemmene* det som riktig å foreslå at oppnevningssmy-

digheten deles mellom Kongen og Stortinget slik at Kongen oppnevner fem medlemmer, og at Stortinget deretter etter innstilling fra Stortingets valgkomite oppnevner Personvernnemndas leder og nestleder (tilsammen syv medlemmer i Personvernnemnda). En slik ordning vil understreke at personvern er en grunnleggende og omforent verdi i det norske samfunnet. *Mindretallet* presiserer for ordens skyld at det ikke er meningen at medlemmene i Personvernnemnda skal være fungerende stortingsrepresentanter – meningen er at Stortinget skal gis myndighet til å oppnevne (noen av) medlemmene i et forvaltningsorgan som skal treffe rettslig bindende avgjørelser. Også Stortinget forutsettes å basere sin oppnevning på kandidatens faglige skikkethet – ikke deres partipolitiske tilhørighet. Medlemmene som velges av Stortinget er ikke å betrakte som representanter for Stortinget eller for noe politisk parti.

18.3.9.3 Bemanningen av Personvernnemnda

Det må stilles kvalifiserte krav til hvem som skal kunne sitte i Personvernnemnda, som skal overta en funksjon som i dag tilligger Justisdepartementet. Medlemmenes kvalifikasjoner vil være avgjørende for om Personvernnemnda klarer å bygge opp den legitimitet og tillit den må ha for å vareta sin funksjon på en tilfredsstillende måte.

Personvernnemndas leder og nestleder bør tilfredsstillende kravene til dommere, jf domstolsloven §§ 53 og 54 annet ledd. Dette betyr ikke at vedkommende må være dommer, men at han eller hun må være kvalifisert til et dommerembete. For øvrig finner ikke utvalget det hensiktsmessig å formalisere kompetansekravene til medlemmene i Personvernnemnda. Avgjørende må være om vedkommende kandidat er egnet til å foreta avveiningen av personvern mot andre samfunnsinteresser som Personvernnemnda kommer til å foreta når den behandler klager, og til å overskue rekkevidden av de beslutningene som treffes.

Personvernnemnda bør sikres både kontinuitet og fornyelse, hvilket tilsier at medlemmenes funksjonstid bør være på fire år. Ideelt sett tilsier kravet til uavhengighet et forbud mot gjenoppnevning. Av hensynet til tilfredsstillende rekruttering går imidlertid utvalget inn for at medlemmene kan gjenoppnevnes én gang.

18.3.9.4 Bør Personvernnemnda ha andre oppgaver enn å behandle klager?

Personvernnemnda skal behandle klager, og har i tillegg anledning til å gripe inn på eget initiativ og omgjøre Datatilsynets avgjørelser dersom de alminnelige vilkårene for omgjøring i forvaltningsloven § 35 er oppfylt. Dette er rent faglige oppgaver. Spørsmålet er om Personvernnemnda i tillegg bør tillegges enkelte administrative gjøremål.

I tråd med at det er departementet som har det overordnede administrative ansvaret for tilsynet, er det naturlig at det er departementet og/eller et eventuelt styre og ikke Personvernnemnda som tar opp eventuelle administrative spørsmål med tilsynet. Også flere andre argumenter taler for en slik løsning. For det første er det viktig å synliggjøre at Personvernnemnda er et selvstendig forvaltningsorgan. For det andre kan det være lettere å rekruttere folk med de ønskede faglige kvalifikasjoner dersom Personvernnemnda utelukkende skal beskjeftige seg med faglige spørsmål.

Personvernnemnda bør orientere om behandlingen av klagesakene i tilsynsmyndighetens årsmelding.

18.3.9.5 Nærmere om forholdet mellom Datatilsynet og Personvernnemnda

Personvernnemnda vil være et eget uavhengig forvaltningsorgan, og er overordnet Datatilsynet ved behandling av enkeltvedtak. Etter forvaltningslovens regler (se forvaltningsloven § 28 flg) vil Personvernnemnda ha full kompetanse i klagesaker. Den kan overprøve Datatilsynets rettsanvendelse, faktumbedømmelse og skjønnsutøvelse (f eks om det skal gis konsesjon, og eventuelt på hvilke vilkår), og selv treffe avgjørelse i saken. Det er ikke bare realitetsavgjørelser som kan være gjenstand for klage, men også f eks beslutning om å ilegge tvangsmulkt for å gjennomføre et vedtak.

Personvernnemnda bør av hensyn til en reell totrinnsbehandling ved klage ikke ha kompetanse til å instruere Datatilsynet om utfallet i enkeltavgjørelser som er til behandling hos Datatilsynet. På den annen side er det klart at Personvernnemnda gjennom sine avgjørelser i klagesaker og gjennom eventuelle omgjøringsvedtak kan gi tilsynet veiledning om hvorledes denne type saker bør avgjøres i fremtiden, herunder hvordan loven skal tolkes og forvaltningsskjønnet utøves.

18.3.9.6 Nærmere om forholdet mellom Personvernnemnda og departementet

Personvernnemnda skal være rettslig uavhengig av regjeringen og departementet. Dette innebærer blant annet at regjeringen og departementet ikke kan instruere Personvernnemnda om utfallet i enkeltsaker, og ei heller gi generelle instruksjoner om lovtolkning eller skjønnsutøvelse (departementet kan imidlertid gi materielle forskrifter der loven gir hjemmel for dette). Regjeringen og departementet kan heller ikke av eget tiltak omgjøre vedtak som Personvernnemnda har truffet. Uavhengigheten i forhold til regjeringen og departementet knytter seg med andre ord til Personvernnemndas realitetsbehandling av klagesaker.

På samme måte som i forhold til Datatilsynet vil Personvernnemnda administrativt være underordnet regjeringen/departementet for såvidt gjelder bl a budsjettansvar og spørsmål om arbeidsordning som loven ikke tar stilling til.

18.3.9.7 Særlig om Personvernnemndas kompetanse i saker der regjeringen/departementet er part

Foran er det lagt til grunn at det skal opprettes en uavhengig klageinstans som skal behandle klager over Datatilsynets avgjørelser. I enkelte tilfelle kan det tenkes at Kongen og/eller departementet er part i en slik klagesak. Spørsmålet blir dermed om den uavhengige Personvernnemnda også skal avgjøre klager i slike saker. Problemstillingens *konstitusjonelle* side er vurdert av Eivind Smith (se vedlegg 5), som legger til grunn til at det ikke er noe konstitusjonelt i veien for at Personvernnemnda avgjør slike saker. Utvalget kan i det vesentlige slutte seg til Smiths begrunnelse og konklusjon. Dermed gjenstår å vurdere om det er *ønskelig* at Personvernnemnda avgjør klagesaker der Kongen og/eller departementet er part. Alternativet ville først og fremst være å la Kongen i statsråd bestemme utfallet i saken.

Utvalget ser klare fordeler med å la Personvernnemnda avgjøre samtlige klager over avgjørelser som Datatilsynet treffer. Blant annet hensynet til en helhetlig praksis og anvendelse av Personvernnemndas betydelige kompetanse på området tilsier dette.

18.3.10 Stortingets kontroll

Dersom det viser seg at tilsynsmyndigheten treffer prinsipielle avgjørelser som stortingsflertallet finner uheldig, er det naturlig for Stortinget å sørge for praksisen-

dring gjennom lovendring. Kontroll kan også finne sted ved behandling av tilsynsmyndighetens budsjetter, og ved behandlingen av Stortingsmeldingen om Datatilsynets årsmelding. Selv om departementet ikke lenger vil treffe avgjørelser i klagesaker eller instruere om hvordan Personvernemnda skal avgjøre klagesakene, og at departementet av den grunn ikke kan kritiseres for behandlingen av disse, betyr ikke dette at regjeringen/statsråden er fritatt for ansvar på saksfeltet. Stortinget kan f.eks. holde regjeringen/statsråden ansvarlig dersom forskriftene til loven ikke er tilfredsstillende eller det ikke settes av tilstrekkelige budsjettmidler.

18.4 DOMSTOLSPRØVING AV TILSYNSMYNDIGHETENS AVGJØRELSER

18.4.1 Gjeldende rett

Spørsmålet om domstolsprøving av Datatilsynets og Justisdepartementets avgjørelser etter personregisterloven reguleres av alminnelige sivilprosessuelle regler. I tråd med læren om forvaltningens frie skjønn vil domstolene kun i unntakstilfelle etterprøve tilsynets eller departementets utøvelse av forvaltningsskjønnet, se utvalgets merknader ovenfor under 18.3.8.2.

18.4.2 EF-direktivet artikkel 22

EF-direktivet artikkel 22 pålegger det enkelte medlemsland å sikre at enhver som mener at hans rettigheter etter nasjonal lovgivning om behandling av personopplysninger er krenket, skal kunne bringe saken inn for domstolene. Direktivbestemmelsen er ikke til hinder for at medlemslandene gir egne regler om administrativ klageadgang, og heller ikke for at det på nasjonalt plan gis regler om at administrativ klageadgang må være uttømt før saken kan bringes inn for domstolene.

18.4.3 Utvalgets vurderinger

Artikkel 22 om mulighet for domstolsprøving antas å være i overensstemmelse med gjeldende norsk rett, og utvalget ser ikke noe stort behov for å foreslå lovendringer.

Utvalget har særskilt vurdert om Datatilsynets avgjørelser ikke skal kunne bringes inn for domstolene før klageadgangen er benyttet, men kommet til at de meget få tilfellene det måtte være snakk om ikke begrunner en slik ordning.

KAPITTEL19

Sanksjoner**19.1 INNLEDNING**

Foran i utredningen er det gjort rede for hvordan utvalget mener reglene for behandling av personopplysninger best kan utformes. Utvalget har lagt vekt på å få frem at personverninteresser er viktige samfunnsinteresser, og på å utforme reglene på en måte som gjør at de – innenfor de rammene bl a direktivet setter – er mest mulig praktikable. Dette er viktige forutsetninger for at reglene i størst mulig grad skal bli respektert og etterlevd. Temaet i dette kapitlet er hvilke rettslige følger det skal få at loven eller vedtak fattet i medhold av loven likevel ikke overholdes.

Artikkel 24 («Sanktioner») i *EF-direktivet* pålegger medlemsstatene å fastsette sanksjoner for overtredelse av de nasjonale bestemmelser som gis til gjennomføring av direktivet:

«Medlemstaterne træffer de nødvendige foranstaltninger til at sikre, at dette direktiv gjennomføres i fuldt omfang, og de fastsetter bl. a. de sanktioner, der skal finde anvendelse i tilfælde af overtrædelse af de bestemmelser, der vedtages til dette direktivs gennemførelse.»

Sanksjonene som direktivet taler om kan være straffebestemmelser, men det er ikke noe krav i direktivet om at overtredelser skal straffesanksjoneres. Formålet med bestemmelsen er å sikre at direktivet gjennomføres i fullt omfang, men den enkelte staten står relativt fritt til selv å bestemme hvilke sanksjoner som bør benyttes. Det samme gjelder artikkel 10 i *Europarådskonvensjonen*, hvor det heter at hver part plikter å innføre «hensiktsmessige» sanksjoner.

Nedenfor drøftes ulike former for offentlige sanksjoner (se 19.2 om straff og 19.4 om bl a tvangsmulkt) og en form for privat sanksjon (se 19.3 om erstatning og oppreisning).

19.2 STRAFF**19.2.1 Gjeldende rett**

Personregisterloven § 38 kriminaliserer både forsettlig og uaktsomme overtredelser. Straffansvaret gjelder bare ved overtredelse av enkelte av lovens regler, se § 38 første ledd. Begrunnelsen for dette er at enkelte av lovens regler ble ansett for å være for skjønnsmessige til at overtredelser burde straffes, jf Ot prp nr 2 (1977-78) s 97 venstre spalte.

Unnlattelse av å etterkomme pålegg om sikring etter personregisterloven § 8 b rammes ikke av straffebestemmelsen i § 38. Dette skyldes antagelig en forglemmelse. Tidligere ble slike pålegg gitt med hjemmel i personregisterloven § 11 og overtredelse av vilkår fastsatt med hjemmel i § 11 var straffesanksjonert i § 38. Etter en endring av loven i 1987 (da § 8 b ble tilføyd) ble ikke straffebestemmelsen endret tilsvarende. Det er imidlertid ikke tvil om behovet for sanksjoner også på dette området.

Straffebudet i personregisterloven § 38 inneholder ikke noen begrensning med hensyn til subjekt (jf uttrykket «den som»), og retter seg f eks mot ansatte og tjenestemenn, og mot innleide konsulenter eller andre hjelpere.

Inntil 1991 inneholdt personregisterloven § 39 regler om straff for juridiske personer. Regelen var begrunnet med at det i et foretak med flere ansatte lett kan oppstå uklare ansvarsforhold, og at det da kan virke urimelig å legge skylden på en enkeltperson. Det ble også lagt vekt på at en regel om foretaksansvar gir et bedre grunnlag for utmåling av bot enn om ansvaret skulle ligge på en enkelt ansatt (jf Ot prp nr 2 (1977-78) s 97 høyre spalte). Personregisterloven § 39 ble opphevet fordi bestemmelsen ville være overflødig etter at det ved lov 20 juli 1991 nr 66 ble innført en generell regel om foretaksstraff i straffeloven kapittel 3 a. I motsetning til personregisterloven § 39 får straffelovens bestemmelser om foretaksstraff også anvendelse på offentlig virksomhet (jf Ot prp nr 27 (1990-91) s 29 høyre spalte). Med bestemmelsen i straffeloven § 48 a første ledd er det gitt generell hjemmel for å ilegge foretak (definert i annet ledd) straff i form av bot. Foretaket kan også fradømmes retten til å utøve virksomheten eller forbys å utøve den i visse former, se straffeloven § 48 a tredje ledd siste punktum sammenholdt med straffeloven § 29.

19.2.2 Utvalgets vurderinger

Når det gjelder straff som sanksjon ved overtredelse av loven og regler og vedtak fattet i medhold av denne, går utvalget i hovedsak inn for å videreføre dagens regler. I tråd med anbefalingen i Ot prp nr 27 (1990-91) s 11 høyre spalte bør *foretaksstraff* fremdeles reguleres i straffeloven. Hensynet til forutberegnelighet varetas ved at gjerningsbeskrivelsen fortsatt vil finnes i særloven.

Forsåvidt gjelder straff for *fysiske personer*, kan det reises spørsmål ved om uaktsomme overtredelser fremdeles skal være straffbare, eller om dette kan være for strengt, særlig for den som på grunn av små ressurser kan ha vansker med å kartlegge rettslige og faktiske konsekvenser som persondatabehandlingen medfører. Utvalget har imidlertid funnet det mest formålstjenlig å videreføre dagens regel. Det legges i den forbindelse vekt på at den som ut fra sine personlige forutsetninger har gjort så godt han har kunnet, normalt ikke vil ha utvist straffbar uaktsomhet selv om handlemåten strider mot en objektiv norm for forsvarlig opptreden, jf NOU 1992: 23 «Ny straffelov – alminnelige bestemmelser» s 119 venstre spalte. Utvalget har også lagt vekt på at det i dag er vanlig å kriminalisere uaktsomme handlinger på særlovgivningens område, noe som blant annet skyldes at krav til forsett kan skape betydelige bevisproblemer. Straffelovkommisjonen går i sin innstilling inn for at uaktsomme handlinger bør kriminaliseres i noe større utstrekning enn i dag, jf NOU 1983: 57 s 146 – 147 og NOU 1992: 23 s 122 høyre spalte. Endelig understreker utvalget at det bare er et utvalg av lovens bestemmelser som vil bli gjort straffbare, se nedenfor om legalitetsprinsippets krav til rimelig klar angivelse av den straffbare handling.

Utvalget mener også at dagens regel om medvirkning bør videreføres.

Utvalget går inn for at strafferammen i større grad bør tilpasses straffverdigheten av overtredelsen. Dagens strafferamme er den samme for lovbrudd av nokså ulik karakter. Overtredelse av reglene for behandling av personopplysninger kan i spesielt graverende tilfeller få store konsekvenser for den fornærmede, og etter utvalgets syn er det her behov for et noe mer nyansert system. Utvalget foreslår derfor at straffen under særdeles skjerpene omstendigheter kan settes til fengsel i inntil to år. Dette gjelder også ved uaktsomme overtredelser, men graden av skyld vil ha betydning i vurderingen av om det foreligger særdeles skjerpene omstendigheter. Ved avgjørelsen av om det foreligger særdeles skjerpene omstendigheter skal det forøvrig legges vekt på faren for stor ulempe eller fare for den registrerte, den tilsiktede vinning ved overtredelsen, overtredelsens varighet og omfang og på om den skyldige tidligere er straffet for overtredelse av tilsvarende overtredelser.

Noen strengere strafferamme enn dette er det neppe behov for – reguleringen her må ses i sammenheng med straffelovens bestemmelser om datakriminalitet (jf oversikten i «Datakriminalitet», ØKOKRIMs stensilserie nr 9, Oslo 1995).

Legalitetsprinsippet slik det er nedfelt i straffeloven § 96 krever at lovbestemmelser som skal straffesanksjoneres må ha en viss grad av presisjon – det må stilles opp relativt faste kriterier for når noe skal være straffbart. I dagens lov er dette løst slik at det bare er et utvalg av lovens bestemmelser der overtredelser straffesanksjoneres. Utvalget legger til grunn at ikke alle bestemmelsene i den nye loven er tilstrekkelig presise til at de bør straffesanksjoneres. Dette gjelder for eksempel §§ 7, 8, 9 og 10. Se forøvrig merknadene til lovforslaget § 42.

19.3 ERSTATNING OG OPPREISNING

19.3.1 Oversikt over gjeldende rett

Personregisterloven § 40 pålegger *kredittopplysningsforetak* objektivt erstatningsansvar (ansvar selv om det ikke er utvist uaktsomhet):

«Har foretak som driver virksomhet som nevnt i § 13, meddelt opplysninger i strid med bestemmelser gitt i eller i medhold av loven her, eller meddelt opplysninger som viser seg uriktige eller åpenbart misvisende, skal foretaket erstatte det tap som påføres den opplysningene gjelder. Dette gjelder uten hensyn til om det er utvist skyld fra noen som har opptrådt på vegne av eller i tjeneste hos firmaet.»

Alternativet «åpenbart misvisende» opplysninger har særlig betydning ved meddelelse av vurderinger, for eksempel i forbindelse med et kredittopplysningsforetaks vurdering av en persons kredittverdighet.

Det er foretaket som er erstatningsansvarlig i henhold til bestemmelsen, ikke enkeltpersonene som har handlet på vegne av foretaket. Datatilsynet har antatt at ansvaret ikke gjelder for virksomheter som er unntatt etter forskrift 21 desember 1979 § 4-2.

Erstatningsansvaret etter § 40 gjelder påvist økonomisk tap, som f.eks. ekstra utgifter i forbindelse med nektet kreditt og advokat- og telefonutgifter.

For andre virksomheter enn kredittopplysningsforetak finnes det ingen lovregel i personregisterloven, men det alminnelige ulovfestede uaktsomhetsansvaret vil gjelde også her.

Personregisterloven gir i dag ikke grunnlag for å kreve erstatning for skade som ikke har resultert i noe økonomisk tap. Oppreisningsregelen i skadeserstatningsloven § 3-6 gjelder bare ved ærekrenkelses og krenking av privatlivets fred (slik disse begrepene brukes i straffeloven §§ 246 flg og 390).

19.3.2 Internasjonale regler

Artikkel 23 i EF-direktivet («Ansvar») pålegger medlemsstatene å gi nærmere regler om erstatningsansvar for den registeransvarlige:

«1. Medlemsstaterne fastsetter bestemmelser om, at enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenlig med de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, har ret til erstatning for den forvoldte skade fra den registeransvarlige.

2. Den registeransvarlige kan helt eller delvis fritages for erstatningsansvar for skade, hvis han beviser, at han ikke er skyld i den begivenhed, der medførte skaden.»

Direktivet oppstiller i utgangspunktet et objektivt erstatningsansvar (ansvar uten skyld). Uttrykket «lidt skade» kan etter sin ordlyd hevdes å omfatte både skade som resulterer i et økonomisk tap, og skade som ikke resulterer i et økonomisk tap. Det er imidlertid usikkert om direktivet må forstås på denne måten. I andre EØS-land synes meningene å være delte, og tolkningsspørsmålet må anses som uavklart.

I artikkel 23 nr 2 åpnes det for at den registeransvarlige helt eller delvis kan fritas for ansvar dersom han godtgjør at han ikke er skyld i den begivenhet som var årsak til skaden. Et slikt ansvar – culpaansvar med omvendt bevisbyrde – vil være mindre strengt for skadevolderen enn et objektivt ansvar.

19.3.3 Justiskomiteens uttalelser i Innst S nr 80 (1991-92)

I Innst S nr 80 (1991-92) fra justiskomiteen om personvern, erfaringer og utfordringer og om Datatilsynets årsmelding for 1990, uttalte komiteen følgende om erstatningsspørsmålet (s 11 høyre spalte):

«Komiteen viser til gjeldende erstatningsregler i personregisterloven, der kredittopplysningsvirksomhet er pålagt et objektivt ansvar for tap som måtte oppstå ved at det er registrert feil opplysninger. Komiteen vil be Regjeringen vurdere om det er ønskelig å utvide ansvarsregelen i § 13 til andre typer registre, f. eks. offentlig virksomhet, og også om det bør innføres en lovhjemmel for oppreisningserstatning. Komiteen viser til at oppreisningsregelen i § 3-5 stiller svært strenge krav for å tilkjenne erstatning, og at det bør vurderes om det i hvert fall innen visse bransjer kan være grunnlag for erstatning på et mindre strengt grunnlag.»

Utvalget er i sitt mandat bedt om å vurdere de forslag justiskomiteen har kommet med.

19.3.4 Utvalgets vurderinger

19.3.4.1 Oversikt

Nedenfor drøftes først om det skal være objektivt eller subjektivt erstatningsansvar når det foreligger økonomisk tap, og deretter om det bør kunne kreves erstatning for ikke økonomisk tap (oppreisning).

19.3.4.2 Erstatning for økonomisk tap

19.3.4.2.1 Bør det lovfestes regler om erstatning for alle former for virksomhet som omfattes av loven?

I dag er det bare erstatningsansvar for kredittopplysningsforetak som reguleres i personregisterloven. Spørsmålet her er om den nye loven bør regulere erstatningsansvaret til alle former for virksomhet som omfattes av loven.

Utvalget har kommet til at en slik løsning er mest oversiktlig, og best egnet til å gjennomføre direktivet. Om en slik endring reelt sett innebærer et strengere ansvar enn i dag for andre virksomheter enn kredittopplysningsforetak, avhenger av hvilket ansvarsgrunnlag som legges til grunn, se nedenfor.

19.3.4.2.2 Objektivt eller subjektivt ansvarsgrunnlag?

Det eneste eksemplet vi i norsk rett i dag har på objektivt erstatningsansvar i denne sammenheng er personregisterloven § 40, se nærmere ovenfor. For alle andre virk-

somheter enn kredittopplysningsvirksomhet gjelder det vanlige ulovfestete culpaansvaret.

Objektivt erstatningsansvar blir tradisjonelt benyttet der det er en stadig, typisk og ekstraordinær skaderisiko ved virksomheten. I slike tilfelle kan virksomheten innkalkulere ansvaret som en driftsutgift, og objektivt ansvar kan ha en gunstig preventiv effekt.

For de fleste typer virksomheter som omfattes av loven er det lite naturlig å tale om at behandlingen av personopplysninger i seg selv utgjør en typisk, stadig og ekstraordinær skaderisiko. Behandlingen er et nødvendig ledd i en «hovedvirksomhet», og ikke noe mål i seg selv. Et unntak er kredittopplysningsvirksomhet, hvor misbruk av personopplysninger nettopp utgjør en slik risiko.

Utvalget går på denne bakgrunn inn for at den behandlingsansvarlige skal være ansvarlig for forvoldelse av økonomisk tap, men at skadevolderen slipper ansvar dersom han eller hun godtgjør at vedkommende ikke har utvist uaktsomhet (se merknadene til lovforslaget § 43).

For kredittopplysningsforetak bør det som i dag gjelde et objektivt ansvar. Utvalget bemerker i den forbindelse at erstatningsansvar i medhold av personregisterloven § 40 svært sjelden forekommer, og på at eventuelle urimelige følger av et objektivt erstatningsansvar kan avhjelpes gjennom lempning etter skadeserstatningsloven § 5-1.

Erstatningsansvaret påhviler i begge tilfelle den behandlingsansvarlige og på den driftsansvarlige dersom denne er en annen enn den behandlingsansvarlige. Ansvarer gjelder ved overtredelse av loven og forskrifter gitt i medhold av den, samt når tilsynsmyndighetens vedtak ikke overholdes og dette påfører noen skade.

19.3.4.3 Oppreisning

19.3.4.3.1 Er det behov for en oppreisningsregel?

Sandvik-utvalget foreslo i NOU 1974: 20 lovregler om erstatningsansvar, herunder regler om erstatning for ikke-økonomisk tap. For kredittopplysningsforetak skulle ansvaret være objektivt. *Seip-utvalget* (som utredet offentlige personregistre) fant ikke grunn til å foreslå særlige erstatningsregler. Når det ikke ble foreslått regler om oppreisning skyldes dette dels at effektivisering av lovreglene etter Seip-utvalgets syn burde skje gjennom straffetrusselen, og dels fordi det utfra hensynet til den enkelte syntes lite naturlig å anvende økonomiske kompensasjonssynspunkter. Departementet fant ikke grunn til å foreslå noen oppreisningsregel, jf Ot prp nr 2 (1977-78) s 62:

«En innføring av særlige oppreisningsregler bør etter departementets oppfatning ikke skje med mindre det er et klart behov for en videregående adgang til å tilkjenne ikke-økonomisk erstatning på dette området. Departementet har ikke funnet at de foreliggende utredninger godtgjør at det er et slikt behov. [...] Behovet for slike særlige sanksjoner mot slike krenkelser antas forøvrig å være tilstrekkelig varetatt ved regler som er foreslått om straff og erstatning.»

Jon Bing og Cato Schiøtz har i en artikkel i *Jussens Venner* 1977 s 241 – 270 argumentert for en egen oppreisningsregel for personregisterkrenkelser, se også Jon Bing i *Lov og Rett* 1977 s 433-434. Forfatterne mener at et vanlig erstatningsansvar vil ha liten verdi på dette området, fordi det sjelden vil kunne dokumenteres noe økonomisk tap. Dessuten pekes det på at en oppreisningsregel kan gjøre straffetrusselen mer effektiv, fordi den krenkede trolig oftere vil melde forholdet til politiet for på den måten å få oppreisningskravet pådømt i straffesaken.

Både Sverige, Danmark og Finland har regler om oppreisning ved misbruk av personopplysninger. Erfaringene går i hovedsak ut på at det har vært få saker med krav om slik oppreisning, og at beløpene gjennomgående har vært små.

Utvalget er i tvil om det er behov for en oppreisningsregel. Erstatningsregler har tradisjonelt både et preventivt og et reparerende formål. Om det av preventive grunner er behov for en oppreisningsregel, kommer blant annet an på hvor effektivt en mener at de eksisterende sanksjonsmidlene virker. Den objektive erstatningsregelen i personregisterloven § 40 er svært sjelden brukt, selv om den kan ha virket som et «ris bak speilet». Straffereglene har heller ikke blitt mye brukt. Den mest effektive sanksjonen i dag er trolig at Datatilsynet kan trekke tilbake personregisterkonsesjonen. Om en oppreisningsregel vil styrke prevensjonen utover dette, kommer blant annet an på hvor stor risiko det er for at det rettes krav mot en, og på hvor alvorlig en venter at reaksjonen vil bli.

For den *skadelidte* vil en oppreisningssum til en viss grad kunne virke reparerende, selv om det ikke alltid vil være like passende å bøte skaden med penger.

En fare med en oppreisningsregel kan være at oppreisningssummen blir meget høy, med de uheldige virkninger dette kan ha. Sett hen til de gjennomgående lave beløp norske domstoler har tilkjent i oppreisningssaker hittil, er det imidlertid liten grunn til å frykte en slik utvikling. Og under enhver omstendighet kan det dersom det er behov lovfestes regler om maksimalt oppreisningsbeløp.

Utvalget har etter atskillig overveielse lagt avgjørende vekt på at det er uhyre vanskelig å finne et adekvat økonomisk uttrykk for denne type skade som ikke har resultert i noe økonomisk tap. Sett fra skadelidtes side vil det gjennomgående være atskillig mer tilfredsstillende dersom skadevolderen pålegges å sørge for at følgene av skaden blir minst mulig. Utvalget går derfor inn for at gjenoppsettregelen i personregisterloven § 8 første ledd siste punktum videreføres og videreutvikles, slik at skadelidte har plikt til å sørge for at feilen så vidt mulig ikke får betydning for den registrerte. Utvalget legger til grunn at en slik løsning – sett i sammenheng med flere andre godt utbyggede sanksjonsmidler – tilfredsstiller direktivets krav til ansvarsregler.

19.4 ANDRE SANKSJONER

19.4.1 Problemstilling

På bakgrunn av at behandling av personopplysninger blir stadig mer utbredt, og behovet for å sørge for forsvarlig bruk av personopplysninger dermed stadig blir viktigere, kan det stilles spørsmålsteget ved om straff og erstatning er tilstrekkelig effektive sanksjoner. Mens strafforfølgning er ressurskrevende og kan ta lang tid, forutsetter erstatningssanksjonen at den skadelidte selv gjør sitt krav gjeldende. Selv om erstatningsreglene som utvalget foreslår kan føre til at det blir noe lettere å få tilkjent erstatning enn etter dagens regler, er det grunn til å tro at mange skadelidte heller ikke i fremtiden ønsker eller har ressurser til å forfølge sitt krav innen rettsapparatet. Utvalget har derfor funnet det hensiktsmessig å vurdere om det foreligger andre sanksjonsmuligheter som et supplement til straff og erstatning.

Datatilsynet har i dag lovhjemmel til å komme med påbud, men har ingen sivilrettslige økonomiske sanksjonsmidler dersom påbudet ikke blir fulgt opp. Det blir imidlertid stadig vanligere å gi tilsynsorganer adgang til å iverksette sivilrettslige administrative sanksjoner som et supplement til straffesanksjoner. Nedenfor gis en redegjørelse for og vurdering av to former for myndighet som det kan være aktuelt å gi til tilsynsmyndigheten; rett til å ilegge tvangsmulkt, og rett til å gi forelegg om inndragning av vinning.

19.4.2 Tvangsmulkt

En etterhvert vanlig form for administrativ sanksjon i norsk rett er bruk av *tvangsmulkt*, dvs en løpende mulkt som ilegges av myndighetene, og som gjerne forhøyes over tid inntil en uønsket atferd (f eks overtredelsen av et pålegg gitt i medhold av loven) opphører. Denne sanksjonsformen er – med større eller mindre variasjoner – lovfestet i en rekke formelle lover, jf for eksempel kredittilsynsloven § 10 siste ledd (hjemmel for Kredittilsynet til å ilegge daglig mulkt ved overtredelse av påbud), børsløven § 6 annet ledd (hjemmel for daglig løpende mulkt dersom opplysningsplikten ikke oppfylles) og konkurranseløven § 6-4 (mulkt kan ilegges dersom et enkeltvedtak ikke respekteres).

Etter utvalgets syn bør også tilsynsmyndigheten på personvernområdet gis mulighet til å ilegge en løpende mulkt der dette finnes nødvendig for å sikre at enkeltvedtak som er truffet i medhold av loven etterleves (lovforslaget § 41). Mulkten bør kunne pålegges både overfor fysiske og juridiske personer, og størrelsen bør fastsettes av tilsynsmyndigheten ut fra alminnelige forvaltningsrettslige prinsipper, herunder hensynet til forholdsmessighet mellom mål og virkemidler. Vedtak om bruk av tvangsmulkt vil være enkeltvedtak i forvaltningslovens forstand, og vil kunne påklages til Personvernemnda. Mulkten begynner ikke å løpe før enten klagefristen er ute, eller – hvis vedtaket påklages – på det tidspunkt Personvernemnda eventuelt opprettholder førsteinstansens vedtak. Effektivitetshensyn tilsier at vedtaket om å ilegge mulkt er tvangsgrunnlag, jf tvangsloven § 7-2 bokstav e.

19.4.3 Inndragning

Som det fremgår ovenfor, foreslår utvalget at tilsynsmyndigheten gis hjemmel til å ilegge tvangsmulkt dersom enkeltvedtak truffet i medhold av loven ikke overholdes. Spørsmålet blir videre om det er behov for å gi tilsynsmyndigheten ytterligere sivilrettslige sanksjonsmuligheter. I konkurranseløven § 6-5 er Konkuransetilsynet gitt myndighet til å utferdige forelegg om avståelse av vinning dersom vinningen er oppnådd ved overtredelse av konkurranseløven eller vedtak i medhold av loven. Dersom forelegget ikke vedtas, har Konkuransetilsynet tre måneder på å reise sivil søksmål mot den forelegget er rettet mot. Hvis det reises straffesak, kan kravet om vinningsavståelse tas med i straffesaken som inndragningskrav etter straffeløven § 34 (den alminnelige inndragningsregelen i straffeløven).

Utvalget har kommet til at Datatilsynet neppe har behov for ytterligere sanksjonsmidler.

KAPITTEL20

Økonomiske og administrative konsekvenser av utvalgets forslag

20.1 INNLEDNING

Utvalget har foreslått tildels betydelige endringer i både personvernregelverket og administrasjonen av dette, se "*Lovens saklige og geografiske virkeområde*" i kapittel 10 – 19 hvor forslagene er nærmere omtalt. I disse kapitlene er administrative og økonomiske konsekvenser av mulige alternativer flettet inn i utvalgets vurderinger. Dette gjelder særlig "*Tilsynsmyndigheten*" i kapittel 18 om tilsynsmyndighetens organisasjon og oppgaver. Utvalget har forøvrig ikke hatt mulighet til å foreta nøyaktige beregninger av forslaget økonomiske konsekvenser. Det er ikke i dag mulig og heller neppe hensiktsmessig å gi noen begrunnet oppfatning om detaljerte budsjettspørsmål. Utvalget vil av disse grunner nøye seg med å gi en oversikt over hovedtrekkene av de økonomiske og administrative konsekvensene forslaget innebærer.

20.2 KONSEKVENSER FOR JUSTISDEPARTEMENTET

Utvalget foreslår at klager over Datatilsynets vedtak ikke lenger skal behandles av Justisdepartementet, men istedet av en egen sakkyndig Personvernemnd. Dette medfører at Justisdepartementet får frigitt ressurser som ellers ville gått med til klagebehandling.

Departementet må sørge for at det opprettes en Personvernemnd. Personvernemndas medlemmer, som forutsettes å være høyt kvalifiserte, vil fungere som medlemmer ved siden av andre stillinger eller verv på samme måte som medlemmene av dagens Datatilsynsstyre. Det forutsettes at honorarene fastsettes på en måte som sikrer tilstrekkelig kvalifiserte medlemmer. I tillegg vil Personvernemnda trolig ha behov for et sekretariat på 1-2 personer som det i så fall må avsettes midler til.

20.3 KONSEKVENSER FOR DATATILSYNET

20.3.1 Innledning

Tilsynsvirksomhet på grunnlag av den nye loven blir en viktig samfunnsoppgave. Nye måter å bruke personopplysninger på krever nye tilsynsverktøy. Utvalget har i tråd med dette foreslått at Datatilsynet gis til rådighet et bredt spekter av oppgaver og reguleringsredskaper, samt en betydelig fleksibilitet og valgfrihet mht hvordan oppgavene skal prioriteres og virkemidlene skal benyttes. Forslagene medfører at Datatilsynet i en overgangsperiode vil ha behov for betydelige økte ressurser, både i form av økt kompetanse hos de ansatte og i form av opprusting av teknisk utstyr.

Nedenfor kommenteres nærmere noen økonomiske og administrative virkninger det nye reguleringsregimet har og kan ha for Datatilsynet.

20.3.2 Omleggingen av konsesjonsordningen – meldeplikt

Utvalget foreslår at *konsesjonsplikten* skal begrenses i forhold til dagens ordning. Dette vil frigjøre ressurser som konsesjonsbehandlingen i dag båndlegger, og over-

gangen til et system med meldeplikt i kombinasjon med en redusert konsesjonsplikt vil isolert sett føre til en redusert arbeidsmengde for tilsynet. Også en *meldepliktordning* forutsetter imidlertid en eller annen form for oppfølging av meldingene. Hvordan denne oppfølgingen skal skje, er opp til tilsynet selv, og utvalget vil nøye seg med å komme med noen innspill om hvorledes den administrative behandlingen av meldingene *kan gjennomføres*.

En *delvis automatisering* av meldingsbehandlingen vil kunne spare manuell arbeidsinnsats hos tilsynet, og åpne for mer effektiv kontroll. Automatiseringen av meldepliktordningen kan deles inn i rutiner for innsamling og oppdatering av meldingene, rutiner for bearbeiding av meldingsopplysningene, og rutiner for kommunikasjon med de meldepliktige.

Når det gjelder rutiner for *innsamling av meldingene* kan det være hensiktsmessig å la den meldepliktige *velge* om han eller hun vil benytte en elektronisk melding eller en tradisjonell papirmelding (jf Den norske IT-veien, Bit for bit, rapport fra Statssekretærutvalget for IT pkt 3.3.6). Forsåvidt gjelder elektroniske meldinger kan dette gjennomføres ved å legge meldingsskjemaet ut på Datatilsynets tekstvev-sider, slik at meldinger kan sendes over nettet i et på forhånd fastlagt format. For den gruppen av meldepliktige som har tilgang til nettet vil bruk av elektroniske meldinger fremstå som brukervennlig og billig. Utvalget understreker at en meldepliktordning i de nærmeste årene ikke utelukkende kan baseres på en elektronisk innrapportering, og at det må stilles samme innholds krav til begge meldingsmåtene.

Forsåvidt gjelder rutiner for bearbeiding av innholdet i meldingene, kan det være hensiktsmessig å sørge for at opplysningene gjøres *søkbare*. På denne måten kan ny teknologi benyttes til å bearbeide og trekke informasjon ut av meldingene. Dette forutsetter at meldingene foreligger i maskinlesbar form (noe som f eks kan oppnås ved å tillate meldinger sendt med elektronisk post og ved å scanne innkomne papirmeldinger). For at meldingene skal gi størst mulig nytte for tilsynet, vil det være en fordel om meldingene inneholder indikatorer for personvernutrusler og kriterier som i en søkeprosess gjør det mulig å skille mellom ulike former for virksomheter. Eksempler på søkekriterier kan være «overføring av opplysninger til tredjeland», hvor søket vil gi en oversikt over behandlingsansvarlige som har gitt melding om at overføring skjer. Datatilsynet kan på dette grunnlaget foreta en stikkprøvebasert kontroll for å undersøke om vilkårene for slik overføring er oppfylt, og – dersom vilkårene ikke er oppfylt – gi pålegg om at overføringen ikke skal finne sted.

Det tredje settet av administrative rutiner knyttet til meldingsbehandlingen gjelder *kommunikasjon med de meldepliktige*. Den meldepliktige bør få en kvittering om at meldingen er mottatt. Dersom det er benyttet elektronisk melding, kan det være aktuelt å gi en elektronisk kvittering. Sammen med kvitteringen kan det også sendes informasjon om rettigheter som tilkommer den registrerte.

Utvalget understreker at automatiseringen ikke må komme mellom saksbehandlerne og de meldepliktige, men snarere etablere kontakten mellom disse og bedre mulighetene for prioritert innsats.

20.3.3 Etterfølgende kontroll og rådgivning

Datatilsynet vil i henhold til utvalgets forslag få flere hjemler til å gripe inn i etterkant og forby eller sette vilkår for behandling av personopplysninger som ikke respekterer lovens nye materielle regler. I tillegg er det ønskelig at Datatilsynet skal yte betydelig bistand på frivillig basis der det ønskes råd om hvordan personvern kan varetas. For at Datatilsynet skal kunne fylle disse oppgavene kreves trolig noe større ressurser enn tilsynet har i dag.

20.3.4 Datatilsynets styre

Utvalget er delt i spørsmålet om Datatilsynet fortsatt skal ledes av et styre (se 18.3.7). En videreføring uten styre vil naturlig frigjøre de ressurser som i dag tilføres styret. Opprettholdes dagens styreordning forventes ressursbehovet å bli omtrent som i dag.

20.3.5 Bør Datatilsynet i større grad være selvfinansierende?

Datatilsynet har i dag inntekter på i underkant av en million kroner hvert år (for budsjetterminen 1997 er det kalkulert med samlede inntekter på 897.000 kroner, jf St prp nr 1 (1996-97) s 98). Inntektene skyldes hovedsaklig at virksomhetene som reguleres i personregisterloven kapitlene 5 – 8 betaler et gebyr på kr 3.000 hvert år. Gebyrordningen har hjemmel i personregisterloven § 5 om dekning av utgifter til kontrollvirksomhet og er fastsatt i forskrift 12 desember 1988 nr 1010. (Datatilsynets utgifter er i 1997 i underkant av 10 millioner kroner). I *Sverige* er tilsynet selvfinansierende ved at det betales gebyr for de oppgaver tilsynet utfører.

Utvalget ser det ikke som ønskelig at Datatilsynet skal være fullstendig selvfinansierende i den forstand at alle utgifter dekkes inn gjennom gebyrer av ulik art. Generelt sett er det grunn til å være varsom med å kreve særskilt betaling for myndighetsutøvelse. En slik utvikling ville foruten prinsipielle betenkeligheter også medføre arbeid med å inndrive forfalte gebyrer. Det bør som i dag være adgang til å kreve dekning av utgiftene ved kontroll.

Forsåvidt gjelder innsending av meldinger, er utvalget derimot skeptisk til å knytte en betalingsplikt til meldingen. Erfaringer fra andre områder viser at en slik ordning kan føre til at enkelte unnlater å melde fra for på den måten å omgå betalingsplikten. Ettersom meldingene i det nye reguleringsystemet vil stå sentralt i kommunikasjonen mellom Datatilsynet og de behandlingansvarlige, er det viktig å legge forholdene til rette for at meldingsplikten faktisk etterleves.

Datatilsynet driver i dag med utstrakt informasjonsvirksomhet, og utvalget ser det som ønskelig at dette arbeidet videreutvikles. For deler av informasjonsmaterialet kan det være naturlig å kreve betaling dersom borgerne ønsker å motta materialet. Dette gjelder for eksempel publikasjonen «Spor», og for kurs og seminarer som Datatilsynet arrangerer. Utvalget understreker at det er en forutsetning at store deler av informasjonsvirksomheten til Datatilsynet fortsatt skal være gratis for brukerne. Gratis i betydningen uhindret tilgang til informasjon er særlig viktig fordi personvern hensyn trolig av mange (ofte feilaktig, se "*Hva er personvern?*" i kapittel 3) oppfattes som motsetning til effektivitetshensyn og økonomiske interesser, og av den grunn nedprioriteres.

Muligheten til å ilegge tvangsmulkt dersom pålegg fra Datatilsynet ikke etterleves vil kunne gi inntekter til staten.

20.4 KONSEKVENSER FOR DE BEHANDLINGSANSVARLIGE

Forslaget gir den enkelte som opplysningene gjelder flere individuelle rettigheter, bl a mer omfattende innsynsrett og krav på varsel ved enkelte former for innsamling av opplysninger. Dette vil påføre de behandlingsansvarlige kostnader. Hvor store kostnadene ved bruken av rettighetene vil bli, er for mange rettigheters vedkommende avhengig av hvor mange registrerte som benytter seg av retten. I dag blir individuelle rettigheter som krever initiativ fra den enkelte relativt sjelden brukt. Skulle det vise seg at bruk av disse rettighetene medfører merkbare kostnader, vil det være naturlig å innkalkulere kostnadene som driftsutgifter. Ettersom bruken og kostnadene forbundet med bruken av individuelle rettigheter formentlig vil fordele

seg jevnt på de behandlingsansvarlige, og tilsvarende rettigheter finnes i andre EØS-land, er det ikke grunn til å tro at kostnadene i særlig grad vil virke konkurransevridende eller vanskeliggjøre lovlig behandling av personopplysninger. Det bør i denne sammenheng også minnes om at forslaget til ny lov i stor grad bygger på et EF-direktiv som Norge – uansett kostnader – har forpliktet seg til å gjennomføre, og at lovforslaget ikke legger opp til vesentlig mer kostnadskrevende ordninger enn det direktivet medfører.

Utvalget antar at kostnadene ved *varslings* kan begrenses ved at varsel gis når den behandlingsansvarlige av andre grunner kommer i kontakt med den registrerte.

Den reduserte *konsesjonsplikten* vil gjøre det lettere å sette i gang med en del behandlingsformer som tidligere ville krevd konsesjon.

Flere *materielle regler* i loven har blant annet som formål å gjør det lettere for den behandlingsansvarlige å vite hva han har å forholde seg til.

Deltagelse i utarbeidelsen av *bransjevise atferdsnormer* vil kreve ressurser, men er frivillig og kan på sikt ha positive økonomiske virkninger fordi reglene virker avklarende. Deltagelse i slikt arbeid kan også være et konkurransefortrinn fremfor virksomheter som ikke deltar, fordi forbrukerne ser på varetagelsen av personvern som noe positivt.

Den behandlingsansvarlige som ikke plikter å sende melding eller søke om konsesjon plikter like fullt å ha viss *informasjon tilgjengelig*, se lovforslaget § 16. Den informasjonen som skal holdes tilgjengelig vil imidlertid som regel allerede foreligge ved utarbeidelsen av behandlingssystemet, og ofte også kreves av andre myndigheter. Merkostnadene her må derfor anses som ubetydelige.

Del III
Utvalgets lovforslag med merknader

KAPITTEL21

Merknader til de enkelte bestemmelsene

"Sammendrag av personregisterlovutvalgets utredning" i Kapittel 1 Lovens formål og område

§ 1 Lovens formål

Lovens formål er å bidra til at behandling av personopplysninger skjer i samsvar med grunnleggende personvern hensyn, herunder behovet for tilstrekkelig opplysningskvalitet, personlig integritet og privatlivets fred.

Til § 1

Paragraf 1 inneholder lovens formålsbestemmelse (jf direktivet artikkel 1 nr 1), og er ny i forhold til personregisterloven. Bestemmelsen ligger innenfor rammene av Stortingets vedtak 21 april 1994 (jf utvalgets mandat 2 c) der det heter at:

«Stortinget ber Regjeringen legge fram forslag til endringer i lov om personregistre, slik at loven får en formålsparagraf som slår fast retten til vern mot utilbørlig inngripen i menneskers privatliv.»

Formålsbestemmelsen har flere funksjoner. For det første gir bestemmelsen uttrykk for den overordnede målsettingen som loven skal bidra til at blir oppfylt; at behandling av personopplysninger behandles på en måte som er i samsvar med grunnleggende personvern hensyn.

For det andre vil formålsbestemmelsen være et relevant moment ved tolkning av lovens øvrige bestemmelser. Formålsangivelsen viser til «grunnleggende personvern hensyn». I dette ligger det en henvisning til festnede oppfatninger om personvern, slik dette vil bli nedfelt i praksis fra domstolene, rettsteori og administrative avgjørelser. På den måten vil formålsbestemmelsen på sikt gi rom for og retning til en rettsutvikling, særlig ved anvendelse av skjønnsmessige og vurderingspregede bestemmelser.

Lovforslaget angir flere virkemidler som skal fremme lovens formål. Det etableres en rekke plikter for den behandlingsansvarlige og den registrerte gis ulike rettigheter. I tillegg skal loven etablere holdninger både hos mulige behandlingsansvarlige og registrerte som sammen med de materielle reglene i lovforslaget skal bidra til at behandling av personopplysninger skjer i samsvar med grunnleggende personvern hensyn.

Utvalgets medlem Georg Apenes understreker ønskeligheten av at lovens formålsparagraf får en klar form og et konkret innhold. Den skal inneholde politiske signaler og ha informasjonsverdi. En regulering i lovs form av bruken av personopplysninger henvender seg til så store deler av befolkningen at den bør betraktes som en allmenlov hvis innhold ideelt sett må kunne være tilgjengelig for alle. Sproget i det fremlagte lovforslaget preges av at utvalgets sammensetning domineres av jurister hvorav de fleste er tilknyttet statsadministrasjonen. Forslag om supplerende medlemmer ble avvist av Justisdepartementet. Sproget er ofte tungt og begrepsbruken utpreget juridisk. Med den tid som har stått til utvalgets disposisjon, har det ikke vært mulig å søke profesjonell bistand med sikte på å øke tilgjengeligheten for ikke-jurister. Dette medlemmet legger vekt på at Stortinget i sitt vedtak av 21. april 1994 forutsatte at de pålagte lovrevisjonsarbeidet skulle ta sitt utgangspunkt i en

betraktning knyttet til en borgerlig rettighet. Regler og rettshåndhevende institusjoner som har som formål å imøtekomme borgerens krav på personvern, er derfor alle funksjoner av en rettighet den enkelte har. Denne retten bør identifiseres og fastslås i lovens formålsparagraf. Europarådets konvensjon 108 om personvern tar i artikkel 1 utgangspunkt i en ideell rettighet («right to privacy») og i konvensjonens innledende avsnitt heter det at retten til beskyttelse av privatlivet i en tid der automatisert databehandling spiller en viktig rolle må betraktes på linje med menneskerettighetene og de grunnleggende friheter. Det må derfor være systematisk naturlig og innlede et regelverk, som i det vesentlige omhandler forpliktende krav til den eller de som skal bruke personopplysninger, med å fastslå den rett som utløser plikt. Utviklingen viser at nye muligheter for å registrere viten om, eller et grunnlag for å trekke slutninger om en person eller en gruppe gjennom registrering av adferd, innebærer nye personverntrussler lovgiver bør forholde seg til. Samtidig bør det slås fast at opplysninger eller for eksempel et biologisk materiale som avgis eller samles for et spesielt formål, ikke kan benyttes for andre formål uten samtykke eller annen, lovlig hjemmel. Etter dette medlems mening innebærer den raske og omfattende, nøyaktige innsikt i genetiske sammenhenger at det i fremtiden bør vises større tilbakeholdenhet ved bruk av personopplysninger om avdøde i forhold til tidligere lovgivning. Under henvisning til overstående, foreslår dette medlemmet slik formulering av loven § 1:

Denne lovens hensikt er å sikre at personopplysninger, knyttet til den enkeltes private livsområde, blir innhentet, bearbeidet, oppbevart og benyttet på grunnlag av samtykke, lovhjemmel eller rettslig beslutning. De samme krav stilles til registrering av adferd.

Den enkeltes ukrenkelighet skal respekteres både i privatliv, arbeidsliv og i offentlige sammenhenger.

Enhver har i utgangspunktet råderett over kunnskap denne gir fra seg om seg selv. Opplysninger, eller et materiale som gir grunnlag for opplysninger, skal bare benyttes til det eller de oppgitte formål de innhentes eller samles for.

Unntak skal være hjemlet i lov.

Lovens regler omfatter fysiske personer. De kommer også til anvendelse hvis opplysninger om døde eller juridiske personer kan knyttes til individ eller slekt og opplysningene må antas å være følsomme.

Formannen og utvalgets øvrige medlemmer viser til Apenes forslag og vil peke på at det i utvalget er enighet om mange av de synspunktene som kommer frem i forslaget. Disse medlemmene mener imidlertid at disse synspunktene er ivaretatt i utvalgets forslag til lovens øvrige bestemmelser og at det ikke er hensiktsmessig med en formålsparagraf med materielle regler (regler som direkte gir uttrykk for hvorledes personopplysninger skal eller kan behandles).

§ 2 Definisjoner

1. Med «personopplysning» menes opplysninger og vurderinger som direkte eller indirekte kan knyttes til en identifiserbar, fysisk person (den registrerte).
2. Med «behandling av personopplysninger» menes enhver operasjon eller serie av operasjoner som utføres på personopplysninger, som for eksempel innsamling og registrering herunder elektronisk overvåkning, systematisering, oppbevaring, endring, søking, utlevering, sammenstilling, blokkering og sletting.
3. Med «personregister» menes registre, fortegnelser mm der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen.

4. Med «behandlingsansvarlig» menes den som bestemmer formålet med en elektronisk behandling eller formålet med et manuelt personregister, samt hvilke operasjoner som skal eller kan utføres på personopplysninger.
5. Med «databehandler» menes den som i henhold til avtale behandler personopplysninger på vegne av den behandlingsansvarlige.
6. Med «elektronisk overvåkning» menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende utstyr.
7. Med «samtykke» menes en uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar at opplysninger om en selv blir behandlet.
8. Med «sensitive personopplysninger» menes personopplysninger om
 - a) rasemessig eller etnisk bakgrunn, eller politisk eller religiøs oppfatning
 - b) at en person har vært mistenkt, siktet, tiltalt eller dømt for straffbare forhold
 - c) helseforhold, herunder opplysninger om arveegenskaper og misbruk av rusmidler
 - d) seksuelle forhold
 - e) medlemskap i fagforeninger.
9. Med «enkeltavgjørelse» menes
 - a) enkeltvedtak, jf forvaltningsloven § 2 bokstavene b) og a), og
 - b) andre avgjørelser som er bestemmende for bestemte private personers rettigheter eller plikter.

Til § 2

Legaldefinisjonene i § 2 er dels en videreføring av definisjonene i personregisterloven § 1, og dels basert på definisjonene i direktivet artikkel 2. De fleste av definisjonene har fått en noe annen utforming enn de tilsvarende definisjonene i direktivet, men innholdet i definisjonene ligger innenfor rammene av direktivets definisjoner.

Nr 1: «personopplysning»

Begrepet «personopplysning» er vidtrekkende, se "*Personopplysninger*" i avsnitt 10.1.1. Det omfatter opplysninger og vurderinger som direkte eller indirekte kan knyttes til identifiserbare fysiske personer. Det gjøres ingen endringer i personregisterlovens definisjon av begrepet.

Formålsbestemmelsen vil ha betydning ved tolkningen av begrepet «personopplysning». Det kan tenkes tilfeller hvor ordlyden i nr 1 isolert sett kan trekke i retning av at en opplysning er «personopplysning», men hvor personvern hensyn ikke kan begrunne at opplysningen vernes.

Lovforslaget omfatter bare opplysninger om *levende* personer. I de tilfellene de registrerte opplysningene om døde personer også gir opplysninger om gjenlevende personer (f eks opplysninger om arvelige sykdommer) vil dette være en personopplysning i lovens forstand, se 10.1.1.3.2.

Lovforslaget omfatter videre bare opplysninger om *fysiske* personer (se 10.1.1.3.1). Dette er en endring i forhold til personregisterloven som også omfatter opplysning om juridiske personer. Loven omfatter likevel opplysninger (om fysiske personer) som knytter seg til juridiske personer (f eks opplysninger om at en person er registrert som innehaver av en virksomhet). Avgjørende for om man skal anses som fysisk eller juridisk person er om man er tildelt organisasjonsnummer. Dette innebærer at de enkeltmannsforetak som er registreringspliktige etter foretaksregisterloven § 2-1, samt de enkeltmannsforetak som er registreringsberettigede etter samme lov § 2-2 og har benyttet seg av denne registreringsretten, vil være å anse

som juridiske personer. For enkeltmannsforetak som ikke har organisasjonsnummer vil det ikke skilles mellom foretaket og den bestemte fysiske personen som er innehaver av foretaket, loven vil omfatte opplysninger om begge disse.

Også opplysninger som for den behandlingsansvarlige fremstår som anonymiserte kan være «personopplysninger» i lovens forstand dersom det finnes referanser eller andre tilknytningspunkter som gjør indentifisering mulig. I SOU 1997: 39 nevnes som eksempel at en som leverer tjenester via Internett registrerer en anonym elektronisk identitet som bare kan knyttes til en identifiserbar enkeltperson dersom man har tilgang til opplysninger som vedkommendes Internettleverandør sitter inne med. Også etter den norske loven vil slike opplysninger kunne være «personopplysninger».

Uttrykket «den registrerte» betyr her «den opplysningene gjelder». «Den registrerte» benyttes også der det ikke foreligger noe personregister i tradisjonell forstand – opplysninger om den enkelte vil like fullt være «registrert» i betydningen innsamlet og oppbevart.

Nr 2: «behandling av personopplysninger»

Definisjonen av behandlingsbegrepet er den samme som i direktivet, se nærmere omtale av dette begrepet i "*Behandlingsbegrepet*" i avsnitt 10.1.2.2. Behandlingsbegrepet er vidt og omfatter enhver operasjon eller rekke av operasjoner – med eller uten bruk av edb – som personopplysninger gjøres til gjenstand for. Det er ikke alle former for behandling av personopplysninger som omfattes av loven. I loven knyttes behandlingsbegrepet enten til elektronisk behandling av personopplysninger eller til manuell behandling hvor personopplysningene inngår eller skal inngå i et personregister. Loven regulerer for eksempel ikke manuell behandling av personopplysninger når personopplysningene ikke skal inngå i et personregister, herunder visse former for manuell saksbehandling.

Bestemmelsen gir eksempler på operasjoner som er behandling av personopplysninger. Andre eksempler som uttrykkelig nevnes i direktivet, men som av lovtekniske hensyn ikke er tatt inn i lovteksten, er bl a «tilpasning», «seleksjon», «bruk», «sammenkjøring» og «tilintetgjørelse». For ordens skyld understrekes det at eksemplene som ikke er tatt inn i lovteksten også omfattes av lovens generelle behandlingsbegrep, og det er ingen realitetsforskjell i forhold til direktivet artikkel 2 bokstav b.

Loven har ikke identiske regler for alle former for behandling. For eksempel er informasjonsplikten etter § 20 knyttet til *innsamling* av personopplysninger, rettings- og slettingsplikten etter § 25 er knyttet til *registrering* av personopplysninger og konsesjonsplikten etter § 33 avhenger av *formålet* med behandlingen.

Nr 3: «personregister»

Personregisterbegrepet opprettholdes som avgrensningskriterium for manuell behandling av personopplysninger, slik at manuell behandling av personopplysninger som inngår eller skal inngå i et personregister omfattes av loven. Det foreslås ingen endringer i personregisterlovens definisjon av «personregister».

Nr 4: «behandlingsansvarlig»

Den som har bestemmelsesrett over opplysningene og den elektroniske behandlingen av disse er behandlingsansvarlig. Også den som bestemmer formålet med manuelle personregistre vil være behandlingsansvarlig.

Selv om man setter arbeidet bort til andre («outsourcing»), vil man selv sitte med bestemmelsesretten – og dermed også ansvaret. De som eventuelt utfører et avtalt arbeid for den behandlingsansvarlige, vil være databehandlere, jf nedenfor (nr 5). Den behandlingsansvarlige er pålagt en rekke plikter etter loven. Dersom det foretas behandling av personopplysninger, vil det også finnes en behandlingsansvarlig.

I utgangspunktet er det bare subjekter som har partsevne som kan være behandlingsansvarlig. Med partsevne menes her det å kunne bli saksøkt under en prosess for domstolene. Fysiske personer og de fleste juridiske personer vil ha partsevne slik uttrykket nyttes her. For at en sammenslutning skal ha partsevne må det imidlertid foreligge en viss form for organisasjon, se nærmere Hov, Rettergang i sivile saker, 2 utg 1994 s 210 flg. Kravet til partsevne er bl a begrunnet i at det kan være nødvendig å bruke rettsapparatet for å gjennomføre krav mot den behandlingsansvarlige.

I en rekke tilfeller vil det være fastsatt i lov hva som er formålet med behandlingen og hvilke operasjoner som skal eller kan utføres på personopplysningene. De aktuelle lovene vil imidlertid ikke uttømmende regulere disse spørsmålene, men i varierende grad overlate til offentlige eller private rettssubjekter å nærmere bestemme hvilke operasjoner som kan eller skal utføres på opplysningene. Også i disse tilfellene følger det av nr 4 hvem som er behandlingsansvarlig. Et konkret eksempel belyser poenget. Lov om offisiell statistikk og Statistisk Sentralbyrå 16 juni 1989 nr 54 bestemmer i § 3-1 hvilke oppgaver Statistisk Sentralbyrå skal vareta, men fastsetter ikke i detalj hvorledes opplysningene skal behandles for at disse oppgavene skal oppfylles. Slike valg – slik bestemmelsesrett – er (i den grad noe annet ikke følger av lov eller forskrift) overlatt til byrået selv. Statistisk Sentralbyrå er med andre ord behandlingsansvarlig.

I særlovgivning kan det være hensiktsmessig å uttrykkelig bestemme hvem som er behandlingsansvarlig (noe personverndirektivet tillater).

Den behandlingsansvarlige vil ofte være en juridisk person. Dette reiser spørsmål om intern fordeling av ansvar for at loven etterlevs. Det formelle ansvaret for at pliktene som den behandlingsansvarlige pålegges oppfylles ligger hos ledelsen i den aktuelle virksomheten. Virksomheten skal imidlertid knytte gjennomføringen av pliktene som den behandlingsansvarlige pålegges til en stilling eller en fysisk person i virksomheten, jf forutsetningsvis lovforslaget § 16 nr 2. Funksjonen bør være knyttet til en bestemt stilling innen virksomheten slik at ansvarsforholdet er klart selv om enkeltpersoner i virksomheten skifter jobb, slutter etc. Funksjonen bør legges til en lederstilling knyttet til behandlingen av personopplysninger slik at stillingsinnehaveren har reell daglig innflytelse på de behandlingene som foretas (f eks daglig leder, eventuelt daglig leder i administrasjonsavdelingen). I en del lovgivning vil det av loven selv fremgå hvem det er naturlig at pliktene påhviler.

Dersom den behandlingsansvarlige går konkurs, vil konkursboet være behandlingsansvarlig.

Nr 5: «databehandler»

Databehandler er den som i henhold til avtale behandler personopplysninger på vegne av den behandlingsansvarlige, se 13.4.2. Databehandlerens rådighet over personopplysninger er regulert i lovforslaget § 13.

Begrepet «databehandler» er langt videre enn begrepet «databehandlingsforetak» etter personregisterloven. Det er tilstrekkelig at noen *behandler* personopplysninger på vegne av den behandlingsansvarlige, dvs for eksempel oppbevarer

opplysninger. Det innebærer at en reparatør av datamaskinutstyr normalt vil måtte anses som en databehandler dersom vedkommende samtidig oppbevarer personopplysningene eller på annen måte har tilgang til dem på vegne av den behandlingsansvarlige. Det er altså ikke noe krav slik personregisterloven oppstiller i dag, at det må skje en bearbeiding av personopplysningene.

Behandlingen må skje *på vegne av* den behandlingsansvarlige. Det må altså skje etter ønske fra den behandlingsansvarlige, og det må skje i henhold til *avtale*. Det er ingen formkrav til avtalen, men det kan være hensiktsmessig at slike avtaler som regel inngås skriftlig.

Nr 6: «fjernsynsovervåkning»

Definisjonen av fjernsynsovervåkning er en videreføring av personregisterlovens definisjon av fjernsynsovervåkning, se "[Fjernsynsovervåkning og annen elektronisk overvåkning](#)" i kapittel 14.

Nr 7: «samtykke»

Definisjonen av «samtykke» er ny i forhold til personregisterloven, og bygger på direktivet artikkel 2 bokstav h). For at det overhodet skal foreligge et samtykke må erklæringen være frivillig. Dette anses for å være selvfølgelig, og er ikke uttrykkelig sagt i lovteksten.

Det stilles imidlertid flere krav til erklæringen for at denne skal være «samtykke» i lovens forstand. For det første må erklæringen være «uttrykkelig». Det holder ikke med et passivt eller stilltiende samtykke, og heller ikke samtykke gjennom såkalt konkludent atferd er tilstrekkelig.

For det andre må erklæringen være «informert». I dette ligger at den registrerte må forstå hva erklæringen gjelder, og hvilke konsekvenser denne får eller kan få. Endelig må samtykket være individuelt (jf uttrykket «den registrerte»), dvs at den enkelte registrerte selv (eller ved en fullmektig) må ha avgitt erklæringen. Et «kollektivt» samtykke, f eks slik at en organisasjon samtykker på vegne av alle medlemmene, vil i utgangspunktet ikke tilfredsstillere kravet med mindre omstendighetene rundt innmeldingen i organisasjonen gjør at innmeldingen i seg selv tilfredsstiller kravet til samtykke (dvs slik at det tydelig fremgår at innmelding medfører behandling av personopplysninger, og innmeldingserklæringen er informert).

Nr 8: «Sensitive personopplysninger»

Bestemmelsen forklarer hva som i denne loven anses som sensitive personopplysninger. Bestemmelsen lovfester sammen med § 9 regelen i direktivet artikkel 8 nr 1. Definisjonen har også betydning i forhold til bestemmelsen om konsesjonsplikt i § 33. Det foreslås enkelte endringer i forhold til det som personregisterloven regner som sensitive personopplysninger (jf personregisterloven § 6 annet ledd).

I en konkret situasjon kan det ikke utelukkes at også andre typer personopplysninger enn de som oppregnes i direktivet (og som danner grunnlag for lovens definisjoner) kan oppleves som sensitive, f eks opplysninger om private økonomiske forhold. At også slike opplysninger kan oppleves som følsomme kan det tas hensyn til ved praktiseringen av loven selv om de ikke defineres som sensitive. Eksempelvis kan det i forbindelse med relevans- og saklighetsvurderingen etter § 7 tas i betraktning hvor følsomme opplysningene oppleves for den enkelte.

Angivelsen av de sensitive personopplysningene har fått en noe annen utforming enn de tilsvarende beskrivelsene i direktivet, men innholdet er det samme.

I tillegg er opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for et straffbart forhold, ansett som sensitive etter loven. Ved en lovendring i 1987 ble den parallelle oppregningen i personregisterloven §§ 7 og 9 utvidet, slik at det ikke lenger var nødvendig at det var innledet noen straffesak. Dette førte bl a til at f eks et vaktsselskaps register over personer som blir pågrepet med ubetalte varer, ble omfattet av oppregningen (jf Ot prp nr 34 (1986-87) s 24 h spalte). Utvalgets forslag viderefører denne bestemmelsen.

Endringene i forhold til personregisterlovens oppregning i § 6 annet ledd er for det første at opplysning om medlemskap i fagforeninger etter loven nå er ansett som sensitivt (se nærmere nedenfor). For det andre er «andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde» (personregisterloven § 6 annet ledd nr 5) ikke lenger med som særskilt punkt i oppregningen. Endelig er det foretatt visse presiseringer av ordlyden i enkelte punkter.

Opplysning om medlemskap i fagforening er i Norge tradisjonelt ikke oppfattet som en sensitiv personopplysning. Det kan derfor være noe fremmed at slike opplysninger bare skal kunne behandles dersom nærmere bestemte vilkår er oppfylt. Det antas imidlertid at unntakene i § 9 vil dekke de tilfellene hvor slik behandling er ønskelig eller nødvendig. Med hjemmel i § 9 kan det behandles opplysninger om medlemskap i fagforeninger dersom den registrerte uttrykkelig samtykker, behandlingen er fastsatt i lov eller den behandlingsansvarlige er forpliktet til å foreta behandlingen i henhold til avtale mellom partene i arbeidslivet.

Arbeidsgiver plikter etter ligningsloven § 6-2 nr 3 å oppgi til ligningsmyndighetene fradragsberettiget fagforeningskontingent dersom det er gjennomført fradrag for dette i lønnsutbetalingene eller dersom lønnstakeren legitimerer å ha betalt direkte til sin fagforening. Dersom den ansatte ikke ønsker at arbeidsgiveren skal kjenne til at han eller hun er medlem i en fagforening og fagforeningskontingenten derfor betales direkte til fagforeningen, forutsetter fagforeningens videregivelse av disse opplysningene til ligningsmyndighetene samtykke fra den opplysningen gjelder. Samtykket må være uttrykkelig, informert og frivillig, jf ovenfor.

Personregisterloven § 6 annet ledd nr 5 (opplysninger om familieforhold) er ikke tatt med i den nye oppregningen av sensitive opplysninger. Dette er ikke ment å medføre materielle endringer. Den nåværende beskrivelsen i nr 5 er uklar og det er vanskelig å se hvilke opplysninger som er ment omfattet av bestemmelsen. Utvalget legger til grunn at de opplysningene den først og fremst vil være aktuell for også vil omfattes av lovens oppregning i bokstav c) (opplysninger om helseforhold). Dette gjelder blant annet en rekke opplysninger om ulike sosiale forhold.

Opplysning om «rase» er endret til opplysning om «rasemessig eller etnisk bakgrunn» uten at dette er ment å medføre noen realitetsendringer. Utvalget mener imidlertid den nye ordlyden bedre dekker dagens praksis som man ønsker å videreføre. I b) er «siktet» tilføyd. Begrepet omfattes på samme måte som «tiltalt» av det videre begrepet «mistenkt», men utvalget finner det hensiktsmessig at også dette nevnes særskilt.

Opplysninger om helseforhold er presisert slik at det klarere enn i dag fremgår at dette også omfatter opplysninger om arveegenskaper og misbruk av rusmidler. Det er mange forskjellige typer opplysninger som omfattes av c) (helseforhold). I tillegg til opplysninger om forskjellige fysiske mangler eller lidelser omfattes opplysninger om psykiske lidelser, sosial tilpasningsevne, omsorgsevne mv. Opplysninger om sosiale forhold mer generelt vil regnes som helseforhold i lovens forstand dersom forholdene i hht forebyggende helsearbeid kan medføre helseproblemer, eller dersom forholdene faktisk medfører slik problemer. Enhver påstand om

en slik sammenheng er imidlertid ikke tilstrekkelig, det må vurderes konkret hvor sannsynlig det er at de aktuelle sosiale forholdene har helsemessig betydning.

«Politisk» i a) omfatter opplysninger om oppfatninger og synspunkter utover ren partipolitisk tilhørighet. Direktivet nevner både politisk og filosofisk overbevisning, og utvalget legger til grunn at begge disse beskrivelsene omfattes av «politisk eller religiøs oppfatning». Det vil imidlertid være å strekke det for langt å si at medlemsskap i interesseorganisasjoner generelt gir uttrykk for en *politisk* oppfatning. Dette må avgjøres konkret.

Dersom en organisasjon anses å være enten politisk eller religiøs, vil medlemsskap uten videre måtte anses for å gi uttrykk for en *oppfatning*. Dette gjelder selv om noen medlemmer kan tenkes å ha andre grunner for å være medlem enn at de sympatiserer med organisasjonens synspunkter. For eksempel vil medlemsskap i statskirken måtte anses som en opplysning om religiøs oppfatning.

I § 2 nr 9 forklares hva som menes med «enkeltavgjørelse». Begrepet brukes flere steder i loven, se f eks § 22 om rett til å kreve begrunnelse for visse fullstendig automatiserte avgjørelser, og § 33 om avgrensningen av konsesjonsplikten. Med enkeltavgjørelse menes for det første «enkeltvedtak» slik dette defineres i forvaltningsloven § 2 første ledd bokstavene a og b. Dette betyr at

- a) det må være en *avgjørelse*,
- b) den må gjelde rettsstillingen for «*private personer* (enkeltpersoner eller andre private rettssubjekter),
- c) avgjørelsen må gjelde dissers «*rettigheter eller plikter*»,
- d) avgjørelsen må være truffet under «*utøving av offentlig myndighet*», og
- e) enkeltvedtaket må gjelde «en eller flere *bestemte*» personer.

Begrepet «enkeltavgjørelser» omfatter også andre avgjørelser (enn enkeltvedtak) som er bestemmende for bestemte private persons rettigheter og plikter, jf første ledd nr 2. Forskjellen til nr 1 er at avgjørelsen ikke treffes som ledd i offentlig myndighetsutøvelse, og alternativet vil følgelig omfatte avgjørelser som treffes i privat sektor. De øvrige vilkårene nevnt i a, b, c og e ovenfor vil imidlertid gjelde også for disse avgjørelsene. Det beslutningsfokuserede personvernet tillegges på denne måten like stor vekt for offentlige som for private behandlingsansvarlige. Grunnlaget for å treffe avgjørelsene kan være f eks lov, avtale eller eiendomsrett. Det sentrale er at det treffes en bestemt type avgjørelse som gjennomgående er av stor betydning for den registrerte.

Rettskildefaktorer som belyser relevante deler av enkeltvedtaksbegrepet (jf vilkårene a, b, c og e) vil gi veiledning også om hvorledes «enkeltavgjørelse» skal forstås. Nedenfor knyttes noen kommentarer til de enkelte vilkårene.

Det følger av nr 2 at formålet med behandlingen må være å treffe en «*avgjørelse*». Uttalelser, forslag og lignende vil ikke være noen slik avgjørelse.

Videre må avgjørelsen være bestemmende for rettsstillingen til «*private personer*». Begrepet omfatter i motsetning til begrepet i forvaltningsloven § 2 a), bare fysiske personer. Andre private rettssubjekter (som for eksempel selskaper og foreninger) omfattes ikke. Offentlige organer eller offentlig eide rettssubjekter omfattes heller ikke.

Avgjørelsen må være «*bestemmende*» for vedkommendes rettsstilling på samme måte som enkeltvedtak etter forvaltningsloven. Det vil derfor også etter nr 2 være realitetsavgjørelser – i motsetning til prosessledende beslutninger – som omfattes. At det nektes innsyn i personopplysninger eller at personopplysninger nektes slettet etter ønske fra den registrerte, vil for eksempel ikke være en avgjørelse som er «bestemmende» for noens rettsstilling.

§ 3 Lovens saklige virkeområde

Loven gjelder for helt eller delvis elektronisk behandling av personopplysninger og for manuell behandling når personopplysningene inngår eller skal inngå i et personregister.

Loven gjelder ikke behandling av personopplysninger for rent personlige formål.

Kongen kan gi forskrift om at loven eller deler av denne ikke skal gjelde for bestemte former for elektronisk behandling av personopplysninger.

Til § 3:

Bestemmelsen gjelder lovens saklige virkeområde og bygger på direktivet artikkel 3. Det foreslås endringer i forhold til personregisterlovens saklige virkeområde som er regulert i personregisterloven § 1, se utvalgets vurderinger i "[Lovens saklige og geografiske virkeområde](#)" i kapittel 10.

Loven gjelder for all elektronisk behandling av personopplysninger, samt for manuell behandling når opplysningene inngår eller skal inngå i et personregister. Dette innebærer at personregisterbegrepet forlates som et hovedbegrep, og at registerbegrepet heretter først og fremst får betydning for manuell behandling av personopplysninger hvor det opprettholdes som et avgrensningskriterium, se 4.3 og utvalgets vurderinger under 10.1.2.1. Det forhold at behandlingen av personopplysningene enten må være elektronisk eller nedfelle seg i et manuelt personregister angir det saklige virkeområde til alle bestemmelsene i loven. Det forhold at enkelte bestemmelser for enkelhets skyld taler om «behandling av personopplysninger» innebærer ikke noen utvidelse av det saklige virkeområde som angitt i § 3.

Delvis elektronisk behandling likestilles med fullstendig elektronisk behandling, f eks slik at behandlingen skjer dels manuelt og dels ved elektroniske hjelpemidler.

Det er nødvendig å trekke en grense mellom manuell behandling og helt eller delvis elektronisk behandling. Direktivet gir meget begrenset veiledning om hvordan grensen skal trekkes. Dersom personopplysningene i sin helhet lagres eller bearbeides i maskinlesbar form, er behandlingen utvilsomt elektronisk. I noen tilfeller vil deler av opplysningene lagres i maskinlesbar form, mens andre deler lagres manuelt (f eks elektronisk journal kombinert med papirarkiv). Spørsmålet blir hva som skal til for at alle opplysningene (også de som er lagret på papir) skal omfattes av reglene om elektronisk behandling. Det betyr at den elektroniske delen av behandlingen må omfatte personopplysninger for at reglene om elektronisk behandling skal komme til anvendelse. Dersom man ikke kan bruke elektroniske hjelpemidler til å søke seg frem til personopplysninger som finnes i papirdokumenter, er behandlingen manuell og ikke delvis elektronisk.

Vanskelige avgrensningsspørsmål reiser seg også blant annet i forbindelse med lyd og billedopptak som lagres ved analoge lagringsmidler, se 10.1.2.3.

Personregisterloven gjelder for «personregistre og bruk av personopplysninger i organ for stat eller kommune og i privat næringsvirksomhet, foreninger eller stiftelser». Denne regelen videreføres, men det er nødvendig å presisere ordlyden slik at det bedre går frem at det bare er behandling av personopplysninger til rent personlige formål som ikke er omfattet, jf *annet ledd*. Ulike former for privat virksomhet er omfattet selv om de ikke kan anses for å drive næringsvirksomhet (for eksempel forskning). Dette er i tråd med praktiseringen av personregisterloven i dag.

Tredje ledd gir Kongen hjemmel til å bestemme i forskrift at loven ikke skal få anvendelse på bestemte former for behandling av personopplysninger. Forskriftshjemmelen må benyttes slik at eventuelle unntak er forenlige med direktivet. I

direktivet artikkel 3 nr 2 presiseres sakområder som direktivet ikke får anvendelse på, og som dermed kan unntas fra lovens anvendelsesområde i medhold av § 3 tredje ledd. Et eksempel på dette er ulike strafferegistre. Slike registre er i dag unntatt fra konsesjonsplikt i medhold av personregisterloven § 41, jf lov 11 juni 1971 nr 52 om strafferegistrering, mens personregisterloven for øvrig i utgangspunktet får anvendelse med mindre det er gjort unntak i forskrift. Lovforslaget her vil i utgangspunktet få anvendelse også på statens behandling av personopplysninger på det strafferettslige området, herunder strafferegistrene, men tredje ledd gir hjemmel til å bestemme at slik behandling av personopplysninger helt eller delvis skal unntas fra lovens anvendelsesområde. Selv om særlige hensyn gjør seg gjeldende på dette området, bør deler av loven få anvendelse, som f eks § 6 om krav til saklighet.

§ 4 Fjernsynsovervåkning og billedopptak

For fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning som ikke er elektronisk behandling av personopplysninger gjelder §§ 7, 24, 40, 41 og § 42 nr 6 tilsvarende.

For billedopptak i forbindelse med fjernsynsovervåkning som ikke er elektronisk behandling gjelder også §§ 31, 32 og 38 tilsvarende.

Med fjernsynsovervåkning menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller lignende apparat.

Til § 4:

Fjernsynsovervåkning og billedopptak er bare elektronisk behandling av personopplysninger dersom det finnes opptak som er søkbare. Ettersom utvalget har kommet til at også visse andre former for overvåkning gjør det ønskelig å stille noen krav til overvåkningen (jf "[Fjernsynsovervåkning og annen elektronisk overvåkning](#)" i kapittel 14), fremgår det uttrykkelig at bestemmelsene om krav til saklig formål m v i § 7, om varsling i § 24 og Datatilsynets mulighet til å gi pålegg etter § 40 og tvangsmulkt etter § 41 også får anvendelse på fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning. Henvisningen til at § 42 gjelder så langt den passer medfører at overtredelse av Datatilsynets pålegg i medhold av § 40 er straffbar også her. For billedopptak får i tillegg reglene om meldeplikt og Datatilsynets tilgang til informasjon anvendelse. Sett under ett fører dette til at denne typen overvåkning blir undergitt strengere kontroll enn i dag, for eksempel vil Datatilsynet i motsetning til idag kunne gi pålegg om at overvåkning i strid med loven skal opphøre. Dette innebærer bl a at det er Datatilsynet, og ikke den som overvåker, som avgjør om formålet med overvåkningen er saklig.

§ 5 Forholdet til ytringsfriheten

Loven gjelder for behandling av personopplysninger som utelukkende finner sted i journalistisk øyemed eller for kunsterisk eller litterær virksomhet. Det skal gjøres unntak fra bestemmelsene i den grad det er nødvendig for å forene hensynet til ytringsfrihet med hensynet til personvern.

Til § 5:

Bestemmelsen gjennomfører direktivet artikkel 9. Forholdet til ytringsfriheten er behandlet i "[Forholdet til ytringsfriheten](#)" i kapittel 17 foran. I 17.5 gis eksempler

på vurderinger av om loven er uforenlig med ytringsfriheten, slik at loven ikke får anvendelse. Denne vurderingen må foretas for hver enkelt bestemmelse.

Med ytringsfrihet menes ikke bare overordnede normer som Grunnloven § 100 og EMK artikkel 8 og 10, men også hensynet til ytringsfrihet mer generelt. Det skal foretas en avveining av personvern mot ytringsfrihet slik at det kan finnes frem til en rimelig balanse.

§ 6 Lovens geografiske virkeområde

Loven gjelder for behandling av personopplysninger når den behandlingsansvarlige er etablert i riket, herunder Svalbard og Jan Mayen.

Loven gjelder også for behandling av personopplysninger som skjer i riket og som forestås av en behandlingsansvarlig som er etablert i stater utenfor EØS-området dersom den behandlingsansvarlige benytter hjelpemidler i Norge. Den behandlingsansvarlige skal i så fall utpeke en representant som er etablert i Norge. Reglene om den behandlingsansvarlige gjelder tilsvarende for representanten.

Annet ledd gjelder ikke dersom hjelpemidlene utelukkende benyttes til å transportere personopplysninger via Norge.

Til § 6:

Den norske loven skal gjelde for behandlingsansvarlige som er etablert i Norge, og for enkelte andre behandlingsansvarlige. Dette utdypes nedenfor. Paragraf 6 bygger på direktivet artikkel 4 (jf fortalen pkt 18 – 21).

Hovedregelen er at den norske loven får anvendelse når den behandlingsansvarlige er etablert i Norge, se *første ledd*. Loven får anvendelse på Svalbard og Jan Mayen, se nærmere 10.2.

Med «etablert» menes at det faktisk utøves aktiviteter innenfor en forholdsvis fast struktur, se direktivets fortale pkt 19. Strukturens rettslige status er ikke i seg selv avgjørende for om den behandlingsansvarlige er etablert i Norge. Dette beror på en helhetsvurdering, hvor det sentrale vurderingstemaet blir om behandlingen som finner sted i Norge er så omfattende og så permanent at den norske loven bør få anvendelse. Dersom et utenlandsk selskap har et datterselskap i Norge, vil datterselskapet anses for å være «etablert i Norge» i lovens forstand. Det samme gjelder utenlandske selskapers filialer i Norge. En utenlandsk handelsreisende som er på forretningsreise i Norge og i den anledning behandler personopplysninger vil derimot ikke være «etablert» slik loven nytter uttrykket.

En behandlingsansvarlig som utelukkende er etablert i Norge, vil bare reguleres av den norske loven, selv om enkelte ledd i behandlingen – f eks innsamling av opplysninger – finner sted i et annet EØS-land. Et eksempel på dette kan være at en behandlingsansvarlig som er etablert i Norge foretar visse former for behandling av personopplysninger i Danmark (f eks innsamling av personopplysninger). Dersom tilsynsmyndigheten i Danmark ønsker å stoppe eller sette vilkår for behandlingen, må dette vurderes ut i fra den norske loven. På tilsvarende måte kan den norske tilsynsmyndigheten måtte anvende den danske loven på behandling av personopplysninger som finner sted i Norge og som foretas av en virksomhet som utelukkende er etablert i Danmark.

Det er ikke noe til hinder for at en behandlingsansvarlig kan anses å være etablert i flere EØS-land samtidig. Hvis for eksempel et multinasjonalt konsern behandler personopplysninger både i Norge, England og Frankrike, og er etablert i alle landene, vil behandlingen av personopplysningene i de ulike landene reguleres av hhv den norske, engelske og franske loven. Det fremgår uttrykkelig av artikkel 4 nr

1 bokstav a) at den behandlingsansvarlige plikter å sørge for at den nasjonale lovgivningen i de respektive etableringsland respekteres.

Annet ledd gjør unntak fra hovedregelen i første ledd ved at den norske loven kan få anvendelse på virksomheten til en behandlingsansvarlig som ikke er etablert i Norge. Bestemmelsen regulerer de tilfellene der en behandlingsansvarlig som er etablert utenfor EØS-området, f eks i Russland, behandler personopplysninger med hjelpemidler som befinner seg i f eks Tromsø. Den norske loven vil da få anvendelse på virksomheten i Norge.

Med hjelpemidler forstås utstyr og fysiske innretninger som benyttes til å behandle personopplysninger. Eksempler på slike hjelpemidler er datamaskiner- og terminaler, telenett og intervju skjemaer. Det sentrale er at hjelpemidlene geografisk befinner seg i Norge slik at de skaper en tilknytning mellom den behandlingsansvarlige og Norge.

Den behandlingsansvarlige som omfattes av bestemmelsen i annet ledd første punktum skal utpeke en representant som er etablert i Norge. Bakgrunnen for dette er at lovens reguleringssystem forutsetter en reell mulighet for kontakt mellom Datatilsynet og den behandlingsansvarlige, noe som ikke så lett lar seg oppfylle uten en representant for den utenlandske behandlingsansvarlige. Representanten likestilles med den behandlingsansvarlige i forhold til loven. Når representanten uttrykkelig nevnes i enkelte bestemmelser, er dette utelukkende begrunnet i lovtekniske hensyn. Datatilsynet vil få informasjon om hvem som er utpekt som representant gjennom meldingen som den behandlingsansvarlige skal sende inn.

Bestemmelsen gjelder ikke der hjelpemidlene utelukkende gjør det mulig å transportere personopplysninger fra ett tredjeland til et annet via Norge, se *tredje ledd*.

"Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte" i Kapittel 2 Alminnelige regler om behandling av personopplysninger

7 Krav til saklighet

Personopplysninger kan bare behandles til lovlige og uttrykkelig angitte formål. Formålet skal være saklig begrunnet ut fra den behandlingsansvarliges virksomhet.

Personopplysningene skal være relevante ut fra det angitte formålet.

Elektronisk overvåkning av sted hvor en begrenset krets av personer jevnlig ferdes, er bare tillatt dersom det ut fra hensynet til virksomheten er et særskilt behov for overvåkingen.

Til § 7:

Bestemmelsen stiller krav til lovlige og saklige formål for elektronisk behandling av personopplysninger (jf første ledd) og for manuell behandling når personopplysningene inngår eller skal inngå i et personregister, jf siste ledd. Bestemmelsen er til dels en videreføring av personregisterloven § 6 første ledd og § 37a første ledd. *Første ledd* første punktum lovfester direktivet artikkel 6 b, og hele bestemmelsen uttrykker prinsippene i direktivet artikkel 7.

Personopplysninger skal bare behandles til lovlige og uttrykkelig angitte formål, jf første ledd. Formålet fastsettes av den behandlingsansvarlige. For de melde- og konsesjonspliktige behandlingene vil formålet fremgå av det innsendte meldeskjemaet eller konsesjonssøknaden. For «frie behandlinger», dvs behandlinger som verken er konsesjons- eller meldepliktige, skal den behandlingsansvarliges angivelse av formålet fremgå av oppregningen som nevnt i § 16.

Angivelsen av formålet vil ha betydning for hva opplysningene kan brukes til, jf § 8. Det vil derfor være viktig for de behandlingsansvarlige å tenke nøye gjennom hvilket formål de har med behandlingen. Samtidig kan det ikke aksepteres at formålsangivelsen er så vid at den kan dekke det meste; for at det skal være et «uttrykkelig angitt formål» i lovens forstand kreves en rimelig grad av presisjon i formålsangivelsen. Hvor presis angivelsen skal være må vurderes bl a på bakgrunn av begrunnelsen for regelen. Etter lovforslaget § 32 annet ledd kan Kongen gi forskrift om hvilke opplysninger meldingene skal inneholde. Sett fra et personvernssynspunkt er det viktig at behandling av personopplysninger skjer ut i fra et definert formål. Jo mer sensitive opplysningene er, og jo større konsekvenser bruken av opplysningene kan få, desto viktigere er en klar avgrensning av formålet. Når den hvis personopplysningene gjelder kjenner formålet, kan vedkommende bistå med korrekte opplysninger i den konkrete sammenhengen og lettere hevde sin interesse i personvern (for eksempel kreve opplysninger slettet etter § 26). Det er dessuten først når man kjenner formålet med behandlingen at det er mulig å vurdere hvilke opplysninger som er relevante, jf annet ledd. Beskrivelsen av personopplysningene kan dessuten variere avhengig av hvilken sammenheng de skal benyttes i.

Formålet skal være saklig begrunnet ut fra hensynet til administrasjon og virksomhet i det organ eller foretak som foretar behandlingen, jf første ledd annet punktum. Man kan på bakgrunn av denne regelen ikke starte en behandling med et hvilket som helst formål selv om det er uttrykkelig angitt. Regelen er mer generelt utformet enn direktivet artikkel 7 som har en uttømmende oppregning av når behandling av personopplysninger kan skje. Oppregningen i direktivet (bokstavene a) – f)) er veiledende for når formålet med behandlingen kan sies å være saklig begrunnet.

Kravet til lovlighet er ikke bare en henvisning til lovfestede regler, men også til ulovfestet personvern (jf dommen om «To mistenkelige personer» i Rt 1952 s 1217 som illustrerer at hensyn til personvern i visse tilfeller går foran andre interesser). Også formålsbestemmelsen vil ha betydning for om kravet til lovlighet er oppfylt.

Den behandlingsansvarlige står fritt til selv å definere sin virksomhet så lenge denne er lovlig. Det kan ikke utelukkes at det i fremtiden kan utvikle seg virksomhetsformer som fra et personvernssynspunkt er uønskede. Å begrense muligheten til å drive slik virksomhet eller gi adgang til å gripe inn og gi pålegg for å vareta personvernshensyn må eventuelt gjøres i særlovgivning som regulerer den aktuelle virksomhetsformen.

Relevanskravet i *annet ledd* viderefører personregisterloven § 6 første ledd som regulerer hvilke opplysninger som tillates registrert. Ordlyden er noe endret fordi det nå foreslås en egen regel om saklig formål i første ledd, men realiteten er den samme. I kravet til særskilt behov etter tredje ledd gjøres ingen endring i forhold til dagens regulering i personregisterloven. For utdypning av kravene etter annet og tredje ledd vises det til personregisterlovens forarbeider (se Ot prp nr 2 (1977-78) s 72 flg) og Datatilsynets praksis på området. Relevanskravet i personregisterloven § 6 første ledd skal etter personregisterloven ligge til grunn for konsesjonsvurderingen etter § 9. Det er derfor etablert omfattende praksis på området mht hva som er å anse som «saklig behov». Denne praksisen vil fortsatt være veiledende for avgjørelser etter den nye loven.

Datatilsynet kan med hjemmel i § 40 stoppe behandlinger som skjer i strid med bestemmelsen, for eksempel fordi formålet ikke er saklig begrunnet ut fra hensynet til administrasjon og virksomhet i foretaket eller fordi personopplysningene som behandles ikke er saklig i forhold til behandlingens formål. Det kan også pålegge den behandlingsansvarlige å definere formålet klarere dersom dette er påkrevet for å oppfylle lovens krav til tilstrekkelig presist angitt formål.

Tredje ledd regulerer spesielt elektronisk overvåkning. Det er en forutsetning at overvåkningen er elektronisk behandling av personopplysninger slik lovforslaget nytter uttrykket, jf merknadene til § 3 ovenfor. Dette omfatter bl a opptak som er digitalisert, dvs lagret i maskinlesbar form. Ettersom utvalget har kommet til at også visse andre former for overvåkning gjør det ønskelig å stille krav som i § 7, fremgår det uttrykkelig av § 4 at § 7 får anvendelse også på fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning.

§ 8 Anvendelse av personopplysninger til andre formål enn det opprinnelige

Personopplysninger som er samlet inn til behandling for et formål kan bare anvendes til andre formål dersom

1. den registrerte samtykker i det nye behandlingsformålet
2. det er fastsatt i lov at det er adgang til å bruke opplysningene til det nye behandlingsformålet, eller
3. fordelene med den nye behandlingen er klart større enn ulempene som den volder for den enkelte og den nye behandlingen ikke er uforenlig med det opprinnelige formålet.

Kongen kan gi forskrift om anvendelse av personopplysninger til nye formål.

Til § 8:

Bestemmelsen regulerer når personopplysninger samlet inn for ett formål kan benyttes til andre formål enn det opprinnelige. Det er en forutsetning at også nye formål er saklig begrunnet ut fra hensynet til administrasjon og virksomhet i det organ eller foretak som foretar behandlingen, jf kravene i § 7.

Hva som menes med samtykke er forklart i § 2 nr 7, mens offentlighetsloven og arkivloven er eksempel på at det i lov er fastsatt at personopplysninger kan nyttes til andre formål enn de opplysningene opprinnelig var innsamlet for.

Videre setter direktivet artikkel 6 nr 1 b) krav om at en senere behandling av personopplysninger ikke må være *uforenlig* med det opprinnelige angitte formålet. Denne regelen er gjenspeilet i § 8 første ledd nr 3 i lovforslaget. Hva som er uforenlig må avgjøres gjennom praksis og eventuelt i forskrift, se tredje ledd. Også formålsbestemmelsen kan gi veiledning.

Når det gjelder bruk til annet formål som har sitt grunnlag i lovhjemmel eller samtykke fra den registrerte, antas det ikke i tillegg å være behov for å uttrykkelig kreve en vurdering av hvorvidt det nye formålet er uforenlig med det opprinnelige. Hensynet må forventes å bli tilstrekkelig varetatt av lovgiver og den registrerte selv.

Nr 3 åpner for at opplysninger samlet inn til ett formål senere kan brukes til et annet selv om dette ikke er hjemlet i lov eller den registrerte ikke har samtykket. Loven krever i så fall at fordelene med den nye behandlingen er *vesentlig* større enn ulempene som den volder for den enkelte, og at den nye behandlingen ikke må være *uforenlig* med det opprinnelige formålet. Det må altså foretas en bred interesseavveining, hvor det kreves kvalifisert interesseovervekt for at opplysningene skal kunne brukes til et nytt formål. Fordelene med den nye behandlingen skal ikke bare omfatte fordelene for den enkelte registrerte, men også fordelene for den behandlingsansvarlige samt samfunnets interesser i at opplysningene kan benyttes til det nye formålet. Momenter i interesseavveiningen kan bl a være hvor forskjellig det nye formålet er fra det opprinnelige, om det nye formålet fordrer bedre opplysningskvalitet enn det opprinnelige, hvor følsomme opplysningene er, om den registrerte kan reservere seg mot enkelte typer bruk og eventuelt hvordan opplysningene er

bearbeidet. Det kan f eks være grunn til å bedømme enkeltstående opplysninger anderledes enn dyptgående beskrivelser av enkeltpersoner. Det må også tas med i avveiningen hva som vil bli resultatet dersom opplysningene må samles inn på nytt. Dersom slik innsamling ikke lenger er mulig, for eksempel fordi kildene ikke lenger er tilgjengelige, kan dette etter omstendighetene tale for å tillate endret formål. Også hensynet til opplysningskvalitet vil imidlertid stå sentralt.

Bruk av personopplysninger til forskning og statistikk anses normalt ikke for å være uforenlig med det opprinnelige formålet, jf direktivet artikkel 6 nr 1 b). Forskning og statistikk er også et område hvor man relativt lett vil komme til at fordelene med behandlingen er vesentlig større enn ulempene for den enkelte. Hensynet til den enkelte skal veies opp mot hensynet til samfunnet forøvrig. Jo mer sensitive opplysningene er, jo strengere blir kravet til vesentlighetsovervekt. Dersom det er planlagt tiltak som skal dempe ulempene for de registrerte, vil dette være av betydning ved vurderingen. Eksempler på slike tiltak kan være ulike sikkerhetsforanstaltninger, informasjon til de registrerte mv. I direktivets fortale pkt 29 fremheves det at tiltakene særlig skal ta sikte på å forhindre at opplysninger som er innsamlet til forskning eller den statistikk bruken blir benyttet til å treffe avgjørelser overfor den registrerte. I lov 16 juni 1989 nr 54 om offisiell statistikk og Statistisk Sentralbyrå er det i § 2-5 nr 1 uttrykkelig bestemt at opplysninger som er innhentet bare kan benyttes til utarbeidelse av offisiell statistikk eller til annen bruk som er godkjent av Datatilsynet og som ikke er til skade for rikets sikkerhet. For andre som driver med forskning eller statistikk kan mulige ulemper for den enkelte avhjelpest ved at de innsamlete opplysningene f eks krypteres eller ved at det foretas systematisk og umiddelbar anonymisering av personidentifiserbart materiale.

Det er vanskelig å sette opp klare grenser for når personopplysninger kan brukes til andre formål etter § 6 nr 3. Denne grensen må bli til gjennom praktiseringen av loven. Datatilsynet kan stoppe behandlinger som er i strid med bestemmelsen eller sette vilkår som minsker ulempene for de registrerte, jf § 40. Bruk av personopplysninger til nytt formål kan utløse krav om konsesjon eller plikt til å sende ny melding.

§ 9 Behandling av sensitive personopplysninger

Sensitive personopplysninger (jf § 2 nr 8) kan bare behandles dersom

1. den registrerte samtykker
2. det er fastsatt i lov at det er adgang til slik behandling
3. den behandlingsansvarlige plikter å foreta behandlingen i henhold til avtale mellom partene i arbeidslivet
4. behandlingen er nødvendig for å beskytte den registrertes eller en annen persons vesentlige interesser, og vedkommende selv ikke er i stand til å gi samtykke som nevnt i nr 1
5. behandlingen utføres av en ideell organisasjon som ledd i organisasjonens rettmessige virksomhet. Behandlingen kan kun omfatte opplysninger om organisasjonens medlemmer eller personer som på grunn av organisasjonens formål er i regelmessig kontakt med den. Personopplysningene kan ikke videreformidles uten den registrertes samtykke
6. behandlingen gjelder opplysninger som den registrerte selv har gjort alminnelig kjent
7. behandlingen er nødvendig for at et rettskrav kan fastsettes, gjøres gjeldende eller forsvares
8. behandlingen er nødvendig for medisinske formål eller for forvaltning av helsetjenester og opplysningene behandles av en helsearbeider med taushetsp-

likt

9. behandlingen er nødvendig for statistiske formål eller forskning og behandlingen ikke kan få direkte virkninger for den enkelte.

Datatilsynet kan bestemme at sensitive personopplysninger også i andre tilfeller kan behandles dersom viktige samfunnsinteresser tilsier det og det settes i verk tiltak for å sikre de registrertes interesser.

Til § 9:

Paragraf 9 begrenser mulighetene til å behandle sensitive personopplysninger elektronisk eller innta slike personopplysninger i et manuelt personregister. Hva som menes med «sensitive personopplysninger» fremgår av § 2 nr 8.

Adgangen til å behandle sensitive personopplysninger begrenses ved å oppstille en uttømmende oppregning av når slike opplysninger kan behandles. Bestemmelsen er en videreføring og utdyping av personregisterloven § 6 annet ledd som bestemmer at registrering av sensitive opplysninger bare kan skje dersom det er nødvendig (et styrket relevanskrav i forhold til personregisterloven § 6 første ledd). Lovforslaget bygger på direktivet artikkel 8 nr 2, 3 og 4.

Bestemmelsen inneholder nødvendige, men ikke alltid tilstrekkelige vilkår for å behandle sensitive personopplysninger. Dersom personopplysningene skal benyttes til å treffe visse former for kvalifiserte beslutninger, må det i tillegg søkes om konsesjon etter § 33.

Nr 1 fastslår at sensitive opplysninger kan behandles dersom den registrerte samtykker. Hva som menes med «samtykke» fremgår av lovforslaget § 2 nr 7, se merknadene ovenfor. Unntaket vil særlig være praktisk i forbindelse med inngåelsen av ulike former for avtaler, som f.eks. en forsikringsavtale. Muligheten til å samtykke gir den registrerte rådighet over personopplysninger om en selv, noe som anses som ønskelig ut fra personvern hensyn. Samtidig er det klart at visse former for behandling av personopplysninger er så viktige at det ikke kan overlates til den enkelte registrerte å bestemme om behandlingen skal kunne finne sted. Det er derfor behov for også andre vilkår for slik behandling, se nedenfor. Muligheten til å samtykke i at personopplysninger behandles gjelder ikke der det følger av lovgivningen at samtykke ikke er tilstrekkelig, jf. direktivet artikkel 8 nr 2 a). Under enhver omstendighet følger det av alminnelige trinnhøydeprinsipper at samtykke ikke kan oppheve lovforbud, og utvalget har ikke funnet det nødvendig å ta med dette i lovteksten.

Paragraf 9 nr 2 gjør det mulig å behandle sensitive personopplysninger dersom adgangen til dette er fastsatt i lov. Unntaket er basert på direktivet artikkel 8 nr 4. Om behandlingen har tilstrekkelig lovhjemmel må avgjøres ved å tolke den aktuelle loven. Hjemmelskravet er ikke statisk, men vil i noen grad variere avhengig av hvor inngripende behandlingen er for den enkelte. Jo mer inngripende behandlingen er for den enkelte, jo strengere krav må settes til klar lovforankring. Et viktig holdpunkt er om lovgiver har vurdert de personvernmessige betenkelighetene ved å behandle sensitive personopplysninger.

Begrunnelsen for unntaket er at lovhjemmel for behandling av sensitive personopplysninger må anses som tilstrekkelig når lovgiver har funnet at viktige samfunnsinteresser gjør slik behandling nødvendig. Eksempler som omfattes av nr 2 er arkivering i henhold til arkivloven.

Paragraf 9 nr 3 gjør unntak fra forbudet mot å behandle sensitive personopplysninger når den behandlingsansvarlige er forpliktet til å behandle personopplysningene i henhold til avtale mellom partene i arbeidslivet. Unntaket lovfester direktivet

artikkel 8 nr 3 b). Direktivet taler om «arbeidsrettslige» forpliktelser og rettigheter, og benytter med andre ord en tematisk avgrensning uavhengig av rettsgrunnlag. Rettslige grunnlag for arbeidsrettslige forpliktelser eller rettigheter vil i Norge enten være lov (se det generelle unntaket i nr 2), arbeidsavtale (se samtykke-unntaket i nr 1) eller tariffavtale (som unntaket her omfatter). For at den behandlingsansvarlige skal være «forpliktet» til å behandle de sensitive personopplysningene, må dette klart fremgå av rettsgrunnlaget, enten dette er lov, arbeidsavtale eller tariffavtale. Som påpekt ovenfor i merknadene til nr 2 er det grunn til kreve klarere hjemmel jo mer inngripende behandlingen er for den enkelte.

Unntaket i nr 4 gjør det tillatt å behandle sensitive personopplysninger når behandlingen er nødvendig for å beskytte den registrertes eller en annen persons vesentlige interesser, og vedkommende selv ikke er i stand til å gi samtykke som nevnt i nr 1. Unntaket bygger på direktivet artikkel 8 nr 2 c), og de to kumulative vilkårene gjør at bestemmelsen er en snever unntaksregel.

I direktivet trekker ordlyden i retning av at behandling av sensitive personopplysninger ikke kan finne sted i tilfeller der den registrerte er i stand til å gi sitt samtykke, men velger å ikke gjøre det selv om dette setter egne vesentlige interesser på spill. Og dersom den registrerte har rettslig handleevne, og er informert, må dette være greit. Mer problematisk blir situasjonen der den registrerte er i stand til å samtykke, men nekter dette slik at tredjemanns vesentlige interesser ikke kan beskyttes. I slike tilfelle kan imidlertid Datatilsynet gjøre unntak i medhold av annet ledd, se nedenfor, og spørsmålet kommer ikke på spissen. «Interesser» dekker alle typer interesser, således f eks interessen i psykisk og fysisk helse, og økonomiske interesser. Hva slags type interesse det dreier seg om kan ha betydning i vurderingen av om interessen er «vesentlig».

Nr 5 gjør det mulig for ideelle organisasjoner å behandle sensitive personopplysninger om organisasjonens medlemmer og personer som «på grunn av organisasjonens formål regelmessig er i kontakt med den» (jf direktivet artikkel 8 nr 2 d)). For medlemmer får unntaket bare selvstendig betydning der medlemmene ikke på annen måte har samtykket i behandlingen, jf nr 1. Når det gjelder ikke-medlemmer, vil det ofte være snakk om klient-lignende forhold, som f eks Frelsesarmeens innsats for hjemløse personer. Unntaket må forstås slik at den regelmessige kontakten som berettiger behandlingen av personopplysningene må være frivillig fra den registrertes side. En organisasjon kan ikke drive jevnlig oppsøkende virksomhet, og på dette grunnlag etablere rett til å behandle sensitive opplysninger om oppsøkte som ikke ønsker å bli kontaktet.

I direktivet gjøres forsøk på å angi hvilke typer organisasjoner unntaket skal omfatte, jf oppregningen som omfatter politiske, religiøse, filosofiske eller faglige organisasjoner. Organisasjonen må være ideell, og virksomheten «rettmessig». Dette innebærer ikke bare et krav om at virksomheten skal være lovlig i snever forstand (dvs ikke forbudt), men også at behandlingen av personopplysningene er saklig begrunnet i virksomheten, se § 7, og at behandlingen må vareta hensynet til personvern på en tilfredsstillende måte (jf direktivets krav til «fornødne garantier»). Dersom personvern hensyn ikke varetas på en tilfredsstillende måte, slik at virksomheten ikke er rettmessig i lovens forstand, kan Datatilsynet i medhold av § 40 bestemme at den aktuelle organisasjonen ikke kan behandle sensitive personopplysninger i medhold av nr 5 inntil tilfredsstillende personverngarantier foreligger.

Unntaket i nr 5 åpner ikke for alle former for behandling av personopplysninger – det fremgår uttrykkelig at bestemmelsen ikke hjemler videreforsending av personopplysningene. Skal de sensitive personopplysningene videreforsendes, krever dette samtykke fra de registrerte.

Paragraf 9 nr 6 hjemler behandling av sensitive personopplysninger som den registrerte selv har gjort alminnelig kjent, jf direktivet artikkel 8 nr 2 e) første alternativ. Med «alminnelig kjent» forstås at opplysningene er gjort kjent for en ubestemt krets av personer, f eks gjennom en biografi eller gjennom ett intervju. Senere behandling av opplysningene kan da lovlig finne sted uten den registrertes samtykke i den nye bruken. Også her gjelder imidlertid saklighetskravet i lovforslaget § 7.

Nr 7 lovfester unntaket i direktivet artikkel 8 nr 2 e) siste alternativ, og hjemler behandling av sensitive personopplysninger der dette er nødvendig for å fastlegge, forsvare eller gjøre gjeldende et rettskrav. Med «rettskrav» forstås rettigheter som pretenderes å bygge på et rettslig grunnlag, dvs et grunnlag som kan påberopes for domstolene (jf tvistemålsloven § 54). For en arbeidsgiver kan det f eks være snakk om å behandle opplysninger om en ansatts sykehistorie for på den måten å underbygge at det foreligger saklig grunn til oppsigelse. Det er ikke nødvendig at saken bringes inn for domstolene, men det ligger en klar begrensning i at behandlingen må være «nødvendig». Behandling av sensitive personopplysninger vil kun være lovlig dersom rettskravet ikke lar seg fastlegge på annen måte.

Nr 8 (jf direktivet artikkel 8 nr 3) tillater behandling av sensitive personopplysninger som ledd i ulike former for helsetjenester. Bestemmelsen har selvstendig betydning ved siden av unntakene i nr 1 (samtykke) og nr 2 (lov) f eks når den registrerte er syk eller skadet og av den grunn ikke er i stand til å samtykke. Unntaket får bare anvendelse der den som yter helsetjenesten er bundet av taushetsplikt som bygger på lov eller på regelverk som er fastsatt av «kompetente nasjonale organer».

Etter § 9 annet ledd kan Datatilsynet bestemme at sensitive personopplysninger kan behandles når viktige samfunnsinteresser tilsier at opplysningene kan behandles og det igangsettes tiltak for å vareta de registrertes interesser (se direktivet artikkel 8 nr 4). I mange tilfeller er viktige samfunnsinteressene nedfelt i lov som hjemler behandling av opplysningene, se merknadene til nr 2 ovenfor. Eksempler på «viktige samfunnsinteresser» gis i direktivets fortale pkt 34 – 36.

Datatilsynet kan bestemme om tiltakene for å sikre de registrertes interesser er tilstrekkelige. Dersom tiltakene ikke er tilstrekkelige, kan Datatilsynet avgjøre at unntaket ikke kan benyttes, jf § 40.

§ 10 Bruk av fødselsnummer

Bruk av fødselsnummer må være saklig begrunnet ut i fra behovet for sikker identifisering.

Datatilsynet kan gi pålegg om at fødselsnummer skal brukes for å sikre tilstrekkelig kvalitet på personopplysninger.

Til § 10:

Paragraf 10 gir en generell regulering av bruk av fødselsnummer, jf utvalgets kommentarer i 12.5.7 og direktivet artikkel 8 nr 7. Bestemmelsen har ingen parallell i personregisterloven.

Første ledd slår fast at bruk av fødselsnummer (fødselsdato samt personnummer) må være saklig begrunnet ut i fra behovet for sikker identifisering. Kravet til saklighet vil bare være oppfylt dersom andre indentifikasjonsmåter – som f eks navn, adresse og kundenummer – ikke er tilstrekkelig. Det vil også ha betydning hvor viktig sikker identifisering er for den registrerte. Den behandlingsansvarliges og samfunnsmessige behov kan også tillegges vekt.

Annet ledd gir Datatilsynet kompetanse til å bestemme at fødselsnummer skal brukes for å sikre tilstrekkelig kvalitet på personopplysninger. Dette bygger på en oppfatning om at personvernet i mange sammenhenger er tjent med at det er sikkerhet mht hvilke personer de aktuelle opplysningene knytter seg til, jf utvalgets vurderinger i 12.5.7. Kravet til tilstrekkelig kvalitet omfatter bl a oppdaterthet og at personopplysningene er dekkende.

§ 11 Sikring av personopplysninger

Den behandlingsansvarlige og databehandleren skal sørge for at personopplysningene til enhver tid er sikret tilstrekkelig konfidensialitet og har den kvalitet og tilgjengelighet som formålet med behandlingen tilsier.

Den behandlingsansvarlige plikter å gjennomføre sikkerhetsvurderinger og etablere og holde vedlike planlagte og systematiske sikkerhetstiltak for å oppnå kravene i første ledd. Sikkerhetstiltakene skal være bygget opp i henhold til alminnelige anerkjente metoder.

Sikkerhetsvurderingen og tiltakene skal dokumenteres og ved forespørsel være tilgjengelig for Datatilsynet og Personvernemnda. De ansatte i Datatilsynet og medlemmene i Personvernemnda plikter å hindre at andre får adgang eller kjennskap til opplysninger om sikkerhetsvurderinger og sikkerhetstiltak dersom slike opplysninger kan svekke sikkerhetstiltakene.

Kongen kan gi forskrift om sikring av personopplysninger.

Til § 11:

Første ledd pålegger den behandlingsansvarlige et *kontinuerlig* ansvar for sikring av personopplysninger. Sikkerhetsvurderingen må skje i forhold til de til enhver tid rådende forhold. Dette innebærer blant annet at også behandling under endrede forhold som er av kort varighet skal tilfredsstille sikkerhetskravene. Sikringen skal således for eksempel omfattes av situasjoner der en databehandler har rådighet over personopplysninger, jf § 13, og perioder der det foregår ombyggingarbeider, flytting til nye lokaler m v.

Behandling av personopplysninger kan etter § 7 bare skje til lovlige og uttrykkelig angitte formål, og opplysningene skal være relevante ut i fra formålet. Sikringen skal være tilstrekkelig i forhold til disse formålene (jf § 11 første ledd). Det er ikke mulig på forhånd å angi noen uttømmende oversikt over kategorier av formål med tilhørende sikringskrav.

Spesielt er det grunn til å peke på at behandling av sensitive personopplysninger kan begrunne strenge sikkerhetskrav. For konsesjonspliktige behandlinger vil sikringskravene således typisk være strenge. Men også behandling av sensitive personopplysninger til andre formål enn å treffe enkeltavgjørelser vil typisk bli omfattet av strenge krav. Selv om en ikke benytter sensitive opplysninger, vil behandling av opplysninger ellers typisk bli omfattet av strenge sikringskrav når sikringsnivået har direkte betydning for ivaretagelse av vesentlige personverninteresser. Opplysninger om private økonomiske forhold er for eksempel ikke omfattet av de generelt sensitive opplysningstypene i § 2 nr 8, men kan likevel, særlig i kombinasjon med andre opplysninger (for eksempel om sosiale forhold), anses som konkret sensitive med forholdsvis strenge krav til sikring.

Plikten til å sørge for sikring av personopplysninger tar utgangspunkt i begrepene «konfidensialitet», «kvalitet» og «tilgjengelighet». I mange tilfelle vil disse begrepene bare angi utgangspunkter som vil måtte konkretiseres og detaljeres

gjennom bruk av slike alminnelig anerkjente metoder som er omtalt i § 11 annet ledd, siste punktum.

Paragraf 11 sier ikke direkte noe om hva som må anses å være «alminnelige anerkjente metoder» for sikkerhetstiltakene. I tillegg til kontrolloppgaver har Datatilsynet i oppgave å gi råd og rettleiding i spørsmål om sikring av personopplysninger, se § 36 nr 5. Denne bestemmelsen sammenholdt med § 11 og kravet om bruk av anerkjente metoder, vil i praksis innebære at Datatilsynets veiledning blant annet vil innbefatte anvisning av relevante metoder og rådgivning ved valg av metode.

Sikkerhetsvurderingen vil i mange tilfelle måtte detaljeres for å oppnå tilstrekkelig presisjon i sikringskravene: For det første må sikkerhetsvurderingen detaljeres gjennom en nærmere utdyping av kravene til konfidensialitet, kvalitet og tilgjengelighet. Krav til kvalitet kan for eksempel *blant annet* sies å inneholde krav til korrekthet, oppdaterthet, relevans og fullstendighet. De metoder det henvises til i § 11 annet ledd skal inneholde slike detaljeringer på ulike nivå. Hvilken detaljeringsgrad som anses nødvendig, vil avhenge av formålet med behandlingen og hvor sensitive opplysningene er.

For det andre kan behovet for detaljering innebære at begrepet «opplysning» må spesifiseres slik at man i stedet opererer med «data», «informasjon» og «system». «Data» er tegn og signaler som er gjenstand for fortolkning, for eksempel som signaler i et datanett eller som koder/betegnelser på et skjema. «Informasjon» er det meningsinnhold som tillegges data når dataene fortolkes. Signalene på disketten fortolkes for eksempel av programvaren og blir til meningsbærende tekst på skjermen, og bokstaven «H» i feltet «yrkesstatus» forstås som «hjemmeværende». «System» sikter til større samfungerende samlinger av data og informasjon, og innebærer at det ikke bare kan stilles krav til data og -informasjon isolert, men også til systemer av data og informasjon.

Den sikkerhetsvurdering som den behandlingsansvarlige plikter å gjennomføre i henhold til § 11 *annet ledd*, bør for det første inneholde en kartlegging av hvilke *krav* som gjelder eller bør gjelde til konfidensialitet, kvalitet og tilgjengelighet, samt en *risikovurdering*, det vil si anslag av risikoen for at kravene ikke kan etterleves eller sannsynligheten for sikkerhetsbrudd forøvrig. Ut i fra risikovurderingen vil det så måtte skje en *tiltaksvurdering*. De krav som er utgangspunkt for hele sikkerhetsvurderingen vil ofte følge av lovgivning, for eksempel i form av bestemmelser om taushetsplikt. På dette grunnlaget bør det så for eksempel anslås hvor stor risiko det er for at taushetsplikten ikke vil bli overholdt og fastsettes tiltak som gir en «tilstrekkelig» sikkerhet. I et slikt tilfelle vil for eksempel passordbeskyttelse, automatisk nedkobling av skjermbilder med personinformasjon og spesiell autorisasjon for elektronisk overføring av opplysninger til andre enn en forhåndsdefinert personkrets, være eksempler på aktuelle tiltak. Hvor mange tiltak og hvor strenge hvert tiltak bør være, det vil si hva som anses å være «tilstrekkelig», vil avhenge av forholdet mellom formålet med behandlingen (jf overfor) og risikovurderingen. Datatilsynets praksis i konsesjonssaker og ved kontroll av sikkerhet ellers og spesielt av sikringstiltak etter § 11 vil på sikt angi et forutsigbart sikringsnivå.

Sikkerhetsvurderingen bør normalt også inneholde konkret angivelse av *mål* for sikringsarbeidet i forhold til de enkelte risikotyper. Det vil videre være aktuelt å fastlegge hvorledes forholdet mellom krav, tiltak og mål skal *evalueres*.

Behandling av personopplysninger vil ofte skje på tvers av språklige og kulturelle grenser. Forskjeller mellom for eksempel organisasjoner, distrikter og nasjoner kan innebære spesielle sikkerhetsproblemer, for eksempel fordi det blir ekstra utfordrende å formidle meningsinnholdet i persondata, med fare for at det oppstår feil personinformasjon. Sikkerhetsvurderingen må også omfatte de spesielle risiki som språklige og kulturelle forskjeller innebærer.

Datatilsynets kan med hjemmel i § 40 pålegge den behandlingsansvarlige å utføre sikringstiltak dersom dette er nødvendig for at lovens krav til sikkerhet skal oppfylles. Også hensyn til forskningsmetode, forretningsdrift, etterforskning, forsvar m v kan begrunne krav til konfidensialitet, kvalitet og tilgjengelighet. Sikringstiltakene vil således kunne ha flere samtidige begrunnelser og hjemler. Datatilsynets adgang til å gjøre unntak fra offentlighet dersom innsyn vil svekke sikkerhet er ikke avgrenset til sikring i henhold til § 11 jf § 40. Slike unntak kan etter en totalvurdering også gjøres ut i fra *andre* sikringshensyn.

Sikkerhetsvurderingen og de tiltak som er gjennomført skal dokumenteres, og denne dokumentasjonen skal på forespørsel være tilgjengelig for Datatilsynet. Dette følger også av § 12 om internkontroll, og dokumentasjonen i henhold til § 11 vil utgjøre en vesentlig del av internkontrollsystemet. Kravene etter § 11 gjelder imidlertid *personopplysninger* og ikke for eksempel generelle opplysninger om behandlinger og behandlingsansvarliges plikt til å inngi melding og søke konsesjon (jf §§ 31 og 33). For mange behandlinger (for eksempel av sensitive opplysninger) vil kravene til vurderinger og dokumentasjon etter § 11 være strengere enn det som følger av internkontrollbestemmelsen i § 12.

Sikkerhetskravene gjelder tilsvarende for databehandler som for behandlingsansvarlige. Dette innebærer både en plikt for behandlingsansvarlige til å gi informasjon om og legge til rette for aktuelle sikringstiltak, og det gir databehandler en plikt til å etterspørre og etterleve eksisterende sikkerhetskrav. I § 13 er det etablert en plikt til å inngå avtale ved utlevering av personopplysninger til databehandler eller andre. I avtale med databehandler bør sikringsspørsmål alltid være omhandlet, men det vil være stor forskjell på hvor omfattende og inngående avtalereguleringene er. Ved utlevering til andre, vil disse bli å regne som behandlingsansvarlige med selvstendig plikt etter § 11.

Taushetspliktsbestemmelsen i tredje ledd annet punktum er begrunnet i at den alminnelige taushetspliktsbestemmelsen i forvaltningsloven § 13 ikke alltid vil være tilstrekkelig omfattende, og det er av avgjørende betydning at den behandlingsansvarlige og databehandleren har tillit til at opplysninger om sikkerhetstiltak m v ikke kommer på avveie. Dersom Datatilsynet fortsatt skal ledes av et styre, jf 18.3.7, må taushetsplikten også omfatte styrets medlemmer, og tredje ledd annet punktum bør i så tilfelle lyde slik:

«De ansatte i Datatilsynet, styremedlemmene og medlemmene i Personvernemnda plikter å hindre at andre får adgang eller kjennskap til opplysninger om sikkerhetsvurderinger og sikkerhetstiltak dersom slike opplysninger kan svekke sikkerhetstiltakene.»

§ 12 Internkontroll

Den behandlingsansvarlige skal kunne dokumentere at det er etablert systemer og rutiner som sikrer overholdelse av reglene i loven samt vilkår og pålegg etter §§ 35 og 40.

Kongen kan gi forskrift om internkontroll.

Til § 12:

Kravene til internkontroll og dokumentasjon av tiltak som er egnet til å sikre overholdelse av personvernregler, gjelder for det første *generelle* regler i lov og forskrift. I tillegg skal dokumentasjonen omfatte tiltak for etterlevelse av regler som gis for *den enkelte* behandling, det vil si for konsesjonsvilkår (§ 35) og for pålegg i henhold til § 40.

Det er ikke fastsatt noen krav til metode for etablering av internkontrollsystem, jf § 12 annet ledd. Etableringen kan imidlertid med fordel bygges på en tilnærming som innebærer aktivitetene: kartlegging av krav (i aktuelle regler), risikovurdering, fastlegging av mål, tiltaksvurdering og evaluering.

Lovforslaget etablerer en plikt for alle behandlingsansvarlige til å gjennomføre de nevnte vurderingene. Det kan imidlertid ikke kreves at vurderingene alltid vil lede ut i konkrete tiltak. En vurdering av retten til innsyn i opplysninger om en selv i § 18 kan for eksempel gi som konklusjon at det ikke er behov for særskilte tiltak, for eksempel fordi henvendelsene er få og det også for øvrig er enkelt å gjennomføre lovens regel i praksis.

Den dokumentasjonen som kreves i henhold til § 12 skal kunne fremlegges for Datatilsynet ved forespørsel. Dette følger § 38 første ledd. Internkontrollsystemet og dokumentasjonen må ajourføres fortløpende i tråd med endrede forhold.

§ 13 Databehandlerens rådighet over personopplysninger

Databehandleren kan ikke uten avtale med den behandlingsansvarlige anvende opplysningene til andre formål enn det oppdraget gjelder. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

Til § 13:

Paragraf 13 regulerer bruk av databehandler, og gjennomfører direktivet artikkel 17 nr 2 – 4. Bestemmelsen er en videreføring av personregisterloven § 23, men bestemmelsen gis et langt bredere anvendelsesområde fordi «databehandlere» omfatter langt flere enn personregisterlovens begrep «databehandlingsforetak».

Hva som menes med «databehandler» fremgår av definisjonen i § 2 nr 5, se utvalgets merknader til denne bestemmelsen.

Bestemmelsen regulerer databehandlerens rådighet over personopplysninger som behandles på vegne av den behandlingsansvarlige. Første punktum gjelder bare anvendelse av opplysningene til andre formål, mens annet punktum gjelder overlattelse til andre for lagring eller bearbeidelse. Annet punktum innebærer at databehandlere ikke kan samarbeide med andre databehandlere om å utføre oppdraget uten at dette avtales med oppdragsgiveren.

§ 14 Frist for oppfyllelse av plikter

Den behandlingsansvarlige skal sørge for at den registrertes krav etter loven §§ 16, 18, 22, 25, 26, 27 og 28 gjennomføres uten ugrunnet opphold og senest innen én måned.

Dersom særlige grunner gjør det umulig å oppfylle pliktene innen en måned kan gjennomføring skje senere. I slike tilfeller skal midlertidig skriftlig svar gis innen fristen. I det midlertidige svaret skal det opplyses om grunnen til forsinkelsen og sannsynlig tidspunkt for gjennomføring.

Til § 14:

Bestemmelsen fastsetter frister for den behandlingsansvarlige til å oppfylle krav fra den registrerte etter loven. Det finnes etter personregisterloven og direktivet bare spredte eksempler på krav til hvor raskt de behandlingsansvarlige skal gi svar på henvendelser fra de registrerte og ellers utføre plikter i forhold til de registrerte, se 11.6.1.

Hva som er å anse som særlige grunner må avgjøres konkret og avhenger bl a av hvilken rettighet som skal gjennomføres (både type plikt og hvor omfattende denne er). Den vanligste årsaken til at den behandlingsansvarlige ikke oppfyller sine plikter i tide vil sannsynligvis være for liten kapasitet. Dette kan være en akseptabel grunn for forsinkelse i noen tilfeller, for eksempel for krav etter § 27 om å få gjennomført en manuell behandling, forutsatt at slike krav behandles sammen med andre klager i den rekkefølge de er kommet inn. Når det gjelder krav etter § 28 til å få sitt navn sperret mot bruk i markedsføringsøyemed, kan det vanskelig tenkes at liten kapasitet er særlig grunn til ikke å gjennomføre sperringen senest innen én måned.

§ 15 Betaling

Rettighetene etter §§ 16, 18, 22, 25, 26, 27 og 28 utøves vederlagsfritt for den registrerte. Dersom særlige grunner gjør det nødvendig, kan Kongen gi forskrift om at den registrerte må betale vederlag til den behandlingsansvarlige for å benytte disse rettighetene.

Til § 15:

Paragraf 15 fastslår at rettighetene etter loven utøves vederlagsfritt for den enkelte. Bestemmelsen lovfester dagens rettstilstand selv om personregisterloven ikke har noen bestemmelse om dette. For kredittopplysningsforetak er det imidlertid i personregisterloven § 20 annet ledd gitt en bestemmelse om at foretaket i visse tilfeller kan beregne seg en rimelig godtgjørelse når opplysninger blir gitt skriftlig. Vederlagsregel er begrunnet i «hensynet til å motvirke at det gis gratis kredittopplysning, ikke i byråenes arbeid og omkostninger ved innsynssystemet», se Ot prp nr 2 1977-78 side 93. Dette er et eksempel på en særlig grunn som kan foranledige forskrift etter § 15.

"Hva er personvern?" i Kapittel 3 Innsynsrett og varslingsplikt m v

§ 16 Rett til generell informasjon om behandling av personopplysninger

Den som ber om det skal få vite hvilke behandlinger av personopplysninger en behandlingsansvarlig foretar.

Den som ber om det skal dessuten få følgende informasjon om en bestemt behandling av personopplysninger:

1. navn og adresse på den behandlingsansvarlige og på dennes eventuelle representant, jf § 6
2. hvem som har det daglige ansvaret for å oppfylle pliktene som hviler på den behandlingsansvarlige
3. behandlingens formål
4. definisjoner og andre beskrivelser av de typer personopplysninger som inngår i behandlingen
5. kilde for opplysningene
6. hvem personopplysningene blir eller vil bli utlevert til, herunder planlagt utlevering av personopplysningene til mottakere i andre stater.

Informasjon kan kreves hos den behandlingsansvarlige eller dennes representant som nevnt i § 6. Den som ber om informasjon kan kreve at informasjonen gis skriftlig.

Kongen kan gi forskrift om unntak fra første ledd dersom dette er nødvendig av hensyn til rikets sikkerhet eller forebyggelse og etterforskning av straffbare handlinger.

Til § 16:

Paragraf 16 lovfester krav om generell informasjon om elektronisk behandling av personopplysninger. Bestemmelsen gir også rett til generell informasjon om manuell behandling av personopplysninger når personopplysningene inngår eller skal inngå i et personregister, se utvalgets merknader i 11.2.3 og 11.2.4 og direktivet artikkel 21 nr 3. Direktivet artikkel 21 nr 3 retter seg mot behandlinger som ikke er meldepliktige. Opplysningene det skal gis innsyn i er i hovedsak de samme som meldingen skal inneholde for de meldepliktige behandlingene, men meldingene vil være mer omfattende. Også for de ikke-meldepliktige behandlingene må altså den behandlingsansvarlige føre en ajourført oversikt som minst inneholder opplysningene det kan kreves innsyn i. Bestemmelsen har en viss parallell i personregisterloven § 7 tredje ledd.

Første ledd gir den som ber om det – med andre ord enhver, slik ordet nyttes i offentlighetsloven § 2 – rett til å få vite hvilke behandlinger en behandlingsansvarlig foretar. Formålet med bestemmelsen er å gi enhver muligheten til å få vite om det er interessant å skaffe seg mer informasjon om en bestemt behandling av personopplysninger, jf annet ledd, og skaffe seg oversikt slik at ev innsynsrett kan benyttes (jf særlig § 18 om rett til innsyn i opplysninger om en selv). Ved å benytte den allmenne retten til informasjon kan man også ta stilling til om man vil la den behandlingsansvarlige få behandle opplysninger om en selv. For eksempel kan det bes om allment innsyn før man tar stilling til om man vil melde seg inn i en plateklubb etc.

Retten til informasjon etter *annet ledd* gjelder «en bestemt behandling av personopplysninger». Den som ønsker å benytte seg av innsynsretten må med andre ord identifisere den behandlingen det ønskes innsyn i. Ettersom informasjonen etter første ledd skal gi tilstrekkelig grunnlag for å peke ut en bestemt behandling, er kravet om identifikasjon en rent praktisk foranstaltning, og gir ikke grunnlag for å avvise den som ber om informasjon.

Annet ledd nr 1 – 6 regner opp de opplysningene det skal gis innsyn i. Det legges opp til at informasjonen skal være generell, standardisert og kortfattet. Både Datatilsynet og den registrerte vil ha andre hjemler til å skaffe seg ytterligere informasjon.

Informasjonen skal i henhold til direktivet omfatte opplysningene som er nevnt i direktivet artikkel 19 nr 1 bokstavene a) – e). Utvalgets forslag tilfredsstiller dette, og pålegger i tillegg den behandlingsansvarlige å gi informasjon om hvem som har det daglige ansvaret for å oppfylle pliktene som hviler på den behandlingsansvarlige (nr 2). I motsetning til meldinger til Datatilsynet omfattes ikke informasjon om sikkerhetstiltak.

I henhold til nr 6 (jf direktivet artikkel 19 nr 1 bokstav d) skal det gis innsyn i hvilke mottakere som opplysningene blir eller vil bli utlevert til. Det er tilstrekkelig å angi kategorier av mottakere, f eks til typer av aktører innenfor visse bransjer etc. Informasjonen om mottakerne kan med andre ord generaliseres – det er ikke nødvendig å navngi eller på annen måte identifisere hver enkelt mottaker. På den annen side kan ikke kategoriseringen gjøres så abstrakt at informasjonen blir intetsigende.

Det skal også informeres om planlagt utlevering av personopplysninger til mottakere i andre stater, og ikke bare opplysninger om videregivelse til tredjeland (stater utenfor EØS-området). Dette er bevisst fra utvalgets side, og har sammen-

heng med den lovtekniske løsningen utlevering til utlandet reguleres på, jf lovforslaget "*Personregisterloven med forskrifter*" i kapittel 5.

Tredje ledd forteller hvem det kan kreves informasjon hos, dvs den behandlingsansvarlige eller dennes representant som nevnt i § 6 (behandlingsansvarlige som ikke er etablert i Norge, men som benytter hjelpemidler som befinner seg her). At innsyn også kan kreves hos representanten følger allerede av § 6 annet ledd siste punktum, men er tatt med av informasjonshensyn. Det følger forutsetningsvis av bestemmelsen at den registrerte ikke kan rette krav om innsyn mot databehandleren. Dette er selvsagt ikke til hinder for at den behandlingsansvarlige kan oppfylle plikten til å gi innsyn ved å instruere databehandleren om dette. For behandlinger hvor det enten er innsendt melding eller gitt konsesjon, kan informasjonen kreves også hos Datatilsynet, jf § 17.

Fjerde ledd gir Kongen kompetanse til å bestemme at innsynsretten ikke skal gjelde dersom dette er nødvendig av hensyn til rikets sikkerhet eller forebyggelse eller etterforskning av straffbare handlinger, jf direktivet artikkel 13 nr 1.

§ 17 Offentlig fortegnelse over konsesjoner og meldinger

Datatilsynet skal føre en systematisk fortegnelse over alle behandlinger som er innmeldt etter § 31 eller gitt konsesjon i medhold av § 33. Av fortegnelsen skal det minst fremgå opplysninger som nevnt i § 16 annet ledd.

Fortegnelsen skal være offentlig på den måten Datatilsynet bestemmer.

Kongen kan gi forskrift om fortegnelsen og gjøre slike unntak fra første ledd som er nødvendig ut fra beredskapshensyn eller hensynet til rikets sikkerhet.

Til § 17:

Paragraf 17 pålegger Datatilsynet å føre en systematisk fortegnelse over alle behandlinger som er innmeldt eller gitt konsesjon, jf første ledd. Bestemmelsen er basert på direktivet artikkel 21 nr 2, og er en videreføring av personregisterloven § 4 (jf utvalgets kommentarer i 11.2.2). Fortegnelsen skal minst inneholde samme opplysninger som nevnt i § 16 annet ledd, jf kommentarene til denne bestemmelsen.

Annet ledd fastslår at fortegnelsen skal være offentlig tilgjengelig. Datatilsynet kan bestemme på hvilken måte fortegnelsen skal offentliggjøres, f eks om den skal legges ut på Internett. Det er av stor betydning at de registrerte gis så lik mulighet til innsyn som mulig uavhengig av hvor i Norge de befinner seg.

Tredje ledd gir Kongen hjemmel til å gi forskrift om fortegnelsen, herunder unntak som er nødvendig ut fra beredskapshensyn eller hensynet til rikets sikkerhet, jf direktivet artikkel 13 nr 1.

§ 18 Den registrertes rett til innsyn

Den registrerte skal på forespørsel få opplyst:

1. hvilke opplysninger om en selv som behandles ved elektroniske hjelpemidler eller som er tatt inn i et manuelt register
2. behandlingens formål
3. hvem opplysningene om en selv blir eller vil bli utlevert til
4. kilden for disse opplysningene
5. hvilke sikkerhetstiltak som er knyttet til behandlingen, dersom innsyn ikke svekker sikkerheten.

Innsyn kan kreves hos den behandlingsansvarlige eller dennes representant som nevnt i § 6. Den registrerte kan kreve at opplysningene skal gis skriftlig.

Til § 18:

Paragraf 18 gir den registrerte rett til innsyn i opplysninger om en selv. Bestemmelsen viderefører og videreutvikler innsynretten i personregisterloven § 7, jf direktivet artikkel 12 a første strekpunkt og utvalgets kommentarer i 11.2.5.

Første ledd nr 1 oppstiller hovedregelen om innsyn i opplysninger om en selv som behandles ved elektroniske hjelpemidler eller som er inntatt i et manuelt (papirbasert) register. Nytt i forhold til personregisterloven § 7 er at innsynsretten i manuelle registre likestilles med innsynsretten i elektronisk lagrede opplysninger. Videre utvides innsynsretten iforhold til private, jf 11.2.5.4, slik at innsynsretten her likestilles med innsynsretten overfor organer for stat eller kommune. Fra hovedregelen gjøres imidlertid enkelte unntak (jf direktivet artikkel 13).

Første ledd nr 2 gir den registrerte krav på informasjon om behandlingens formål. I motsetning til § 16 annet ledd nr 3, som gir rett til generell og kortfattet informasjon om formålet med behandlingen(e), har den registrerte krav på informasjon om formålet med den behandlingen som berører den registrerte. Kravet om konkret og individualisert innsyn gjelder tilsvarende for nr 3 om utlevering og nr 4 om kildeangivelsen. Innsyn i kilden skal sette den registrerte istand til å finne ut hvor informasjonen om ham eller henne er hentet fra.

I tillegg har den registrerte krav på innsyn i opplysninger om sikkerhetstiltak, jf nr 5. Dette gjelder likevel ikke dersom innsyn svekker sikkerheten. Det må her sones mellom ulike sikkerhetstiltak. Tiltak som skal sikre at ikke uvedkommende skal kunne få tilgang til personopplysningene vil lett omfattes av unntaket fra innsyn. Andre sikkerhetstiltak, f eks tiltak for å høyne opplysningskvaliteten, vil det derimot sjelden være aktuelt å gjøre unntak fra.

Innsynsrett skal gis «fritt og uhindret, med rimelige mellomrom og uten større ventetid eller større utgifter», jf direktivet artikkel 12 bokstav a) innledningsvis og lovforslaget §§ 14 (frister) og 15 (betaling).

§ 19 Unntak fra den registrertes rett til innsyn

Innsynsretten etter § 18 gjelder ikke opplysninger som bare brukes til statistikk, forskning eller generelle planleggingsformål dersom behandlingen ikke får noen direkte betydning for den registrerte.

Innsynsretten gjelder ikke opplysninger som det må anses utilrådelig at den registrerte får kjennskap til, av hensyn til vedkommendes helse eller forholdet til personer som står dem nær. Opplysningen kan på anmodning likevel gjøres kjent for en representant for den registrerte når ikke særlige grunner taler mot det.

Den registrerte kan ikke kreve innsyn i opplysninger i dokumenter som er unntatt fra innsyn etter forvaltningsloven § 18. Overfor behandlingsansvarlige som ikke er organ for stat eller kommune kan det ikke kreves innsyn i opplysninger i dokumenter som er utarbeidet for den interne saksforberedelse av

1. den behandlingsansvarlige selv
2. særskilte rådgivere eller sakkyndige, eller
3. annen sammenslutning eller stiftelse innenfor eget konsern eller organisasjon.

Selv om opplysninger er unntatt etter reglene i tredje ledd, har den registrerte rett til innsyn i faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum. Dette gjelder likevel ikke når den registrerte på annen måte har tilgang til de faktiske opplysningene.

Dersom innsyn kan motvirke muligheten for å få en sak som er under behandling avklart, kan den som kravet om innsyn retter seg mot bestemme at den registrerte ikke skal gis innsyn så lenge undersøkelser pågår.

Kongen kan gi forskrift om unntak fra og vilkår for bruk av innsynsretten.

Til § 19:

Paragraf 19 gjør visse unntak fra innsynsretten.

Første ledd gjør unntak fra innsynsretten der personopplysningene utelukkende benyttes til statistikk, forskning eller generelle planleggingsformål. Dette er en videreføring av personregisterloven § 7 første ledd annet punktum (jf foran 3.3.4 om det beslutningsfokuserede personvernet). Det stilles imidlertid opp et vilkår om at unntaket fra innsynsretten kun gjelder når de nevnte formålene ikke får noen direkte betydning for den enkelte. Dette innebærer at den registrerte likevel har innsynsrett dersom behandlingen enten får rettsvirkninger eller direkte faktiske virkninger for den registrerte. Utvalget har på denne måten ment å lovfeste Datatilsynets praksis i dag, jf 11.2.5.4.5.

Annet ledd gjør unntak fra innsynsretten der det må anses som utilrådelig at den registrerte får kjennskap til opplysningene av hensyn til den registrertes helse eller forholdet til personer som står dem nær. Unntaket viderefører personregisterloven § 7 første ledd siste punktum. Nytt i forhold til personregisterloven er at opplysningene likevel kan gjøres kjent for en representant for den registrerte når ikke særlige grunner taler mot det, jf den tilsvarende regelen i forvaltningsloven § 19 første ledd bokstav c og utvalgets merknader i 11.2.5.4.4.

Tredje ledd regulerer forholdet til innsynsrett etter forvaltningsloven § 18, jf personregisterloven § 7 annet ledd siste punktum og utvalgets vurderinger i 11.2.5.4.3. Et hovedsynspunkt er at innsynsrett etter personopplysningsloven ikke skal rekke lenger enn innsynsrett etter forvaltningsloven. Selv om det mest hensiktsmessige kunne være å knytte innsynet direkte til personopplysningene, er innsyn forankret i dokumenter (jf formuleringen «innsyn i opplysninger i dokumenter») slik at uttrykksmåten harmonerer med forvaltningsloven.

Den registrerte kan ikke kreve innsyn i opplysninger i dokumenter som er unntatt fra innsyn i medhold av forvaltningsloven § 18. Utvalget har valgt en noe annen formulering enn i personregisterloven, slik at unntak fra innsynsretten krever at det aktuelle dokumentet som rommer opplysningene *blir* unntatt fra partsoffentlighet, og ikke bare kan bli unntatt.

Også i privat sektor og i offentlige virksomheter som ikke er «organ for stat eller kommune» er det behov for å gjøre unntak fra innsyn i interne dokumenter. Utvalget foreslår at dette gjennomføres ved en lignende formulering som i dag finnes i personregisterforskriften § 1-5 annet ledd (interne dokumenter i manuelle personalregistre).

Nytt i forhold til personregisterloven er at det skal gis innsyn i faktiske personopplysninger, jf fjerde ledd. Regelen er basert på den tilsvarende regelen i forvaltningsloven § 18, men gjelder i lovforslaget både for organer for stat eller kommune, for andre offentlige virksomheter og for behandlingsansvarlige i privat sektor. Begrunnelsen for bestemmelsen er at det ikke er så stort behov for å unnta faktiske opplysninger som vurderinger som knytter seg til enkeltpersoner. Retten til innsyn i faktiske opplysninger etter femte ledd gjelder ikke dersom den registrerte på annen måte har tilgang til disse opplysningene.

Femte ledd gir den behandlingsansvarlige anledning til på visse vilkår å utsette tidspunktet for offentlighet, jf forvaltningsloven § 20 første ledd og personregisterforskriften 1979 § 1-2 første ledd annet punktum.

I *siste ledd* gis Kongen kompetanse til å gi forskrift om unntak fra og vilkår for bruk av innsynsretten. Bestemmelsen er en videreføring av personregisterloven § 7

siste ledd. Eventuelle innskrenkninger i innsynsretten i forskrift må være i samsvar med direktivet artikkel 13.

Utvalget understreker for ordens skyld at den behandlingsansvarlige kan gi innsyn i mer enn det loven krever (merinnsyn) såfremt dette ikke strider mot lovlig etablert taushetsplikt. I mange tilfelle kan slikt mer innsyn være ønskelig, og behandlingsansvarlige bør vurdere om muligheten skal benyttes.

§ 20 Informasjonsplikt ved innsamling av personopplysninger fra den registrerte

Ved innsamling av personopplysninger fra den registrerte skal den behandlingsansvarlige opplyse den registrerte om hvem som er behandlingsansvarlig, formålet med innsamlingen av opplysningene samt om det er frivillig å levere fra seg opplysningene. Informasjonsplikten gjelder ikke dersom den registrerte må antas allerede å kjenne til dette.

Ytterligere informasjon skal gis dersom det må antas å være nødvendig for at den registrerte skal kunne ivareta egne interesser. Eksempler på slik informasjon er hvem opplysningene kan bli utlevert til, samt i hvilken grad den registrerte kan kreve innsyn, retting eller sletting av opplysningene.

Til § 20:

Paragraf 20 pålegger den behandlingsansvarlige å informere den registrerte når det innsamles opplysninger fra denne. Bestemmelsen er ny i forhold til personregisterloven, og gjennomfører direktivet artikkel 10 (jf utvalgets merknader i 11.2.6).

Første ledd gir uttrykk for det minimum av informasjon som skal gis til den registrerte. Dersom den registrerte må antas allerede å kjenne til det som det skal informeres om, gjelder ikke informasjonsplikten.

Det er ikke alltid tilstrekkelig å gi slik informasjon som nevnt i første ledd. Formålet med informasjonsplikten er å gi den registrerte mulighet til å gjøre bruk av sine rettigheter etter loven som f eks innsyn, retting m v. Dette er bakgrunnen for at *annet ledd* pålegger den behandlingsansvarlige å gi tilleggsinformasjon dersom dette er nødvendig for at den registrerte skal kunne vareta egne interesser. Lovteksten gir også eksempler på slik tilleggsinformasjon.

Det er den behandlingsansvarlige som i første omgang må vurdere konkret om det er behov for å gi tilleggsinformasjon som nevnt i annet ledd. Vurderingen kan bli overprøvet av Datatilsynet, som i medhold av § 40 kan gi pålegg om at ytterligere informasjon skal gis dersom det anses som nødvendig. Dersom den behandlingsansvarlige ønsker å standardisere informasjonen av effektivitetshensyn, er det selvsagt ikke noe i veien for at det automatisk gis tilleggsinformasjon dersom denne informasjonen er omfattende nok til å dekke alle tilfeller.

§ 21 Varslingsplikt ved innsamling av personopplysninger fra andre enn den registrerte

Dersom personopplysningene innhentes fra andre enn den registrerte, skal den behandlingsansvarlige gi informasjon som nevnt i § 15 annet ledd til den registrerte når registrering skjer. Dersom opplysningene skal videregis innen rimelig tid, kan varslingen utsettes til første gangs videregivelse av opplysningene.

Første ledd gjelder ikke dersom

1. varslingen er umulig eller uforholdsmessig vanskelig,
2. den registrerte må antas å være kjent med behandlingen, eller
3. det er fastsatt i lov at det er adgang til å registrere eller videreggi opplysningene.

Til § 21:

Mens § 20 pålegger den behandlingsansvarlige informasjonsplikt når det samles inn opplysninger fra den registrerte, oppstiller § 21 varslingsplikt når opplysninger om den registrerte samles inn fra andre kilder. Når det er varslet etter § 20 vil det i mange tilfeller ikke være behov for å varsle etter § 21 fordi den registrerte allerede er informert. Paragraf 21 har ingen parallell i personregisterloven, og lovfester direktivet artikkel 11 (jf om direktivet artikkel 11 i 11.2.6.3 og utvalgets vurderinger i 11.2.6.6).

Første ledd oppstiller hovedregelen om at det skal varsles, og sier også hva slags informasjon som skal gis, jf henvisningen til § 16 annet ledd om rett til innsyn i generelle opplysninger om behandling av personopplysninger. Informasjonen skal som hovedregel gis samtidig som opplysningene lagres (registreres). Det kan være fordelaktig at administrative rutiner ordnes slik at innsamling automatisk iverksetter varsling.

Med varsel menes i utgangspunktet individuelt varsel, dvs eget varsel til hver enkelt registrert. Dersom individuelt varsling er uforholdsmessig vanskelig, kan varsel gis på annen måte, f eks ved annonser. Dersom kollektivt varsel er uhensiktsmessig, gjelder ingen varslingsplikt.

Dersom opplysningene som samles inn skal videregis, kan varsling utsettes til videregivelse skjer. Utsatt varsling ved videregivelse forutsetter at videregivelsen skjer innen rimelig tid. Begrunnelsen for denne reservasjonen er at det ville være uheldig dersom varslingsplikten ble undergravet ved at varsling ble utsatt i påvente av en (mulig) videregivelse langt inn i fremtiden. Hva som er rimelig tid må vurderes konkret, jf den tilsvarende fristsangivelsen i bl a kjøpslovens fristbestemmelser. Datatilsynets praksis vil her etterhvert gi veiledning, jf lovforslaget § 40.

Som det fremgår av utvalgets vurderinger i 11.2.6.6 ser utvalget klart et behov for å benytte seg av muligheten direktivet gir for å gjøre unntak fra varslingsplikten. Slike unntak finnes i § 21 annet ledd.

I nr 1 gjøres unntak fra varslingsplikten der varslingen er umulig eller uforholdsmessig vanskelig, jf direktivet artikkel 11 nr 2 og den lignende formuleringen i forvaltningsloven § 16 tredje ledd bokstav a) første alternativ. Begrunnelsen for dette unntaket er en avveining av den registrertes nytte av varslingen mot de ressurser den behandlingsansvarlige må bruke for å få gjennomført varslingen. I vurderingen av hva som er «uforholdsmessig» må det tas hensyn til hvor viktig det typisk er for den registrerte å bli varslet om den aktuelle behandlingen.

Nummer 2 gjør unntak fra varslingsplikten når den registrerte må antas allerede å være kjent med behandlingen, jf direktivet artikkel 11 nr 1. Begrunnelsen for unntaket er at det i disse tilfellene ikke er behov for varsling. For at dette unntaket skal få anvendelse, må imidlertid den registrerte kjenne til opplysningene som nevnt i § 16 annet ledd.

Nummer 3 slår fast at varsling ikke er nødvendig når registreringen eller videregivelsen er fastsatt i lov, jf direktivet artikkel 11 nr 2. I disse tilfellene gir loven informasjon til den registrerte, og eget varsel er unødvendig.

§ 22 Rett til begrunnelse for fullstendig automatiserte avgjørelser

Dersom det foreligger en avgjørelse som definert i § 2 nr 9 som fullt ut er basert på automatisk behandling av personopplysninger, kan den som avgjørelsen retter seg mot kreve å få begrunnet resultatet. I begrunnelsen skal den behandlingsansvarlige redegjøre for regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen.

Til § 22:

Paragraf 22 gir den registrerte rett til å kreve begrunnelse for fullstendig automatiserte beslutninger, jf direktivet artikkel 12 bokstav a tredje strekpunkt og 11.4 foran. Bestemmelsen er ny i forhold til personregisterloven.

Vilkårene for at bestemmelsen skal få anvendelse er for det første at det foreligger en fullstendig automatisert beslutning, jf det tilsvarende uttrykket i § 27 og utvalgets merknader i den forbindelse. Avgjørelsen må dessuten være bestemmende for den som avgjørelsen retter seg mot. Interne avgjørelser omfattes ikke, og ei heller avgjørelser som ikke pålegger den registrerte plikter.

Annet punktum sier hva begrunnelsen skal inneholde, dvs regelinnholdet i data-maskinprogrammene som ligger til grunn for beslutningen. Med «regler» forstås generelle normer som styrer avgjørelsesprosessen, som f eks (tolkninger av) rettsregler, avtaler og skjønnsmessige retningslinjer. For organer for stat eller kommune gjelder allerede i dag langt på vei en slik plikt i henhold til annen lovgivning, jf nærmere 11.4.2. For andre virksomheter, og særlig innenfor privat sektor, vil denne begrunnelsesplikten være ny. Utvalget antar imidlertid at få beslutningsprosesser vil omfattes av regelen, jf 11.4.4.

§ 23 Varslingsplikt ved bruk av personprofiler

Når det treffes enkeltavgjørelser som definert i § 2 nr 9 eller gjøres henvendelser til den registrerte på grunnlag av personprofiler som er ment å beskrive atferd, preferanser, evner eller behov, skal den behandlingsansvarlige opplyse den registrerte om hvem som er behandlingsansvarlig, hvilke opplysningstyper som er anvendt, samt kildene for disse opplysningene.

Til § 23:

Bestemmelsen stiller krav til varsling ved bruk av «personprofiler». Med «personprofiler» sikter en til opplysninger som er sammensatt for å beskrive preferanser, adferd, behov, evner m v. Opplysningene vil typisk være «elektroniske spor», dvs personopplysninger som blir rutinemessig innsamlet i systemer for betalingsformidling, elektroniske informasjonstjenester og annet. Personprofiler kan imidlertid også bestå av opplysninger som er samlet inn på annen måte. En personprofil kan for eksempel være basert på opplysninger om typisk tidspunkt og sted vareinnkjøp, inntektskategori, boligstrøk og alder. En personprofil basert på slike opplysningstyper kan for eksempel gjelde personer som handler mat på bensinstasjoner og i kiosker etter klokken 20.00 mer enn 3 ganger i uken, med inntekt over 300.000 og bolig i bydelene X og Y. Slike profiler kan danne grunnlag for antagelse om bestemte behov, for eksempel antagelser om at personene er aktuelle som kunder for bestilling av matvarer over Internett. Personprofiler kan også tenkes anvendt for verving av medlemmer i organisasjoner, rekruttering av givere til ideelle organisasjoner eller for politisk påvirkning/mobilisering. Personprofiler blir også anvendt for å treffe enkeltavgjørelser, for eksempel ved behandling av lånesøknader.

Forslaget § 23 innebærer en plikt til å varsle om at personprofiler er anvendt, hvilke kilder og opplysningstyper som er anvendt og hvem som er behandlingsansvarlig for profilen. Det kreves ikke at det varsles hvilke konkrete antagelser som ligger bak den enkelte personprofil. Bestemmelsen gjelder både ved bruk av profiler til beslutninger og henvendelser. Det forhold at det har vært gjennomført en manuell vurdering i tillegg til en maskinell bruk av personprofiler, har i seg selv ikke betydning forplikten til å varsle. Bestemmelsen supplerer §§ 20, 21 og 22 ved direkte å regulere en viktig anvendelse av personinformasjon som skaper personvernbehov

som de andre nevnte bestemmelsene bare *delvis* imøtekommer, bl a fordi disse øvrige varslingsbestemmelsene ikke pålegger varsling om at personprofilen er utarbeidet og hvorledes dette er gjort.

Personprofiler forutsetter for det første at den som utarbeider profilene har tilgang til personopplysninger (noe taushetspliktregler kan være til hinder for). For det andre må en slik bruk være i samsvar med kravene til formål i § 7. Endelig kan bestemmelsen om bruk av personopplysninger til nye formål ha betydning for muligheten til å utarbeide personprofiler, jf § 8.

§ 24 Varslingsplikt ved elektronisk overvåkning

Ved elektronisk overvåkning på offentlig sted eller arbeidssted skal det ved skilting eller på annen måte gjøres tydelig oppmerksom på at stedet blir overvåket og hvem som er behandlingsansvarlig.

Til § 24:

Bestemmelsen regulerer elektronisk overvåkning spesielt. Det er en forutsetning at overvåkningen er elektronisk behandling av personopplysninger slik lovforslaget nytter uttrykket, jf merknadene til § 3 ovenfor. Dette omfatter blant annet opptak som er digitalisert, dvs lagret i maskinlesbar form. Ettersom utvalget har kommet til at også visse andre former for overvåkning gjør det ønskelig å stille krav som nevnt i § 24, fremgår det uttrykkelig av § 4 at § 24 får anvendelse også på fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning. Se forøvrig "*Fjernsynsovervåkning og annen elektronisk overvåkning*" i kapittel 14.

Grunnen til at det her er gitt egne regler om varslingsplikt for elektronisk overvåkning er at de alminnelige reglene om varsling passer dårlig på denne typen elektronisk behandling. Det vil her ikke være noen direkte kontakt mellom den behandlingsansvarlige og de registrerte, og den behandlingsansvarlige vil ikke kjenne til de registrertes identitet. Dette gjør at regelen om individuelt varsel vanskelig kan gjennomføres.

Når det gjelder anvendelsen av bestemmelsen på fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning er regelen en videreføring av straffeloven § 390 b.

Hva som menes med «elektronisk overvåkning» fremgår av § 2 nr 6, se merknadene til denne bestemmelsen.

Varslingsplikten gjelder på «offentlig sted» og «arbeidssted». Uttrykkene skal forstås på samme måte som i straffeloven § 390 b.

"Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet" i Kapittel 4 Retting og sletting mv

§ 25 Plikt til å rette, slette, supplere og sperre mangelfulle personopplysninger

Dersom det er registrert personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å registrere, skal den behandlingsansvarlige sørge for at opplysningene rettes, slettes eller suppleres såfremt mangelen kan få betydning for den registrerte. Har mangelen ført til at det er gitt eller brukt slike opplysninger, skal den behandlingsansvarlige såvidt mulig sørge for at feilen ikke får betydning for den registrerte.

Dersom opplysningene på grunn av annen lovgivning ikke kan slettes eller rettes kan Datatilsynet gi pålegg om at opplysningene skal sperres for å forhindre at de blir brukt.

Til § 25:

Paragraf 25 regulerer den behandlingsansvarliges plikt til å rette, slette, supplere og sperre mangelfulle personopplysninger. Bestemmelsen er en videreføring og videreutvikling av personregisterloven § 8 og gjennomfører direktivet artikkel 6 nr 1 d). Se utvalgets merknader i 11.5.

Første ledd første punktum pålegger den behandlingsansvarlige å rette, slette eller supplere uriktige eller ufullstendige opplysninger eller opplysninger som det ikke er adgang til å ta inn i registeret såfremt mangelen kan få betydning for den registrerte. Det er gjort enkelte materielle endringer i forhold til den parallelle bestemmelsen i personregisterloven § 8. Tidligere praksis om når en mangel kan anses å få betydning for den registrerte, er relevant også for tolkningen av denne bestemmelsen. Historiske opplysninger, dvs opplysninger som er tatt ut av ordinær administrativ bruk, og opplysninger lagret for forskning- og statistikkformål vil som regel ikke fall inn under § 25, se Ot prp nr 2 (1977-78) side 76. Dette skyldes at mangel ved slike opplysninger sjelden vil ha betydning for den registrerte.

Den behandlingsansvarlige skal foreta retting, sletting eller supplering av eget tiltak. Det er ikke nødvendig med noe initiativ fra den registrertes side. I valget mellom å rette, slette eller supplere de mangelfulle personopplysningene må den behandlingsansvarlige ta hensyn til den registrertes og andre berørtes behov for å kunne dokumentere hva som har skjedd. Dersom den behandlingsansvarlige har gjort en feil som kan være erstatningsbetingende, kan det etter omstendighetene være rettsstridig å slette opplysningene for på den måten å hindre at den registrerte kan dokumentere grunnlaget for et eventuelt erstatningskrav.

Den behandlingsansvarlige skal etter første ledd annet punktum sørge for at feil som er begått, ikke får betydning for den registrerte. Av ordlyden i annet punktum går det frem at dette gjelder for alle typer feil, også dersom det er registrert opplysninger som det ikke er adgang til. Dette var uklart etter personregisterloven, selv om bestemmelsen ble tolket slik av Datatilsynet. Dersom den registrerte ikke er fornøyd med hva den behandlingsansvarlige gjør av eget tiltak eller etter henvendelse fra den registrerte, kan vedkommende bringe saken inn for Datatilsynet. Datatilsynet kan pålegge den behandlingsansvarlige å utføre tiltak som nevnt i første ledd første og annet punktum, jf § 40. Et slikt pålegg er imidlertid ikke avhengig av klage fra den registrerte.

Den behandlingsansvarliges plikt etter annet punktum er betinget av at dette er mulig («skal den behandlingsansvarlige såvidt mulig sørge for...»). Dette skal tolkes strengt. Den behandlingsansvarlige må akseptere betydelige kostnader for å rette opp en feil eller vil få (eller allerede har fått) betydning for den registrerte. Denne restitusjonsplikten er en av grunnene til at utvalget ikke har funnet det nødvendig å foreslå rett til erstatning for ikke-økonomisk tap (oppreisning), se "[Økonomiske og administrative konsekvenser av utvalgets forslag](#)" i kapittel 20.

Dersom opplysningene etter første ledd på grunn av annen lovgivning ikke kan slettes eller rettes, kan Datatilsynet gi pålegg om at opplysningene skal sperres for å forhindre at de blir brukt, jf *annet ledd*. Dette er nytt i forhold til personregisterloven i dag. «Sperring» kan innebære både et forbud mot å bruke opplysningene uten samtykke fra den registrerte, samt krav om å etablere nødvendige tekniske foranstaltninger for å hindre at opplysningene brukes. Aktuell lovgivning som kan forby sletting er for eksempel journalforskriften til legeloven som idag som den

store hovedregel forbyr sletting i pasientjournaler. Statsråd Gudmund Hernes har i Stortingets spørretime 9 april 1997 opplyst at det i ny lov om helsepersonell og ny lov om pasientrettigheter vil bli foreslått at det blir innført større muligheter til å få slettet uriktige opplysninger i journal.

§ 26 Sletting og sperring av personopplysninger

Den behandlingsansvarlige plikter, når det ikke lenger er saklig grunn for oppbevaring, å slette personopplysninger som behandles elektronisk eller som inngår eller skal inngå i et manuelt personregister. Med saklig grunn forstås blant annet at oppbevaring er pålagt i eller i medhold av lov eller at den behandlingsansvarlige behandler opplysningene til det formål de er innsamlet for.

Den registrerte kan, dersom dette ikke strider mot annen lov, likevel kreve slike opplysninger om seg selv sperret eller slettet dersom dette finnes forsvarlig ut fra en samlet vurdering av andres interesser, personverninteresser, samfunnsmessige interesser og den ressursinnsats som kravet forutsetter. Datatilsynet kan gi pålegg om slik sperring eller sletting. Slikt pålegg går foran bestemmelsene om kassasjon i lov 4 desember 1992 nr 126 om arkiv § 9.

Til § 26:

Paragraf 26 regulerer sletting og sperring av personopplysninger som ikke er mangelfulle. Bestemmelsen har ingen parallell i personregisterloven, men sletting av personregistre reguleres i Datatilsynets konsesjoner. Bestemmelsen, som gjennomfører direktivet artikkel 6 e og artikkel 14 nr 1, reiser tildels meget vanskelige avveiningsspørsmål. Mens personvern hensyn ofte kan tale for sletting av personopplysninger, kan andre tungtveiende samfunnshensyn som f.eks. muligheter til historieforskning og behovet for rettssikkerhet tilsi varsomhet med å slette mulig dokumentasjon. Bestemmelsen avveier disse interessene mot hverandre. Se forøvrig "*Plikt til å rette, slette og supplere*" i kapittel 11.5 og "*Tilgang til opplysninger m m*" i 18.2.3.3.

Første ledd første punktum pålegger den behandlingsansvarlige å slette visse former for personopplysninger når det ikke lenger er saklig grunn til å oppbevare disse. For det første omfattes personopplysninger som behandles elektronisk (f.eks. opplysninger som foreligger i maskinlesbar form, se nærmere om dette i merknadene til § 3 foran). For det andre omfatter slettingsplikten personopplysninger som inngår eller skal inngå i et manuelt personregister. Personopplysninger i manuelle saksmapper, som ikke utgjør noe personregister, omfattes ikke av bestemmelsen. Dette skyldes at slike opplysninger ikke omfattes av lovens virkeområde, jf § 3.

I visse tilfeller kan det være tvil om behandlingen er delvis elektronisk eller manuell. Dette er drøftet nærmere i merknadene til § 3 ovenfor.

Hva som menes med saklig grunn er eksemplifisert i første ledd annet punktum. Eksempler på lovgivning som pålegger plikt til å oppbevare personopplysninger er regnskapslovgivning og arkivregelverk.

I enkelte særlige tilfelle kan varetakelsen av personveninteresser begrunne tiltak som gjør at personopplysninger blir utilgjengelige. *Annet ledd* regulerer disse tilfellene ved at det gir den registrerte en rett til å kreve seg slettet så fremt visse forutsetninger er tilstede. Det må etter en konkret bedømmelse finnes forsvarlig at personverninteresser går foran andre interesser. De andre interessene det er snakk om, kan for det første være interessen andre enkeltpersoner har i å kunne fremskaffe dokumentasjon (rettssikkerhetsbehov). At A krever opplysninger om seg selv slettet

eller sperret, kan føre til at B mister muligheten til f.eks. å dokumentere et rettskrav. Også mer generelle samfunnsmessige interesser må tas i betraktning, som f.eks. hensynet til fremtidig historieforskning. Vurderinger av om kravet om sletting eller sperring skal gjennomføres bør således omfatte både eksisterende og sannsynlige fremtidige interesser. Dersom det skulle være uenighet mellom den registrerte og den behandlingsansvarlige om det er grunnlag for å kreve sletting, gir loven Datatilsynet kompetanse til å treffe en avgjørelse og eventuelt gi pålegg om sletting. Slettingen eller sperringen kan bestå i at opplysningene gjøres utilgjengelig eller at det treffes tiltak slik at opplysningene ikke lenger omfattes av lovens saklige virkeområde.

Det er en forutsetning at kravet om sletting ikke strider mot annen lovgivning. Utvalget foreslår i den forbindelse å videreføre prinsippet i arkivloven § 9 d om at Datatilsynets slettingsvedtak i medhold av personregisterloven §§ 8 og 11 går foran arkivlovens generelle bestemmelser om kassasjon, se annet ledd siste punktum.

§ 27 Rett til å kreve manuell behandling av personopplysninger

Den som en avgjørelse retter seg mot eller som saken ellers direkte gjelder, kan kreve at personopplysningene behandles manuelt dersom avgjørelsen

1. er en enkeltavgjørelse som definert i § 2 nr 9 eller som på annen måte har vesentlig betydning for vedkommende, og
2. fullt ut er basert på automatisk behandling, og
3. karakteriserer personlige egenskaper.

Retten til å kreve en manuell behandling som nevnt i første ledd gjelder ikke dersom det er truffet tilstrekkelige tiltak for å ivareta vedkommendes personverninteresser, og

1. avgjørelsen er hjemlet i lov, eller
2. avgjørelsen knytter seg til inngåelse eller oppfyllelse av kontrakt.

Til § 27:

Paragraf 27 gir den registrerte rett til å kreve manuell avgjørelse, jf direktivet artikkel 15 nr 1. Som det fremgår av utvalgets vurderinger i 11.3.2, dreier det seg om en regel med et meget begrenset anvendelsesområde. Som det fremgår nærmere av 11.3.2 kan det imidlertid tenkes at bestemmelsen vil bli mer praktisk i fremtiden.

Et første vilkår for at bestemmelsen skal gjelde er at det foreligger en enkeltavgjørelse som nevnt i § 2 nr 9.

For det annet må den foreliggende beslutningen utelukkende være basert på automatisk behandling. I dette ligger at beslutningsprosessen kun skjer i et datamaskinsystem. Dersom et eller flere mennesker tar del i beslutningsprosessen, f.eks. ved å tolke resultatet av datamaskinbehandlingen, er ikke dette vilkåret oppfylt. Den manuelle delen av behandlingen må imidlertid være reell, og nedfelt i fullmakter eller praksis.

Dersom beslutningen i tillegg karakteriserer personlige egenskaper, som f.eks. personlige ferdigheter, evner eller karaktertrekk, kan den registrerte kreve at beslutningen overprøves manuelt. Dersom f.eks. bankene benytter «bankkiosker» hvor det kan søkes om lån, vil kunden via en kundeterminal kunne kreve at «systemets» avgjørelse etterprøves av ansatte i banken.

Fra dette utgangspunktet gjøres imidlertid unntak i annet ledd som kan føre til at bestemmelsens rekkevidde reduseres betydelig. Retten til å kreve manuell vurdering gjelder ikke der beslutningen enten er hjemlet i lov, eller knytter seg til

inngåelse eller oppfyllelse av kontrakt. Bestemmelsen får ikke anvendelse på «bankkiosk»-eksemplet ovenfor dersom det er truffet tiltak for å vareta den registrertes personverninteresser – f eks ved at den registrerte gis rett til å uttale seg før avgjørelsen treffes. Datatilsynet har kompetanse til å avgjøre om personverntiltakene er tilstrekkelige, jf § 40. Hvor strenge krav som stilles til personverntiltakene, vil ha avgjørende betydning for hvor stor virkning bestemmelsen vil få.

§ 28 Rett til å kreve sitt navn sperret mot bruk i markedsføringsøyemed

Kongen kan gi forskrift om at det skal opprettes et sentralt reservasjonsregister samt nærmere regler for registeret.

Den registrerte kan kreve sitt navn sperret mot bruk til direkte markedsføring. Sperring kan kreves både i det sentrale reservasjonsregisteret og i markedsførers adresseregister.

En behandlingsansvarlig som markedsfører direkte plikter å oppdatere adresseregisteret i henhold til det sentrale reservasjonsregisteret før første gangs utsendelse og minst to ganger pr år. Kongen kan i forskrift gjøre unntak fra denne plikten.

Mottakere av direkte reklame skal få opplyst hvem som har oppgitt personopplysningene som ligger til grunn for henvendelsen.

Denne bestemmelsen gjelder ikke for markedsføring av egne produkter fra den behandlingsansvarlige hvor den registrerte har et løpende kundeforhold.

Til § 28:

Paragraf 28 gir den registrerte rett til å kreve sitt navn sperret mot bruk i markedsføringsøyemed. Bestemmelsen er en videreføring av personregisterloven §§ 8a og 28 første ledd. Paragrafen gjennomfører direktivet artikkel 14 b). Nytt for bestemmelsen er at den i tillegg etablerer en plikt for den behandlingsansvarlige til å oppdatere sitt adresseregister i henhold til det sentrale reservasjonsregisteret minst to ganger pr år. Se utvalgets merknader i 11.3.1.3.

Bestemmelsen forutsetter i *første ledd* at det opprettes et sentralt reservasjonsregister, noe regjeringen etter det utvalget erfarer allerede arbeider med. I første ledd gis også hjemmel til å gi nærmere forskrift om et slikt register. Forskriftshjemmelen er utformet slik at den gir en mulighet til å gi forskrift om registeret, men er ikke til hinder for at registeret forankres i annet regelverk enn lovforslaget her dersom dette anses ønskelig. For eksempel kan det være hensiktsmessig at nærmere regler om registeret gis i markedsføringsloven og eventuelt forskrift til denne loven.

Den registrerte kan kreve sitt navn sperret mot bruk til direkte markedsføring, jf *annet ledd* første punktum. Dette omfatter all adressert reklame (i postkasse, på telefaks og e-post), samt telefonsalg. Telefonsalg er ikke omfattet av ordlyden i personregisterloven § 8a («utsending av direkte reklame og liknende publikasjoner»), og dette er bakgrunnen for at ordlyden er endret i § 28. Med «direkte markedsføring» menes direkte henvendelser til enkeltpersoner med det formål å selge varer eller tjenester. Rene vervekampanjer, f eks i regi av idelle organisasjoner, vil sjelden være «markedsføring» slik denne loven nytter ordet.

Sperring kan kreves både i det sentrale reservasjonsregisteret og i markedsførers adresseregister, jf *annet ledd* annet punktum. Den behandlingsansvarliges plikt til å oppdatere adresseregisteret i henhold til det sentrale reservasjonsregisteret er begrenset til to ganger pr år, jf *tredje ledd*, og det kan derfor være ønskelig for enkelte også å kunne reservere seg direkte hos den som markedsfører.

Plikten til å oppdatere adresseregisteret i henhold til det sentrale reservasjonsregisteret gjelder generelt, både for adresserings- og distribusjonsforetak (etter personregisterloven § 25) som forestår markedsføring for andre og for eksempel for idrettsklubber eller som driver med telefonsalg for å skaffe inntekter til klubben. Den vil også gjelde for ulike støtteforeninger og lignende som selger skrapelodd eller annet til støtte for ulike formål. Det vil således ikke være adgang til å bruke telefonkatalogen som kilde ved telefonsalg med mindre det i denne fremgår hvilke abonnenter som har reservert seg mot slik markedsføring. Plikten påhviler den behandlingsansvarlige. Forskriftshjemmelen gir Kongen mulighet til å gjøre unntak for enkelte grupper fra plikten til å oppdatere adresseregisteret i henhold til det sentrale reservasjonsregisteret. For eksempel kan det være aktuelt å gjøre unntak for ideelle organisasjoner og foreninger som markedsfører direkte i beskjedent omfang.

Mottakere av direkte reklame skal få opplyst hvem som har oppgitt personopplysningene som ligger til grunn for henvendelsen, jf *fjerde ledd*. Loven fastsetter med andre ord obligatorisk kildemerking for adressert reklame, samt pålegger de som markedsfører via telefon å opplyse hvem som er kilde for personopplysningen. Bestemmelsen lovfester Datatilsynets praksis som setter dette som vilkår i sine konsesjoner for adresserings- og distribusjonsforetak. Etter personregisterloven § 28 første ledd annet punktum kan en registrert *kreve å få opplyst* hvem som er foretakets kilde for registreringer, men har ingen rett til å få dette automatisk.

Bestemmelsen gjelder ikke for markedsføring av egne produkter når mottakeren har et løpende kundeforhold hos den behandlingsansvarlige, jf *femte ledd*. Hva som skal til for at det skal foreligge et løpende kundeforhold må vurderes på bakgrunn av hvilken bransje og hvilke varer eller tjenester det dreier seg om. Typiske eksempler på løpende kundeforhold er langvarige avtaleforhold som f.eks. avtale om banklån og livsforsikring.

"Personregisterloven med forskrifter" i Kapittel 5 Videregivelse av personopplysninger til utlandet

§ 29 Vilkår for videregivelse av personopplysninger til utlandet – hovedregel

Videregivelse av personopplysninger til utlandet kan bare skje dersom staten som mottakeren skal behandle personopplysningene i regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte. Stater som har gjennomført direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, oppfyller kravet til tilstrekkelig forsvarlig regulering.

I vurderingen av om stater som ikke har gjennomført direktiv 95/46/EF regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte, skal det bli lagt vekt på opplysningenes art, de planlagte behandlingenes formål og varighet, den aktuelle statens rettsregler om behandling av personopplysninger, regler for god forretningsskikk og sikkerhetsforanstaltninger hos mottakeren. Det skal også legges vekt på om den aktuelle staten har tiltrådt Europarådets konvensjon 28 januar 1981 nr 108.

Til § 29:

Paragraf 29 gir hovedregelen for videregivelse av opplysninger til utlandet, jf direktivet artikkel 2 og artikkel 25 og utvalgets vurderinger i *"Overføring av personopplysninger til utlandet"* i kapittel 16. Videregivelse av opplysninger til utlandet reguleres i dag av personregisterloven kapittel 9. Her som andre steder i loven knytter

«behandling av personopplysninger» seg til enten elektronisk behandling eller manuell behandling av personopplysninger som inngår eller skal inngå i et personregister. Dette er for enkelhets skyld ikke sagt uttrykkelig i § 29, men følger av § 3. Se "*Utvalgets vurderinger*" i kapittel 16.4.

Verken direktivet eller lovforslaget regulerer videregivelse av personopplysninger når dette har rent personlige formål, jf § 3.

Publisering av personopplysninger ved hjelp av internasjonale kommunikasjonskanaler som f.eks. Internett kan regnes som videregivelse av personopplysninger til utlandet. Slik videregivelse vil ofte være unntatt fra reguleringen i §§ 29 og 30, jf lovforslaget § 5 som gjennomfører direktivet artikkel 9.

I tråd med direktivet artikkel 25 er det et vilkår for videregivelse av opplysninger til utlandet at staten som mottakeren befinner seg i regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte, jf § 29 *første ledd*. Direktivets krav til «fri utveksling» av personopplysninger (jf presiseringene i 16.4.1) i artikkel 2 varetas ved at stater som har gjennomført direktivet skal anses for å tilfredsstillere kravet til tilstrekkelig forsvarlig regulering. Dette vil typisk være stater innenfor EØS-området. Den lovtekniske løsningen utvalget har valgt innebærer imidlertid at en stat innenfor EØS-området som ikke har gjennomført direktivet i tilstrekkelig grad ikke uten videre anses for å tilfredsstillere kravet til tilstrekkelig forsvarlig regulering. På den annen side vil en stat utenfor EØS-området som på eget initiativ gjennomfører EF-direktivet av den grunn anses for å tilfredsstillere kravet til tilstrekkelig forsvarlig regulering.

For stater som ikke har gjennomført direktivet, vil det bero på en helhetsvurdering om kravet til tilstrekkelig forsvarlig behandling av personopplysninger er oppfylt. Paragraf 29 *annet ledd* gir en ikke-uttømmende oppregning av momenter som skal vektlegges i denne vurderingen. Avklaring mht. hvilke stater som oppfyller dette kravet vil komme relativt raskt blant annet på grunnlag av Kommisjonens aktive rolle på dette området, se direktivet artikkel 25 nr 3 – 7. Den behandlingsansvarlige kan få veiledning ved å henvende seg til Datatilsynet.

§ 30 Videregivelse av personopplysninger til stater som ikke regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte

Videregivelse av personopplysninger til utlandet kan skje selv om den aktuelle staten ikke regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte dersom

1. den registrerte har gitt sitt samtykke til videregivelsen
2. Norge har plikt til å foreta slik videregivelse etter folkerettslig overenskomst eller som følge av medlemskap i internasjonal organisasjon
3. det er fastsatt i lov at det er adgang til å videregje opplysningene
4. videregivelsen er nødvendig for å inngå eller oppfylle en kontrakt mellom den registrerte og den behandlingsansvarlige
5. videregivelsen er nødvendig for å inngå eller oppfylle en kontrakt i den registrertes interesse
6. videregivelsen er nødvendig for å beskytte den registrertes vesentlige interesser.

Dersom særlig grunner taler for det, kan Datatilsynet tillate videregivelse selv om vilkårene i første ledd ikke er oppfylt.

Kongen kan gi forskrift om videregivelse av personopplysninger til tredjeland.

Til § 30:

Etter § 29 kan personopplysninger bare videregis til mottakere i stater som regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte. I tråd med direktivet artikkel 26 gjøres det imidlertid i § 30 unntak fra denne regelen slik at videregivelse i visse tilfelle kan skje selv om staten som mottakeren befinner seg i ikke tilfredsstillende kravet i § 28 (jf 16.4.2.2 foran). Her som andre steder i loven knytter «behandling av personopplysninger» seg til enten elektronisk behandling eller manuell behandling av personopplysninger som inngår eller skal inngå i et personregister. Dette er for enkelthets skyld ikke sagt uttrykkelig i § 30, men følger av § 3.

Det første unntaket gjelder der den registrerte har samtykket i videregivelsen (jf direktivet artikkel 26 nr 1 bokstav a). Samtykket må være informert og uttrykkelig, jf § 2 nr 7 og merknadene til denne bestemmelsen.

For det andre kan videregivelse finne sted dersom Norge i henhold til folkerettslig overenskomst eller som følge av medlemskap i en internasjonal organisasjon har plikt til å gi personopplysningene videre (jf direktivet artikkel 26 nr 1 bokstav d). Regelen er en videreføring av personregisterforskriften § 8-1 annet ledd.

Det tredje unntaket som oppstilles i § 30 er der det i lov er fastsatt at det er adgang til å videregje opplysningene (jf direktivet artikkel 26 nr 1 bokstav d). Hvorvidt det foreligger tilstrekkelig lovhjemmel for videregivelse vil bero på en tolking av den aktuelle lovbestemmelsen. Hvor strenge krav som må stilles til klar lovhjemmel vil blant annet være avhengig av hvilke virkninger videregivelsen har for den registrerte. Jo større virkninger overføringen kan få, jo klarere må lovhjemmelen være for at unntaket i nr 3 skal få anvendelse.

For det fjerde gjøres unntak fra kravet om tilstrekkelig forsvarlig regulering når videregivelsen av personopplysningene er nødvendig for å inngå eller oppfylle en kontrakt mellom den registrerte og den behandlingsansvarlige (jf direktivet artikkel 26 nr 1 bokstav b). Unntaket kan ha en viss selvstendig betydning ved siden av samtykke-unntaket i nr 1 (se § 2 nr 7 om de strenge kravene til samtykke). Å inngå en kontrakt (eller starte kontraktsforhandlinger) innebærer med andre ord at personopplysninger kan videregis til utlandet uansett om den registrerte eksplisitt har samtykket i videregivelsen (såfremt videregivelsen er nødvendig for å oppfylle kontrakten).

Et typisk eksempel som omfattes av unntaket er at den registrerte ønsker å inngå eller oppfylle kjøpsavtale med en selger i et annet land, og som av den grunn må gi fra seg navn, adresse m m til selgeren i utlandet.

Unntaket i nr 5 gjør det mulig å videregje personopplysninger til utlandet selv om staten som mottakeren befinner seg i ikke fyller vilkåret i § 28 dersom videregivelsen er nødvendig for å inngå eller oppfylle en kontrakt i den registrertes interesse (jf direktivet artikkel 26 nr 1 bokstav c). I motsetning til unntaket i nr 4 er det her ikke krav om at den registrerte selv er part i kontrakten, som typisk vil være inngått mellom den behandlingsansvarlige og en tredjemann. Det kreves imidlertid at kontrakten er i den registrertes interesse, dvs at kontrakten må ha en viss positiv betydning for den registrerte. Interesse henspiller ikke bare på rettigheter, men kan også være oppfylt ved at avtaleinngåelsen fører med seg visse positive faktiske konsekvenser for den registrerte. Det må kunne dokumenteres at kontrakten får slike virkninger for bestemte personer.

I nr 6 gjøres unntak fra § 29 dersom videregivelsen er nødvendig for å beskytte den registrertes vesentlige interesser. Vesentlighetsvilkåret må fortolkes strengt.

"Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern" i Kapittel 6 Meldeplikt og konsesjonsplikt m v

§ 31 Meldeplikt

Enhver behandlingsansvarlig som benytter elektroniske systemer for behandling av personopplysninger skal gi melding til Datatilsynet på fastsatt skjema i god tid før behandlingen tar til.

Slik melding skal også sendes ved opprettelse av et manuelt personregister dersom det skal inneholde sensitive personopplysninger, jf § 2 nr 8.

Meldeplikten gjelder ikke for behandlinger som utelukkende gjør bruk av allment tilgjengelige personopplysninger.

Kongen kan gi forskrift om at visse typer behandlinger skal være unntatt fra meldeplikten etter første og annet ledd, underlagt en forenklet meldeplikt eller underlagt konsesjonsplikt. For behandlinger som unntas fra meldeplikt kan det gis forskrift om forhold som nevnt i § 35 annet ledd. Det kan også gis forskrift for å begrense de ulemper behandlingen ellers kunne medføre for den enkelte.

Til § 31:

Bestemmelsen har som lovteknisk utgangspunkt meldeplikt for all elektronisk behandling av personopplysninger, samt for opprettelse av manuelle personregistre dersom registeret skal inneholde sensitive personopplysninger, se utvalgets merknader i 12.5.4 og direktivet artikkel 18. Fra dette utgangspunktet gjøres unntak i tredje ledd og i forskrift i medhold av fjerde ledd. Behandlinger for rent personlige formål er ikke omfattet av meldeplikten, jf § 3.

Første ledd pålegger den behandlingsansvarlige som benytter elektroniske systemer for behandling av personopplysninger å gi melding om dette til Datatilsynet. Paragraf 32 bestemmer hva en slik melding skal inneholde. Meldingen sendes i utgangspunktet bare én gang – ikke hver gang man behandler personopplysninger elektronisk. Det er med andre ord behandlingsmåten – systemet for behandling – som skal meldes.

Dersom det senere oppstår endringer i de behandlingene man foretar i forhold til de opplysningene som er oppgitt på meldingen, må ny melding sendes med oppdaterte opplysninger, jf § 31 tredje ledd. Det må derfor sendes ny melding dersom det for eksempel skal behandles nye typer opplysninger eller opplysningene skal utleveres eller gjøres tilgjengelig på en annen måte enn oppgitt i den opprinnelige meldingen.

Det vil også være aktuelt å unnta en del behandlinger fra meldeplikt (slik det i dag er gjort unntak fra konsesjonsplikt), se nærmere om dette nedenfor. Målsettingen er (jf *"Regulering og kontroll"* i kapittel 12) at meldeplikten sammen med konsesjonsplikten skal være like omfattende som dagens konsesjonsplikt, og forskriftsregulering vil være nødvendig for å oppnå dette.

Avgrensningen av meldeplikten vil etter dette i utgangspunktet være ganske lik avgrensningen av konsesjonsplikten etter personregisterloven § 9, med den forskjell at konsesjonsplikten er knyttet til opprettelsen av personregistre mens meldeplikten etter den nye loven er knyttet til behandling av personopplysninger som nevnt i § 3 (jf fjerde ledd som gir forskriftshjemmel til å innsnevre meldeplikten).

Tredje ledd unntar fra meldeplikt behandlinger som «utelukkende gjør bruk av allment tilgjengelige personopplysninger». Det betyr at personopplysninger som er gjort allment tilgjengelig kan leses, søkes i, nedlastes, lagres, videregis mv uten at

dette utløser meldeplikt. Slike operasjoner kan imidlertid utgjøre en elektronisk behandling av personopplysninger og vil i så fall være regulert av lovens øvrige bestemmelser.

At opplysninger er gjort «allment tilgjengelig» innebærer at hvem som helst kan be om innsyn i opplysningene uten at det stilles særskilte krav om saklig grunn eller lignende hos vedkommende. Det er ikke tilstrekkelig at opplysningene er gjort tilgjengelig for en begrenset krets av personer. Dersom opplysningene på en eller annen måte er publisert (for eksempel lagt ut på Internett) vil opplysningene være allment tilgjengelig. Det samme vil være tilfelle dersom det tilbys innsyn i opplysningene for enhver mot betaling (for eksempel opplysninger registrert i Brøn-nøysundregistrene). At opplysninger er allment tilgjengelig sier ikke nødvendigvis noe om hvor sensitive opplysningene er. For eksempel kan en biografi inneholde opplysninger om en persons helse, men disse sensitive opplysningene vil være allment tilgjengelig.

Det er krav om at man i behandlingen utelukkende gjør bruk av allment tilgjengelige opplysninger. Dersom opplysningene skal sammenstilles og benyttes sammen med andre personopplysninger som ikke er allment tilgjengelig, vil hele behandlingen være meldepliktig etter hovedregelen.

Det vil være behov for at visse typer behandlinger unntas fra meldeplikten. Dette kan fastsettes i forskrift, jf *fjerde ledd*. Dette vil først og fremst gjelde behandlinger som omfatter lite sensitive personopplysninger og som ellers må anses kurante ved at det for eksempel er godt kjent blant de fleste at slike behandlinger foretas. Det kan også i forskrift fastsettes at visse behandlinger skal være unntatt fra meldeplikt og i stedet underlagt konsesjonsplikt etter § 33. Unntakene i personregisterforskriften kan gi en viss veiledning mht hvilke unntak som bør gjøres i forskrift. Det kan også være hensiktsmessig at høringsinstansene gjøres særskilt oppmerksom på problemstillingen. Det kan være aktuelt å vurdere om enkelte offentlige organer bør undergis en forenklet meldeplikt.

Meldingen skal sendes på fastsatt skjema i god tid før behandlingen tar til. Hva som er å anse som «god tid» vil variere ut i fra hvor omfattende persondatabehandlingen skal være. Dette må i utgangspunktet bero på den behandlingsansvarliges eget skjønn. En behandling som omfatter opplysninger om et stort antall personer, samlet inn fra en rekke forskjellige kilder bør imidlertid meldes tidligere enn en mindre behandling som kun omfatter opplysninger om noen få personer samlet inn fra disse personene selv. Det samme gjelder dersom behandlingen omfatter svært sensitive opplysninger. Utvalget antar at en slik variasjon med hensyn til tidspunktet for når melding skal sendes ikke vil bli problematisk i praksis. Store omfattende behandlinger vil være planlagt i god tid av den behandlingsansvarlige og det vil være i dennes interesse å komme i en tidlig dialog med Datatilsynet for eventuelt å gjøre nødvendige tilpasninger i systemet. Dette behovet blir mindre for ikke-sensitive persondatabehandlinger.

Behandlingen kan starte når melding er sendt. Meldingen er en informasjonsbærer, og ingen konsesjonssøknad. Det er ikke nødvendig å vente på et eventuelt svar fra Datatilsynet, slik tilfellet er etter dagens konsesjonsordning. Datatilsynet kan imidlertid i etterkant stoppe en ulovlig behandling eller stille vilkår for at behandlingen kan fortsette, jf § 40.

I *annet ledd* bestemmes at melding som omtalt ovenfor også skal sendes ved opprettelse av et manuelt personregister dersom det skal inneholde sensitive personopplysninger, se utvalgets merknader til § 2 nr 8 om disse opplysningskategoriene.

Datatilsynet vil ha behov for oversikt over overføringer av personopplysninger til utlandet (jf utvalgets vurderinger i 16.4.2.4). Denne informasjonen vil fremgå av den alminnelige meldeplikten i § 31. Dersom det opprinnelig ikke var tale om å gi

opplysningene videre til utlandet, men dette senere viser seg å være ønskelig, vil det være plikt til å gi ny og ajourført melding. Datatilsynet vil imidlertid på bakgrunn av den informasjonen meldingen gir kunne gripe inn og stanse videregivelse dersom lovens vilkår for videregivelse ikke er oppfylt. Dette er utslag av den generelle etterfølgende kontrollkompetansen Datatilsynet er gitt i medhold av § 40.

§ 32 Meldingens innhold

Meldingen skal inneholde opplysninger om

1. navn og adresse på den behandlingsansvarlige og på dennes eventuelle representant, jf § 6
2. hvem som har det daglige ansvaret for å oppfylle pliktene som hviler på den behandlingsansvarlige
3. behandlingens formål
4. definisjoner og andre beskrivelser av de typer personopplysninger som inngår i behandlingen
5. kildene for personopplysningene
6. grunnlaget for innhenting av opplysningene
7. hvem personopplysningene blir eller vil bli utlevert til
8. planlagt utlevering av personopplysningene til mottakere i andre stater, og
9. hvilke sikkerhetstiltak som er knyttet til behandlingen.

Kongen kan gi forskrift om hvilke opplysninger meldingene skal inneholde, samt regler om gjennomføringen av meldepliktsordningen.

Den behandlingsansvarlige er ansvarlig for at det til enhver tid er innsendt melding som gir riktige opplysninger. Ny melding med oppdaterte opplysninger skal sendes etter 3 år, med mindre det i løpet av denne tiden er sendt endringsmelding. Kongen kan gi forskrift som skal sikre meldingenes kvalitet og kan for enkelte typer av behandlinger fastsette andre regler for når ny melding skal sendes.

Til § 32:

Paragraf 32 angir hvilke opplysninger meldingen minst skal inneholde. Se utvalgets merknader i 12.5.4.3 og direktivet artikkel 19.

Det vil være nødvendig å supplere og detaljere de opplysningene som er regnet opp i bestemmelsen i forskrift, jf *annet ledd*. Slik forskrift bør tre i kraft sammen med loven for at meldeplikten skal få den funksjonen den er tiltenkt. Det kan for eksempel være nødvendig for Datatilsynet å få opplysninger om måten opplysningene blir innhentet på, hvilken informasjon som gis til de det innsamles opplysninger om mv. Det er mulig at meldeskjemaene bør differensieres noe slik at man ved mindre omfattende behandlinger kan gi færre opplysninger.

På samme måte er det behov for i forskrift å regulere nærmere gjennomføringen av meldepliktordningen, se 12.5.4.4 og 20.3.2.

Etter *tredje ledd* er den behandlingsansvarlige ansvarlig for at det til enhver tid er innsendt melding som gir riktige opplysninger. Det betyr at det må sendes ny melding for eksempel dersom behandlingen er avsluttet, nye opplysninger samles inn eller opplysningene skal utleveres til andre enn opprinnelig angitt. Det krever også ny melding dersom opplysningene skal anvendes til et annet formål. Slik ny anvendelse forutsetter dessuten at vilkårene i § 7 er oppfylt. Dersom det ikke er meldt endringer i forhold til den opprinnelige meldingen, skal ny melding sendes etter 3 år. Fristen avbrytes med andre ord ved at det sendes en endringsmelding og ny 3 års frist begynner deretter å løpe. Dette innebærer at opplysningene på

meldeskjemaene aldri skal være eldre enn 3 år, hvilket har stor betydning for opplysningenes kvalitet. Datatilsynet har på bakgrunn av dette mulighet til å rette en henvendelse til de behandlingsansvarlige (med fordel kan slike henvendelser genereres automatisk fra Datatilsynets system) som har oversittet 3 års-fristen, og på denne måten avklare om dette skyldes en forglemmelse, at behandlingen er avsluttet eller at virksomheten er opphørt. Opphør av behandlingen vil ikke utløse ny meldeplikt dersom det i den opprinnelige medlingen er oppgitt når behandlingen vil avslutte.

§ 33 Konesjonsplikt

Det kreves samtykke fra Datatilsynet (konesjon) for å behandle sensitive personopplysninger (jf § 2 nr 8) når formålet med behandlingen er å treffe enkeltavgjørelser som definert i § 2 nr 9.

Kongen kan gi forskrift om at visse typer behandlinger skal være unntatt fra konsesjonsplikten etter første ledd, og i stedet underlagt meldeplikt etter § 31. For slik behandling skal det gis forskrift om forhold som nevnt i § 35 annet ledd. Det kan også gis forskrift for å begrense de ulemper behandlingen ellers kunne medføre for den enkelte.

Til § 33:

Paragraf 33 angir hvilke persondatabelandlinger som er konsesjonspliktige. Konsesjonsplikten innsnevres vesentlig i forhold til personregisterloven § 9 første ledd. Etter direktivet artikkel 20 kan persondatabelandlinger som innebærer «særlige risiko» for personers rettigheter og friheter underlegges konsesjonsplikt. Behandlingene som omfattes av § 33 antas å innebære en slik særlig risiko, se utvalgets merknader i 12.5.5. Konsesjonsplikten er knyttet til en bestemt bruk av sensitive personopplysninger, nemlig at det treffes avgjørelser som typisk har stor betydning for den enkelte, jf *første ledd*. Hva som menes med «enkeltavgjørelser», fremgår av § 2 nr 9 og merknadene til denne bestemmelsen.

Utvalget legger ved avgrensningen av konsesjonsplikten større vekt på det beslutningsfokuserede personvernet (jf 3.3.4) enn det som ble lagt til grunn ved utarbeidelsen av personregisterloven (som i større grad baserer seg på en teknologiahengig avgrensning av konsesjonsplikten).

Behandling av sensitive opplysninger forutsetter at et av vilkårene i § 9 er oppfylt. Kravet om konsesjon gjelder i tillegg til vilkårene i § 9 dersom den elektroniske behandlingen av sensitive personopplysninger skjer med det formål å treffe enkeltvedtak eller andre enkeltavgjørelser som er bestemmende for bestemte private personers rettigheter eller plikter. Konsesjonsplikten gjelder bare for manuell behandling av sensitive personopplysninger i den grad det opprettes et manuelt personregister med det formål å treffe avgjørelser som definert i § 2 nr 9 (jf lovens anvendelsesområde, se § 3).

Kravet om konsesjon for å behandle sensitive personopplysninger når formålet er å treffe enkeltvedtak, jf første ledd, innebærer at deler av forvaltningens virksomhet vil være konsesjonspliktig etter denne bestemmelsen. Utvalget er klar over at det kan virke kunstig å kreve konsesjon når det er lovbestemt at behandling skal skje. I og med at behandlingsbegrepet er så vidt, kan det imidlertid vanskelig tenkes at alle elementene i behandlingsbegrepet vil være regulert i loven. Det vil derfor ut fra personvern hensyn være behov for at Datatilsynet kommer inn og setter vilkår om dette på forhånd. At det er konsesjonsplikt i disse tilfellene innebærer primært at Datatilsynet kontrollerer disse behandlingene *før* behandlingen iverksettes i motsetning til

den etterkontrollen som ville være mulig dersom behandlingene «bare» var underlagt meldeplikt. Konesjonsbehandlingen må betraktes som en forhåndskontroll av at forvaltningens virksomhet tilfredsstillende grunnleggende krav til personvern, og ikke som en mulighet for Datatilsynet til å nekte forvaltningen å utføre oppgaver som det i lov og budsjettvedtak etc er forutsatt at forvaltningen skal utføre. Etter personregisterloven er «personregistre i organ for stat eller kommune opprettet ved lov» fritatt fra konsesjonsplikt, jf § 41. Det er sikker rett at det er *registeret* og ikke *organet* som skal være opprettet ved lov. Unntaket er ikke videreført i den nye loven. Mange av de registrene som er fritatt fra konsesjonsplikt etter personregisterloven § 41 vil ikke være omfattet av konsesjonsplikten etter den nye loven § 33, fordi registrene ikke opprettes med det formål å treffe enkeltvedtak. Og når offentlige myndigheter treffer enkeltvedtak på grunnlag av sensitive personopplysninger, er det ønskelig at Datatilsynet i forkant vurderer den behandlingen av personopplysninger som skal skje og eventuelt setter vilkår der dette er nødvendig, for eksempel knyttet til sikkerheten.

Konesjonsplikten etter § 33 gjelder bare dersom sensitive personopplysninger inngår og behandlingen skjer med det formål å treffe avgjørelser som er bestemmende for privates «rettigheter eller plikter», jf § 2 nr 9. Ved tolkningen av begrepet må man også her se hen til hvordan begrepet er tolket etter forvaltningsloven. Ordet «rettighet» er tolket i relativt vid mening slik at for eksempel tildeling av akademiske grader (i den grad det er utøving av offentlig myndighet) er enkeltvedtak selv om det ofte ikke er tale om annen «rett» enn adgang til å bruke tittelen, se Frihagen, Forvaltningsrett II, side 74. Helt uvesentlige bånd som legges på den enkelte faller imidlertid utenfor. Dette vil for eksempel være tilfelle for ordensregler som iverksettes på arbeidsplassen. Etter forvaltningsloven § 2 annet ledd regnes «[a]vgjørelse som gjelder ansettelse, oppsigelse, suspensjon, avskjed eller forflytning av offentlig tjenestemann», som enkeltvedtak. Det er naturlig at «enkeltavgjørelse» i § 33 forstås på samme måte overfor ansatte i det private næringslivet. Dette innebærer i så tilfelle at personalregistre vil være konsesjonspliktig etter bestemmelsen (slik personalregistre også er etter personregisterloven § 9 i dag). Utvalget antar at det på dette området bør utarbeides forskrift som unntar personalregistre fra konsesjonsplikt.

Generelt vil tildeling av ulike typer «knapphetsgoder» (sykehusplass, barnehageplass, skoleplass mv) anses som avgjørelser som er bestemmende for privates rettigheter eller plikter. Likeens innvilgelse av lån eller avtale om forsikring. Mange behandlinger av personopplysninger omfatter imidlertid sjelden sensitive personopplysninger, og vil av den grunn ikke være konsesjonspliktig.

Avgjørelsen må være avgjørende for «bestemte» private personers rettsstilling. Tolkningen her vil bli den samme som forvaltningsloven. Det avgjørende vil i utgangspunktet være om vedkommende avgjørelse er rettet mot en ubestemt krets eller mot en eller flere bestemte personer. Man kan imidlertid ikke bare se på avgjørelsens ordlyd, men må i vurderingen ta hensyn til hvordan avgjørelsen reelt sett får virkning. Dersom avgjørelsen etter sitt innhold og de konkrete omstendigheter tar sikte på en bestemt eller noen få bestemte personer, må den anses som det selv om ordlyden er generelt utformet. Konesjonsplikten avhenger av formålet med behandlingen. Det er i den sammenheng det reelle formålet som er avgjørende. Den behandlingsansvarlige kan ikke «komme seg unna» konsesjonsplikten ved å oppgi et formål som ikke er konsesjonspliktig. Datatilsynet kan med hjemmel i § 40 jf § 7 kreve en presisering av formålsangivelsen. Formålsangivelsen vil dessuten være avgjørende for anvendelsen av personopplysningene, jf §§ 7 og 8.

Elektronisk overvåking vil i noen tilfeller være konsesjonspliktig avhengig av formålet med overvåkingen (om formålet er å treffe en avgjørelse som definert i §

2 nr 9 på grunnlag av sensitive personopplysninger). Dersom det igangsettes elektronisk overvåkning av et arbeidssted med det formål å avdekke om arbeidstagerne bryter sine plikter etter ansettelsesavtalen, vil dette være konsesjonspliktig (formålet med behandlingen av opplysningene er å kunne begrunne en oppsigelsesak). Dersom overvåkingen skjer for eksempel på et offentlig sted med det formål å avdekke kriminelle forhold, og beslutningen som treffes består i en anmeldelse til politiet, vil dette være en prosessledende beslutning – og overvåkingen vil ikke være konsesjonspliktig. Utvalget antar at det kan være hensiktsmessig å forskriftsregulere elektronisk overvåkning generelt slik at reglene kan være mer ensartet. Slik overvåkning bør i så tilfelle underlegges meldeplikt.

Etter *annet ledd* kan Kongen gi forskrift om at visse typer behandlinger skal være unntatt fra konsesjonsplikt etter første ledd, og i stedet underlagt meldeplikt etter § 31. Det er ikke mulig å unnta behandlinger som nevnt i § 33 første ledd både fra konsesjonsplikt og meldeplikt. I og med at konsesjonsplikten er snevret vesentlig inn, antar utvalget at behovet for å fritta visse behandlinger fra konsesjonsplikt vil være relativt lite. Føring av personalregistre (som også i dag er fritatt fra konsesjonsplikt i forskriftene til personregisterloven) utgjør imidlertid en type behandling av personopplysninger som fortsatt bør være unntatt fra konsesjonsplikt. For slik behandling skal det gis forskrift om forhold som nevnt i § 35 annet ledd dersom dette anses nødvendig for begrense de ulempene behandlingen ellers kunne medføre.

§ 34 Vurderingen av om konsesjon skal gis

Ved vurderingen av om konsesjon skal gis, skal det innenfor den rammen som er fastsatt i loven kapittel 2, vurderes om behandlingen av de sensitive personopplysningene kan volde ulemper for den registrerte som ikke løses tilfredsstillende av vilkår fastsatt i medhold av § 35 første ledd. Dersom slike ulemper kan oppstå, må det overveies om de blir oppveid av hensyn som taler for at behandlingen kan finne sted.

Til § 34:

Bestemmelsen angir den interesseavveiningen som skal foretas ved vurderingen av om konsesjon skal gis. Bestemmelsen er en videreføring av personregisterloven § 10, se Justisdepartementets merknader til denne bestemmelsen i Ot prp nr 2 (1977-78) side 80. Se forøvrig utvalgets merknader i 12.5.5.5.

Bestemmelsen er ment å gi uttrykk for at det er personvern hensyn som skal søkes fremmet ved konsesjonsordningen, dette følger også av lovens formål, jf § 1. Det fremgår videre at samtykke bare kan nektes når behandlingen kan volde problemer for den enkelte. Paragrafen henviser til § 35 annet ledd som gir en liste over hvilke momenter Datatilsynet bør ta i betraktning når konsesjonsspørsmålet skal avgjøres, se merknadene til denne bestemmelsen.

§ 35 Vilkår for konsesjonspliktige behandlinger

Når det blir gitt samtykke etter § 33, skal det fastsettes nærmere vilkår for behandlingen dersom slike vilkår anses nødvendige for å begrense de ulempene behandlingen ellers kunne medføre.

I vurderingen av om det er nødvendig å sette vilkår etter første ledd bør det blant annet tas i betraktning om

1. det er lagt til rette for at de registrerte kan gjøre nytte av rettighetene etter loven,

- herunder om de vil bli gitt tilstrekkelig informasjon om sine rettigheter og mulighetene til å gjøre nytte av dem
2. personopplysningene vil bli tilstrekkelig korrekte, dekkende og ajourførte i forhold til formålet med behandlingen, jf § 7
 3. personopplysningene vil bli behandlet med den diskresjon som regler om taushetsplikt og formålet med behandlingen gjør nødvendig
 - 4) det er planlagt informasjons- og veiledningstiltak som står i et rimelig forhold til kontrolltiltak
 4. det er etablert tilstrekkelig sikkerhet i forhold til formålene med behandlingen av personopplysninger.

Til § 35:

Bestemmelsen angir forhold Datatilsynet bør ta i betraktning når konsesjons-spørsmålet skal avgjøres, se 12.5.5.5. Bestemmelsen er en delvis videreføring av personregisterloven § 11, men vilkårangivelsen i § 11 er omformulert til mer generelle momenter. Listen er ikke uttømmende, men gir eksempler på hensynene bak personvernet, se utvalgets merknader i "*Hva er personvern?*" i kapittel 3. Bestemmelsen åpner for at nye hensyn kan gjøre seg gjeldende gjennom teori og praksis. Den legger ikke føringer på vektleggingen av de forskjellige hensynene og begrenser ikke Datatilsynets kompetanse. Hensynet til forutberegnelighet for den som søker konsesjon er også varetatt ved at den alminnelige forvaltningsrettslige vilkårlære, sett i sammenheng med lovens formål, setter rammer for hvilke konsesjonsvilkår som kan stilles.

Fokuseringen på vilkår gjenspeiler at konsesjonsvurderingen sjelden er et spørsmål om konsesjon skal gis, men som oftest på hvilke betingelser konsesjon skal gis.

*"Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse" i
Kapittel 7 Tilsyn og sanksjoner*

§ 36 Datatilsynets organisering og oppgaver

Datatilsynet skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Datatilsynet ledes av en direktør som utnevnes av Kongen. Direktøren kan utnevnes for en tidsavgrenset periode.

Kongen kan ikke gi Datatilsynet instruksjoner om håndhevingen av loven, og heller ikke om myndighetsutøvelsen i enkelttilfeller. Datatilsynets enkeltvedtak kan ikke omgjøres av Kongen.

Datatilsynet skal

1. behandle søknader om konsesjoner, motta meldinger og vurdere om det skal gis pålegg der loven gir hjemmel for dette
2. kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet
3. holde seg orientert om den generelle nasjonale og internasjonale utviklingen i behandlingen av personopplysninger og om de problemer som knytter seg til slik behandling, samt gi informasjon om dette
4. identifisere og formulere personvernetrusler, og gi råd om hvorledes de kan unngås eller begrenses
5. gi råd og rettledning i spørsmål om personvern og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder gi bistand i utarbeidelsen av bransjevise atferdsnormer

6. etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om behandling av personopplysninger, herunder være høringsinstans ved utarbeidelsen av lover og forskrifter som har direkte betydning for personvern
7. gi Kongen eller det departement Kongen fastsetter årlig melding om sin virksomhet.

Til § 36:

Bestemmelsen bygger på personregisterloven § 2 og § 3 annet ledd, og lovfester vesentlige deler av direktivet artikkel 28 (jf utvalgets vurderinger i "[Tilsynsmyndigheten](#)" i kapittel 18). Bestemmelsen viderefører grunnlaget for et Datatilsyn og organiseringen av dette, og gir en oversikt over oppgavene Datatilsynet skal vareta. Se "[Datatilsynets oppgaver i fremtiden](#)" i kapittel 18.2 og "[Administrasjon av loven – organisering av tilsynsmyndigheten](#)" i 18.3.

Utvalget er delt i synet på om Datatilsynet fortsatt bør ledes av et styre. Utvalgets leder og medlemmene Apenes, Kristiansen, Meinich og Schartum går inn for at Datatilsynet bør ledes av tilsynets direktør og at det ikke er behov for noe styre, jf første ledd og 18.3.7.

Medlemmene Bredengen, Gundersen, Hestnes, Håøy og Koch går inn for at Datatilsynet bør ledes av et styre, jf 18.3. Disse medlemmene foreslår at første ledd gis følgende utforming:

«Datatilsynet skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Datatilsynet ledes av et styre som skal ha syv medlemmer. Medlemmene blir oppnevnt av Kongen som også fastsetter hvem som skal være styrets leder og nestleder. Datatilsynets direktør kan utnevnes for en tidsavgrenset periode.»

Utvalget er forøvrig enig i utformingen av § 36.

Første ledd slår fast at Datatilsynet skal være et uavhengig forvaltningsorgan. Viktige sider ved uavhengigheten presiseres i annet ledd, jf nedenfor.

Datatilsynet skal være et faglig uavhengig forvaltningsorgan, jf 18.3. Dette innebærer at klager over tilsynets avgjørelser nå skal avgjøres av Personvernemnda istedet for av Justisdepartementet, jf § 36 og utvalgets merknader til denne bestemmelsen, og at Kongen/departementene ikke kan instruere Datatilsynet om lovtolkning eller myndighetsutøvelse i enkelttilfelle, jf *annet ledd*.

Tredje ledd bygger på personregisterloven § 3 annet ledd og gir en punktvis oppregning av Datatilsynets oppgaver. Bestemmelsen er ikke i seg selv hjemmel for utøvelse av offentlig myndighet, men gir en oversikt over de funksjoner tilsynet er tillagt. Bestemmelsen sier ikke noe om hvordan Datatilsynet skal prioritere de ulike oppgavene. I noen grad følger dette forutsetningsvis av andre bestemmelser i loven, f eks slik at Datatilsynet plikter å avsette ressurser til å behandle konsesjonsøknader. Øvrige prioriteringer må foretas av tilsynet selv i lys av de til enhver til tilgjengelige ressurser.

I henhold til 1) skal tilsynet behandle søknader om konsesjoner samt motta meldinger og vurdere å gi pålegg der loven hjemler dette (se f eks § 40). Hovedvekten av tilsynets arbeid vil flyttes fra behandling av konsesjoner og over til informasjonsvirksomhet og etterfølgende kontroll. Det nye reguleringsregimet forutsetter således økt vektlegging av oppgavene som nevnes i 2). Det fremgår her at tilsynet skal føre kontroll med at lover og forskrifter om behandling av personopplysninger skal etterleves. Også behandling av personopplysninger som reguleres av særlovgivning vil være gjenstand for Datatilsynets kontroll slik at Datatilsynet kan under-

søke om den behandlingsansvarlige følger hjermmelslovens bestemmelser om behandling av personopplysninger.

Nr 3) viderefører personregisterloven § 5 nr 1, likevel slik at bestemmelsen er justert i den grad det er nødvendig fordi reguleringsobjektet nå er behandling av personopplysninger og ikke (bare) personregistre.

Nr 4) er ny i forhold til personregisterloven, men er langt på vei en kodifisering av tilsynets praksis. I henhold til bestemmelsen skal tilsynet identifisere og formulere personvernetrusler og gi råd om hvordan disse kan unngås eller begrenses. Bestemmelsen forutsetter at Datatilsynet – uavhengig av innkomne konsesjonsøknader – aktivt formulerer personvernetrusler og midler for å imøtegå disse.

I henhold til 5) skal Datatilsynet gi råd om sikkerhet i forbindelse med behandling av personopplysninger, samt veilede om andre spørsmål om personvern. Nytt i forhold til personregisterloven er at tilsynet skal bidra ved utarbeidelse av bransjevisse atferdsnormer, jf 12.5.9 og direktivet artikkel 27. Dette innebærer at en bransje kan utarbeide et sett regler for behandling av personopplysninger i bransjen, for eksempel innen forsikringsvirksomhet. Reglene skal være et supplement til offentligrettslige regler gitt i eller i medhold av personregisterloven, men det etableres ikke noen plikt til å utarbeide atferdsnormer.

Det vil som oftest være ønskelig at Datatilsynet deltar i utarbeidelsen av atferdsnormene, ikke minst for å sikre at disse er i samsvar med gjeldende rett og ulovfestede personvernregler.

Atferdsnormene vil gi uttrykk for bransjens syn på hva som er rimelige krav til behandling av personopplysninger, og gir mulighet til å lage mer presise regler innenfor de rammene loven gir. Unnlattelse av å følge normene vil kunne medføre reaksjoner fra bransjeorganisasjoner, men vil ikke i seg selv resultere i noen offentligrettslig reaksjon.

Nr 6) fremhever at Datatilsynet skal være høringsinstans ved utarbeidelse av lover og forskrifter som har direkte betydning for personvern (jf direktivet artikkel 28 nr 2). Formuleringen avviker noe fra den parallell bestemmelsen i personregisterloven § 3 annet ledd nr 4), og pålegger en plikt til å høre Datatilsynet i forbindelse med regelverksarbeid. Datatilsynet vil i medhold av denne bestemmelsen være selvstendig høringsinstans, og få høringsaker sendt direkte til seg (ikke som tidligere via Justisdepartementet). På denne måten kan tilsynet utnytte hele høringstiden effektivt ved tidlig å vurdere de personvernproblemstillingene forslaget måtte reise.

I nr 7) pålegges Datatilsynet å gi en årsmelding (jf direktivet artikkel 28 nr 5). Også dette punktet er nytt i forhold til personregisterloven, men innebærer ikke noen realitetsendring ettersom Datatilsynet helt siden opprettelsen i 1980 årlig har levert slik melding til Justisdepartementet (jf nærmere 18.2.3.5). Årsmeldingene vil i fremtiden være en viktig informasjonsformidler fra et faglig uavhengig Datatilsyn til det departement tilsynet administrativt er underlagt.

§ 37 Personvernemndas oppgaver og organisering

Personvernemnda avgjør klager over Datatilsynets avgjørelser. Nemnda kan bestemme at tre av nemndas medlemmer, herav leder og/eller nestleder kan behandle klager over avgjørelser som etter sin art må avgjøres uten opphold. Nemnda orienterer årlig Kongen om behandlingen av klagesakene.

Personvernemnda skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Paragraf 36 annet ledd gjelder tilsvarende.

Personvernemnda har fem medlemmer som oppnevnes for fire år. Medlemmene blir oppnevnt av Kongen, som også fastsetter hvem som skal være

nemndas leder og nestleder. Leder og nestleder skal ha kompetanse som nevnt i domstoloven § 54 annet ledd.

Til § 37:

Første ledd regulerer hvilke oppgaver Personvernemnda skal ha (jf 18.3.9.5). Nemndas sentrale oppgave er å behandle klager over Datatilsynets enkeltvedtak og andre avgjørelser som kan påklages, jf første punktum. De nærmere reglene om klage følger av forvaltningsloven kapittel VI (jf 18.3.8.1).

Medmindre noe annet uttrykkelig er sagt, gir ikke loven utvidet klageadgang i forhold til det som følger av forvaltningsloven – verken mht hvilke avgjørelser som kan påklages, eller mht hvem som har rettslig klageinteresse. Når det benyttes «avgjørelser» i første ledd istedetfor «enkeltvedtak» skyldes dette dels at alle pålegg etter § 40 kan påklages (jf nærmere nedenfor om § 40), dels at beslutning om stedlig kontroll kan påklages (jf § 38 og forvaltningsloven § 15) og dels at normer om god forvaltningsskikk i visse tilfeller kan tilsi at enkeltvedtakslignende avgjørelser kan påklages.

Visse former for klagesaker kan det være behov for å avgjøre meget raskt. Særlig gjelder dette klager over beslutning om stedlig kontroll, jf § 40 og forvaltningsloven § 15 fjerde ledd (se merknadene til § 38 nedenfor). Det kan i slike tilfelle være vanskelig å få innkalt samtlige medlemmer i nemnda på kort varsel, samtidig som avgjørelsens prosessuelle art (beslutningen om kontroll er ingen realitet-savgjørelse) ikke gjør det påkrevet med like omstendelig behandling som klager over realitetsavgjørelser. Utvalget går derfor inn for at nemnda, dersom den ønsker det, skal kunne bestemme at slike klager skal kunne avgjøres av tre av nemndas medlemmer, herunder nemndas leder.

I likhet med Datatilsynet bør Personvernemnda årlig orientere om sin virksomhet. Rent praktisk kan det være hensiktsmessig at årsmeldingen til nemnda inntas som en egen del av Datatilsynets årsmelding.

Når det gjelder spørsmålet om hvem som bør oppnevne medlemmene i personvernemnda og hvor mange medlemmer nemnda skal ha, går et flertall i utvalget bestående av Bredengen, Gundersen, Hestnes, Håøy, Koch, Kristiansen og Meinich inn for ordningen som fremgår av bestemmelsens tredje ledd slik denne er presentert ovenfor, jf 18.3.9.2.

Utvalgets leder og medlemmene Apenes og Schartum går i stedet inn for at oppnevningsspørsmålet løses ved at tredje ledd utformes slik:

«Personvernemnda har syv medlemmer som oppnevnes for fire år. Fem av medlemmene oppnevnes av Kongen. Lederen og nestlederen oppnevnes av Stortinget. Lederen og nestlederen skal ha kompetanse som nevnt i domstoloven § 54 annet ledd.»

§ 38 Datatilsynets tilgang til opplysninger m v

Datatilsynet kan kreve de opplysningene som trengs for at det kan gjennomføre sine oppgaver.

Tilsynet kan kreve å få adgang til de stedene der personregistre, billedopptak som nevnt i § 4, personopplysninger som behandles elektronisk og hjelpemidlene for elektronisk behandling av personopplysninger fins. Tilsynet kan gjennomføre de prøver eller kontroller som det mener er nødvendige og kreve nødvendig bistand fra personalet slike steder for å få utført prøvene eller kontrollene. Beslutninger om stedlig kontroll kan påklages til Personvernemnda.

Datatilsynets rett til å kreve opplysninger og tilgang til lokaler og hjelpemidler er ikke begrenset av taushetsplikt.

Kongen kan gjøre unntak fra første til tredje ledd som er nødvendige av hensyn til rikets sikkerhet. Kongen kan også gi forskrift om dekning av utgiftene ved kontroll. Skyldig bidrag til dekning av utgiftene er tvangsgrunnlag for utlegg.

Til § 38:

Paragraf 38 er i stor grad en videreføring av personregisterloven § 5, og gjennomfører direktivet artikkel 28 nr 3 første strekpunkt (se utvalgets generelle kommentarer i 18.2.3.3 ovenfor).

Første ledd slår fast at Datatilsynet kan kreve de opplysningene som er nødvendige for at tilsynet skal kunne gjennomføre sine oppgaver. Bestemmelsen er identisk med personregisterloven § 5 første ledd første punktum. Datatilsynets rett til å kreve opplysninger er ikke begrenset av taushetsplikt, jf *tredje ledd*.

Annet ledd er i det vesentlige en videreføring av personregisterloven § 5 første ledd annet og tredje punktum med de justeringer som er nødvendige fordi den nye loven bl a regulerer elektronisk behandling av personopplysninger og ikke (bare) personregistre. Første og annet punktum regulerer stedlig kontroll. Loven sier ikke noe om det skal foretas kontroll, hvor ofte kontroll ev skal foretas eller hvor grundig kontrollen skal være. Dette må vurderes av Datatilsynet i lys av tilsynets prioriteringer og den ressursituasjon som til enhver tid foreligger. Reglene om melding kan danne grunnlag for kontroll, jf forslaget §§ 31 og 32.

Bestemmelsene om stedlig kontroll suppleres av reglene i forvaltningsloven § 15 om fremgangsmåten ved granskning o l. Etter § 15 fjerde ledd kan den som granskningsforretningen angår klage over beslutningen om å fremme forretningen. Slik klage avgjøres av Personvernemnda, jf lovforslaget annet ledd tredje punktum. Klage over beslutning om stedlig granskningsforretning vil ofte måtte avgjøres hurtig, og kan avgjøres av tre av nemndas medlemmer, jf lovforslaget § 38 første ledd.

I *tredje ledd* slås det fast at taushetsplikt heller ikke begrenser adgangen til å foreta stedlig kontroll som nevnt i annet ledd.

Hensynet til rikets sikkerhet kan tale for at Datatilsynet ikke bør ha ubegrenset adgang til alle registre. *Fjerde ledd* første punktum gir derfor adgang til å gjøre unntak fra reglene i første til tredje ledd ut fra hensynet til rikets sikkerhet, jf den tilsvarende bestemmelsen i personregisterloven § 5 tredje ledd første punktum og kgl resolusjon 21 desember 1979 III. (Resolusjonen unntar personregistre som er nødvendige ut fra beredskapshensyn eller rikets sikkerhet.) Den foreslåtte forskriftshjemmelen vil som i dag bl a gi adgang til å unnta registre i den sivile og militære etterretningstjenesten.

Fjerde ledd annet punktum gir Kongen adgang til å gi forskrift om dekning av utgiftene ved kontroll, mens tredje punktum slår fast at forfalt bidrag til dekning av utgiftene er tvangsgrunnlag for utlegg. Bestemmelsen er identisk med personregisterloven § 5 tredje ledd annet og tredje punktum og skal forstås på samme måte (jf for øvrig NOU 1975: 10 s 80 om Seip-utvalgets § 12).

§ 39 Unntak fra taushetsplikt

Datatilsynets ansatte og medlemmer av Personvernemnda kan uten hinder av taushetsplikt etter forvaltningsloven § 13 gi opplysninger til utenlandske tilsynsmyndigheter når dette er nødvendig for at tilsynsmyndigheten eller utenlandske tilsynsmyndigheter skal kunne treffe vedtak, eller for å gjennomføre slike vedtak.

Til § 39:

Samarbeidet med andre lands tilsynsmyndigheter vil tilta i tiden som kommer (jf direktivet nr 6). I denne forbindelse kan det være behov for å utveksle personopplysninger som er underlagt taushetsplikt etter forvaltningsloven § 13. Unntakene fra taushetsplikt i forvaltningsloven § 13 b nr 5 gjelder i henhold til alminnelige interlegale prinsipper kun for norske forvaltningsorganer, og gir dessuten bare adgang til å videreformidle opplysninger når det er nødvendig for å fremme *avgiverorganets oppgaver*. Et særskilt unntak fra taushetsplikten synes derfor nødvendig.

Dersom Datatilsynet fortsatt skal ha et styre (jf 18.3.7.1), må bestemmelsen utformes slik at unntaket fra taushetsplikt også omfatter styremedlemmene:

«Datatilsynets ansatte, styremedlemmer og medlemmer av Personvernemnda kan uten hinder av taushetsplikt etter forvaltningsloven § 13 gi opplysninger til utenlandske tilsynsmyndigheter når dette er nødvendig for at tilsynsmyndigheten eller utenlandske tilsynsmyndigheter skal kunne treffe vedtak, eller for å gjennomføre slike vedtak.»

§ 40 Pålegg om opphør av ulovlige behandlinger m v

Datatilsynet kan gi pålegg om at behandling av personopplysninger i strid med denne loven skal opphøre eller stille vilkår som må oppfylles for at behandlingen skal være i samsvar med loven. Pålegg kan påklages til Personvernemnda.

Ved vurderingen av om det skal gis pålegg etter første ledd skal det særlig tas i betraktning forhold som nevnt i § 35 annet ledd nr 1-5.

Til § 40:

Paragraf 40 gir Datatilsynet generell hjemmel til å gi pålegg om at behandling av personopplysninger i strid med loven skal opphøre, eller i stedet bestemme vilkår som må oppfylles for at behandlingen blir i samsvar med loven. Ved at påleggskompetansen knyttes til at behandlingen må ha vært i strid med loven, synliggjøres at det bare er behandling av personopplysninger som nevnt i § 3 som omfattes (dvs elektronisk behandling av personopplysninger eller manuell behandling når personopplysningene inngår eller skal inngå i et personregister).

Personregisterloven har i dag påleggshjemmel i enkelte bestemmelser, jf f eks § 8 annet ledd, men ingen generell påleggshjemmel. Bestemmelsen er sentral i fokusskiftet fra forutgående kontroll gjennom konsesjon til etterfølgende kontroll og eventuelt inngrep.

Kompetansen til å gi pålegg knytter seg til lovens bestemmelser, og § 40 gir ikke hjemmel til å gi pålegg om strengere regulering enn det som følger av loven selv. En del bestemmelser er imidlertid skjønnsmessig utformet, og Datatilsynet vil i disse tilfellene kunne gi pålegg som presiserer hvilket innhold lovteksten skal tillegges innenfor de rammene ordlyden setter.

Datatilsynet kan velge om det skal gis pålegg om at behandlingen skal opphøre, eller om det skal fastsettes vilkår som må være oppfylt for at behandlingen skal kunne fortsette. Det kan bare settes vilkår som bringer behandlingen i samsvar med lovens øvrige bestemmelser – Datatilsynet har ingen alminnelig kompetanse til å erstatte lovens regler med vilkår som fraviker fra lovens materielle bestemmelser (uavhengig av om vilkårene er strengere eller mer liberale). I valget mellom pålegg om opphør eller vilkårsfastsettelse må det tas hensyn til at førstnevnte reaksjon ofte vil være mest inngripende, jf den alminnelige forvaltningsrettslige lære om forholdsmissighet mellom mål og virkemidler.

Det fremgår uttrykkelig av annet ledd tredje punktum at pålegg gitt i medhold av § 40 kan påklages til Personvernemnda. Avgjørelse om at behandlingen skal opphøre vil være enkeltvedtak etter forvaltningsloven, og klageadgangen vil da følge av forvaltningsloven kapittel VI. Avgjørelser om å fastsette vilkår kan imidlertid i visse tilfelle måtte betraktes som prosessuelle avgjørelser som ikke omfattes av klageadgangen i forvaltningsloven kapittel VI. Eksempler på dette kan f.eks. være at Datatilsynet i medhold av § 40 pålegger den behandlingsansvarlige å gi opplysninger til Datatilsynet. Utvalget finner at også slike pålegg bør kunne påklages, og avskjærer annet ledd tredje punktum eventuell tvil klageadgangen.

Annet ledd gir gjennom henvisningen til § 34 annet ledd en rekke momenter i vurderingen av om pålegg skal gis.

Datatilsynet kan illegge den som pålegget retter seg mot tvangsmulkt dersom pålegget ikke overholdes, jf § 41.

§ 41 Tvangsmulkt

Dersom pålegg i medhold av §§ 10, 25, 26 eller 40 ikke overholdes, kan Datatilsynet bestemme at den avgjørelsen retter seg mot skal betale en daglig løpende mulkt til staten inntil forholdet rettes.

Mulkten løper ikke før klagefristen er ute. Hvis vedtaket om tvangsmulkt påklages, løper ingen mulkt før vedtak om mulkt treffes av Personvernemnda.

Mulkten er tvangsgrunnlag for utlegg

Til § 41:

Paragraf 41 gir Datatilsynet kompetanse til på visse vilkår å ilegge tvangsmulkt, jf utvalgets generelle merknader i 19.4.2. Ettersom tvangsmulkt er en sivilrettslig administrativ sanksjon kan det i en del tilfeller være aktuelt å ilegge tvangsmulkt selv om lovovertrедelsen ikke er straffbar.

Overtredelse av lovens materielle regler gir ikke i seg selv adgang til å ilegge tvangsmulkt.

Loven sier ikke noe om mulktens størrelse. Dette må bestemmes av Datatilsynet i lys av alminnelige forvaltningsrettslige prinsipper, herunder hensynet til rimelig forholdsmessighet mellom mål og virkemidler. Momenter i fastsettelsen av mulktens størrelse kan f.eks. være hvor viktig avgjørelsen som overtres er, hvor klar overtrедelsen er, hvilke fordeler overtrедelsen innebærer for den som gjør seg skyld i den, hvilke ulemper overtrедelsen medfører for den registrerte og for samfunnet for øvrig, og hvor sterk økonomi pliktsubjektet har.

Avgjørelse om å ilegge tvangsmulkt vil være enkeltvedtak i forvaltningslovens forstand, og vil kunne påklages, jf forvaltningsloven kapittel VI og § 41 *annet ledd*.

Tvangsmulkt vil som hovedregel ikke løpe før klagefristen på tre uker (jf forvaltningsloven § 29) er utløpt, og dersom vedtaket om tvangsmulkt påklages løper tvangsmulkten først fra det tidspunkt Personvernemnda eventuelt opprettholder Datatilsynets vedtak.

I *siste ledd* er det fastsatt at påløpt mulkten er tvangsgrunnlag for utlegg, jf tvangsfullbyrdedelsesloven § 7-2 e.

§ 42 Straff

Med bøter eller fengsel inntil ett år eller begge deler straffes den som forsettlig eller aktløst

1. unnlater å innhente samtykke etter §§ 33 eller 46

2. unnlater å sende melding etter §§ 31 eller 46
3. overtrer vilkår fastsatt etter § 35 eller § 40
4. behandler personopplysninger i strid med §§ 11, 13 eller 28
5. unnlater å varsle etter §§ 20, 21, 23 eller 24
6. unnlater å etterkomme pålegg fra Datatilsynet etter §§ 10, 25, 26 eller 40
7. unnlater å gi opplysninger etter §§ 16 eller 18 jf 19.

Ved særdeles skjerpene omstendigheter kan fengsel inntil to år idømmes. Ved avgjørelsen av om det foreligger særdeles skjerpene omstendigheter skal det blant annet legges vekt på faren for stor skade eller ulempe for den registrerte, den tilskattede vinning ved overtredelsen, overtredelsens varighet og omfang, utvist skyld, og på om den skyldige tidligere er straffet for overtredelse av tilsvarende bestemmelser.

Medvirkning straffes på samme måte.

I forskrift som gis i medhold av loven, kan det fastsettes at overtredelse av forskriften skal straffes med bøter eller fengsel inntil ett år eller begge deler.

Til § 42:

Straffebestemmelsen avviker på enkelte punkter fra personregisterloven § 38, jf utvalgets vurderinger i 19.2.

Enkelte av bestemmelsene i lovforslaget er etter utvalgets syn for ubestemt til at de bør straffesanksjoneres, og det er derfor lagt til grunn samme lovtekniske løsning som i personregisterloven § 38 ved at de straffesanksjonerte bestemmelsene uttrykkelig er nevnt, jf *første ledd*.

Straffebudets subjekt «den som» omfatter bl a ansatte hos den behandlingsansvarlige og andre hjelpere som denne benytter (f eks databehandlere). Foretaksstraff reguleres av straffeloven kapittel 3 a.

Annet ledd er nytt i forhold til personregisterloven § 38 slik at fengsel inntil to år nå kan idømmes dersom det foreligger særdeles skjerpene omstendigheter. Lovteksten nevner en del veiledende momenter som skal tas i betraktning i vurderingen av om det foreligger slike omstendigheter. Momentangivelsen er ikke uttømmende og sier heller ikke noe om hvor stor vekt de ulike momentene skal tillegges. Endringen fører bl a til at foreldelsesfristen nå vil være 5 år, jf straffeloven § 67 første ledd.

Medvirkning straffes som i dag på samme måte, jf *tredje ledd* og tilsvarende personregisterloven § 38 annet ledd.

Fjerde ledd viderefører forskriftshjemmelen i personregisterloven § 38 tredje ledd.

Straffebestemmelsen vil suppleres av straffeloven kapittel 3 a om straffeansvar for foretak og de strengere bestemmelsene om datakriminalitet, jf bl a strl §§ 145 annet ledd (beskyttelsesbrudd), 151 b (ødeleggelse av informasjonssamling m m), 261 (rettsstridig bruk av bl a datautstyr) 291, 292 og 391 (skadeverk), 270 første ledd nr 2 og 391 a (databedrageri). De nevnte bestemmelsene i straffeloven er kommentert nærmere bl a i ØKOKRIMs stensilsérie nr 9 «Datakriminalitet» (Oslo 1995).

§ 43 Erstatning

Har den behandlingsansvarlige eller dennes databehandler behandlet personopplysninger i strid med denne loven eller vedtak gitt i medhold av den, skal den behandlingsansvarlige erstatte det økonomiske tapet som skaden påfører den registrerte.

Den behandlingsansvarlige kan fritas for ansvar dersom han godtgjør at tapet ikke skyldes feil eller forsømmelse på den behandlingsansvarliges side.

Kongen kan gi forskrift om objektivt ansvar for virksomheter som formidler personopplysninger (§ 45) og som har meddelt opplysninger som viser seg uriktige eller åpenbart misvisende.

Til § 43:

Paragraf 43 gir regler om erstatning, jf direktivet artikkel 23 og utvalgets vurderinger i "*Sanksjoner*" i kapittel 19 (se særlig 19.3). Bestemmelsen avviker på flere punkter fra personregisterloven § 40.

I motsetning til personregisterloven § 40, som bare regulerer erstatningsansvaret for kredittopplysningsforetak, gjelder paragraf 43 generelt for behandlingsansvarlige, jf *første ledd* første punktum. Det er bare økonomiske tap som kan kreves erstattet, jf 19.3.4. At den behandlingsansvarlige også hefter for databehandlerens feil og forsømmelser er i samsvar med alminnelige erstatningsrettslige regler om kontraktsmedhjelperansvar, og formuleringen i første ledd er ment som en henvisning til disse reglene.

Den behandlingsansvarlige er i utgangspunktet ansvarlig, men kan fritas for ansvar dersom han eller hun godtgjør at vedkommende ikke har opptrådt uaktsomt. Det oppstilles med andre ord ikke et objektivt ansvar, men et culpaansvar hvor det er en presumpsjon for at uaktsomhet er utvist. For at den behandlingsansvarlige ikke skal være ansvarlig, må denne godtgjøre at vedkommende ikke har opptrådt uaktsomt. Lignende ansvarsformer benyttes flere steder i lovgivningen for øvrig (se f.eks. håndverkertjenesteloven § 28 (3)), og ligger innenfor rammen av direktivet artikkel 23. Det er tilstrekkelig for å unngå ansvar at det sannsynliggjøres at den behandlingsansvarlige har utvist tilstrekkelig aktsomhet – dersom det er 51 % sannsynlig at den behandlingsansvarlige har utvist uaktsomhet vil han eller hun være ansvarlig, dersom det er 51 % sannsynlig at vedkommende ikke har utvist uaktsomhet, vil den behandlingsansvarlige ikke være ansvarlig. Dette er for såvidt i samsvar med alminnelige bevisbyrdereregler, jf Hov, «Rettergang i sivile saker» (2 utg 1994) s 443. Presumpsjonen for uaktsomhet vil imidlertid være avgjørende der det er like sannsynlig at det er utvist uaktsomhet som at det ikke er utvist uaktsomhet, eller der hvor dette ikke lar seg bringe på det rene. Det vil i disse tilfellene nå være den behandlingsansvarlige som må føre bevis for at han ikke har utvist skyld. Presumpsjonsregelen vil dessuten mer generelt gi den behandlingsansvarlige en oppfordring til å bringe klarhet i forhold som kan føre til eller som har ført til et tap for en registrert.

For visse former for virksomhet kan det være nærliggende å pålegge den behandlingsansvarlige et objektivt ansvar, jf 19.3.4.2.1 og *annet ledd* som gir Kongen adgang til i forskrift å bestemme at objektivt ansvar skal gjelde for virksomhet som formidler personopplysninger (jf personregisterloven § 40).

"Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger" i Kapittel 8 Forholdet til andre lover. Ikraftsetting. Overgangsregler, m v

§ 44 Forholdet til andre lover

Loven gjelder også for behandling av personopplysninger som er regulert i annen lov i den utstrekning ikke annet følger av hjemmelsloven.

Til § 44:

I likhet med personregisterloven er lovforslaget her ment å være en generell lov, dvs en lov som i utgangspunktet får anvendelse både i privat og offentlig sektor. En rekke andre lover vil også i større eller mindre grad regulere slike former for behandling av personopplysninger som lovforslaget her omfatter. Eksempler på slike lover er såkalte registerlover i snever forstand, dvs lover som oppretter og nærmere regulerer bestemte personregistre. Ettersom lovforslaget her får anvendelse ikke bare på personregistre, men også på elektronisk behandling av personopplysninger mer generelt, vil lovforslaget supplere flere lover enn det personregisterloven gjorde. Utgangspunktet er da at lovforslaget her kommer til anvendelse med mindre noe annet fremgår av annen lovgivning. Se forøvrig ovenfor merknadene til § 33 om såkalte «§ 41-registre».

§ 45 Forskriftsregulering av bestemte former for virksomheter

Kongen kan gi forskrift om behandling av personopplysninger for særskilte virksomheter og bransjer.

Til § 45:

En av de bransjene som bør undergis egen forskriftsregulering er kredittopplysningsvirksomhet, se "*Særlige regler for visse virksomheter*" i kapittel 13.

§ 46 Overgangsregler

Innehavere av konsesjon etter lov om personregistre mm § 9 som blir meldepliktige eller konsesjonspliktige i medhold av denne lov "*Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern*" i kapittel 6, skal sende melding etter § 31 eller søke konsesjon etter § 33 innen tre år fra loven trer i kraft. Konsesjonsvilkårene gjelder i den utstrekning de ikke strider mot denne loven.

Behandlingsansvarlige som ikke har konsesjon etter lov om personregistre mm § 9 og som foretar behandling av personopplysninger som blir meldepliktige eller konsesjonspliktige i medhold av denne lov "*Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern*" i kapittel 6, skal sende melding etter § 31 eller søke konsesjon etter § 33 innen ett år fra loven trer i kraft.

Kongen kan gi forskrift med utfyllende overgangsregler.

Til § 46:

Lovforslaget her legger opp til en regulering av personopplysninger som på mange måter skiller seg nokså sterkt fra personregisterloven. Det blir derfor særskilt viktig å avveie hensynet til at lovforslaget snarest mulig bør få den tilsiktede effekt, mot behovet de behandlingsansvarlige har til å innrette seg etter de nye reglene.

Dette er varetatt i § 46 på den måten at innehavere av konsesjon etter personregisterloven § 9 som også blir konsesjonspliktige i medhold av lovforslaget, skal søke konsesjon etter § 33 innen tre år fra loven trer i kraft. Konsesjonsvilkårene gjelder i den utstrekning de ikke strider mot den nye loven. Innehavere av konsesjon etter personregisterloven § 9 som blir meldepliktige i medhold av lovforslaget, skal sende melding etter § 31 innen tre år fra loven trer i kraft.

Behandlingsansvarlige som ikke har konsesjon etter personregisterloven § 9 og som foretar behandling av personopplysninger som blir konsesjonspliktige i medhold av lovforslaget, skal søke konsesjon etter § 33 innen ett år fra loven trer i kraft. Behandlingsansvarlige som ikke har konsesjon etter personregisterloven § 9 og som foretar behandling av personopplysninger som blir meldepliktig etter lovforslaget, skal sende melding etter § 31 innen ett år fra loven trer i kraft.

§ 47 Ikrafttredelse

Loven trer i kraft fra den tiden Kongen bestemmer. De ulike paragrafene kan settes i kraft til ulik tid.

KAPITTEL22

Lovforslaget

Lov om behandling av personopplysninger (personopplysningsloven)

"Sammendrag av personregisterlovutvalgets utredning" i Kapittel 1 Lovens formål og område

§ 1 Lovens formål

Lovens formål er å bidra til at behandling av personopplysninger skjer i samsvar med grunnleggende personvern hensyn, herunder behovet for tilstrekkelig opplysningskvalitet, personlig integritet og privatlivets fred.

Alternativt forslag til § 1:

Denne lovens hensikt er å sikre at personopplysninger, knyttet til den enkeltes private livsområde, blir innhentet, bearbeidet, oppbevart og benyttet på grunnlag av samtykke, lovhjemmel eller rettslig beslutning. De samme krav stilles til registrering av adferd.

Den enkeltes ukrenkelighet skal respekteres både i privatliv, arbeidsliv og i offentlige sammenhenger.

Enhver har i utgangspunktet råderett over kunnskap denne gir fra seg om seg selv. Opplysninger, eller et materiale som gir grunnlag for opplysninger, skal bare benyttes til det eller de oppgitte formål de innhentes eller samles for.

Unntak skal være hjemlet i lov.

Lovens regler omfatter fysiske personer. De kommer også til anvendelse hvis opplysninger om døde eller juridiske personer kan knyttes til individ eller slekt og opplysningene må antas å være følsomme.

§ 2 Definisjoner

1. Med «personopplysning» menes opplysninger og vurderinger som direkte eller indirekte kan knyttes til en identifiserbar, fysisk person (den registrerte).
2. Med «behandling av personopplysninger» menes enhver operasjon eller serie av operasjoner som utføres på personopplysninger, som for eksempel innsamling og registrering herunder elektronisk overvåkning, systematisering, oppbevaring, endring, søking, utlevering, sammenstilling, blokkering og sletting.
3. Med «personregister» menes registre, fortegnelser mm der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen.
4. Med «behandlingsansvarlig» menes den som bestemmer formålet med en elektronisk behandling eller formålet med et manuelt personregister, samt hvilke operasjoner som skal eller kan utføres på personopplysninger.
5. Med «databehandler» menes den som i henhold til avtale behandler personopplysninger på vegne av den behandlingsansvarlige.
6. Med «elektronisk overvåkning» menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende utstyr.
7. Med «samtykke» menes en uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar at opplysninger om en selv blir behandlet.

8. Med «sensitive personopplysninger» menes personopplysninger om
- rasemessig eller etnisk bakgrunn, eller politisk eller religiøs oppfatning
 - at en person har vært mistenkt, siktet, tiltalt eller dømt for straffbare forhold
 - helseforhold, herunder opplysninger om arveegenskaper og misbruk av rusmidler
 - seksuelle forhold
 - medlemsskap i fagforeninger.
9. Med «enkeltavgjørelse» menes
- enkeltvedtak, jf forvaltningsloven § 2 bokstavene b) og a), og
 - andre avgjørelser som er bestemmende for bestemte private personers rettigheter eller plikter.

§ 3 Lovens saklige virkeområde

Loven gjelder for helt eller delvis elektronisk behandling av personopplysninger og for manuell behandling når personopplysningene inngår eller skal inngå i et personregister.

Loven gjelder ikke behandling av personopplysninger for rent personlige formål.

Kongen kan gi forskrift om at loven eller deler av denne ikke skal gjelde for bestemte former for elektronisk behandling av personopplysninger.

§ 4 Fjernsynsovervåkning og billedopptak

For fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning som ikke er elektronisk behandling av personopplysninger gjelder §§ 7, 24, 40, 41 og § 42 nr 6 tilsvarende.

For billedopptak i forbindelse med fjernsynsovervåkning som ikke er elektronisk behandling gjelder også §§ 31, 32 og 38 tilsvarende.

Med fjernsynsovervåkning menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller lignende apparat.

§ 5 Forholdet til ytringsfriheten

Loven gjelder for behandling av personopplysninger som utelukkende finner sted i journalistisk øyemed eller for kunstnerisk eller litterær virksomhet. Det skal gjøres unntak fra bestemmelsene i den grad det er nødvendig for å forene hensynet til ytringsfrihet med hensynet til personvern.

§ 6 Lovens geografiske virkeområde

Loven gjelder for behandling av personopplysninger når den behandlingsansvarlige er etablert i riket, herunder Svalbard og Jan Mayen.

Loven gjelder også for behandling av personopplysninger som skjer i riket og som forestås av en behandlingsansvarlig som er etablert i stater utenfor EØS-området dersom den behandlingsansvarlige benytter hjelpemidler i Norge. Den behandlingsansvarlige skal i så fall utpeke en representant som er etablert i Norge. Reglene om den behandlingsansvarlige gjelder tilsvarende for representanten.

Annet ledd gjelder ikke dersom hjelpemidlene utelukkende benyttes til å transportere personopplysninger via Norge.

"Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte" i Kapittel 2 Alminnelige regler om behandling av personopplysninger

§ 7 Krav til saklighet

Personopplysninger kan bare behandles til lovlige og uttrykkelig angitte formål. Formålet skal være saklig begrunnet ut fra den behandlingsansvarliges virksomhet.

Personopplysningene skal være relevante ut fra det angitte formålet.

Elektronisk overvåkning av sted hvor en begrenset krets av personer jevnlig ferdes, er bare tillatt dersom det ut fra hensynet til virksomheten er et særskilt behov for overvåkingen.

§ 8 Anvendelse av personopplysninger til andre formål enn det opprinnelige

Personopplysninger som er samlet inn til behandling for et formål kan bare anvendes til andre formål dersom

1. den registrerte samtykker i det nye behandlingsformålet
2. det er fastsatt i lov at det er adgang til å bruke opplysningene til det nye behandlingsformålet, eller
3. fordelene med den nye behandlingen er klart større enn ulempene som den volder for den enkelte og den nye behandlingen ikke er uforenlig med det opprinnelige formålet.

Kongen kan gi forskrift om anvendelse av personopplysninger til nye formål.

§ 9 Behandling av sensitive personopplysninger

Sensitive personopplysninger (jf § 2 nr 8) kan bare behandles dersom

1. den registrerte samtykker
2. det er fastsatt i lov at det er adgang til slik behandling
3. den behandlingsansvarlige plikter å foreta behandlingen i henhold til avtale mellom partene i arbeidslivet
4. behandlingen er nødvendig for å beskytte den registrertes eller en annen persons vesentlige interesser, og vedkommende selv ikke er i stand til å gi samtykke som nevnt i nr 1
5. behandlingen utføres av en ideell organisasjon som ledd i organisasjonens rettmessige virksomhet. Behandlingen kan kun omfatte opplysninger om organisasjonens medlemmer eller personer som på grunn av organisasjonens formål er i regelmessig kontakt med den. Personopplysningene kan ikke videreformidles uten den registrertes samtykke
6. behandlingen gjelder opplysninger som den registrerte selv har gjort alminnelig kjent
7. behandlingen er nødvendig for at et rettskrav kan fastsettes, gjøres gjeldende eller forsvares
8. behandlingen er nødvendig for medisinske formål eller for forvaltning av helsetjenester og opplysningene behandles av en helsearbeider med taushetsplikt
9. behandlingen er nødvendig for statistiske formål eller forskning og behandlingen ikke kan få direkte virkninger for den enkelte.

Datatilsynet kan bestemme at sensitive personopplysninger også i andre tilfeller kan behandles dersom viktige samfunnsinteresser tilsier det og det settes i verk tiltak for å sikre de registrertes interesser.

§ 10 Bruk av fødselsnummer

Bruk av fødselsnummer må være saklig begrunnet ut i fra behovet for sikker identifisering.

Datatilsynet kan gi pålegg om at fødselsnummer skal brukes for å sikre tilstrekkelig kvalitet på personopplysninger.

§ 11 Sikring av personopplysninger

Den behandlingsansvarlige og databehandleren skal sørge for at personopplysningene til enhver tid er sikret tilstrekkelig konfidensialitet og har den kvalitet og tilgjengelighet som formålet med behandlingen tilsier.

Den behandlingsansvarlige plikter å gjennomføre sikkerhetsvurderinger og etablere og holde vedlike planlagte og systematiske sikkerhetstiltak for å oppnå kravene i første ledd. Sikkerhetstiltakene skal være bygget opp i henhold til alminnelige anerkjente metoder.

Sikkerhetsvurderingen og tiltakene skal dokumenteres og ved forespørsel være tilgjengelig for Datatilsynet og Personvernemnda. De ansatte i Datatilsynet og medlemmene i Personvernemnda plikter å hindre at andre får adgang eller kjennskap til opplysninger om sikkerhetsvurderinger og sikkerhetstiltak dersom slike opplysninger kan svekke sikkerhetstiltakene.

Kongen kan gi forskrift om sikring av personopplysninger.

Alternativt tredje ledd annet punktum:

De ansatte i Datatilsynet, styremedlemmene og medlemmene i Personvernemnda plikter å hindre at andre får adgang eller kjennskap til opplysninger om sikkerhetsvurderinger og sikkerhetstiltak dersom slike opplysninger kan svekke sikkerhetstiltakene.

§ 12 Internkontroll

Den behandlingsansvarlige skal kunne dokumentere at det er etablert systemer og rutiner som sikrer overholdelse av reglene i loven samt vilkår og pålegg etter §§ 35 og 40.

Kongen kan gi forskrift om internkontroll.

§ 13 Databehandlerens rådighet over personopplysninger

Databehandleren kan ikke uten avtale med den behandlingsansvarlige anvende opplysningene til andre formål enn det oppdraget gjelder. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

§ 14 Frist for oppfyllelse av plikter

Den behandlingsansvarlige skal sørge for at den registrertes krav etter loven §§ 16, 18, 22, 25, 26, 27 og 28 gjennomføres uten ugrunnet opphold og senest innen én måned.

Dersom særlige grunner gjør det umulig å oppfylle pliktene innen en måned kan gjennomføring skje senere. I slike tilfeller skal midlertidig skriftlig svar gis innen fristen. I det midlertidige svaret skal det opplyses om grunnen til forsinkelsen og sannsynlig tidspunkt for gjennomføring.

§ 15 Betaling

Rettighetene etter §§ 16, 18, 22, 25, 26, 27 og 28 utøves vederlagsfritt for den registrerte. Dersom særlige grunner gjør det nødvendig, kan Kongen gi forskrift om at den registrerte må betale vederlag til den behandlingsansvarlige.

"Hva er personvern?" i Kapittel 3 Innsynsrett og varslingsplikt m v

§ 16 Rett til generell informasjon om behandling av personopplysninger

Den som ber om det skal få vite hvilke behandlinger av personopplysninger en behandlingsansvarlig foretar. Den som ber om det skal dessuten få følgende informasjon om en bestemt behandling av personopplysninger:

1. navn og adresse på den behandlingsansvarlige og på dennes eventuelle representant, jf § 6
2. hvem som har det daglige ansvaret for å oppfylle pliktene som hviler på den behandlingsansvarlige
3. behandlingens formål
4. definisjoner og andre beskrivelser av de typer personopplysninger som inngår i behandlingen
5. kilde for opplysningene
6. hvem personopplysningene blir eller vil bli utlevert til, herunder planlagt utlevering av personopplysningene til mottakere i andre stater.

Informasjon kan kreves hos den behandlingsansvarlige eller dennes representant som nevnt i § 6. Den som ber om informasjon kan kreve at informasjonen gis skriftlig.

Kongen kan gi forskrift om unntak fra første ledd dersom dette er nødvendig av hensyn til rikets sikkerhet eller forebyggelse og etterforskning av straffbare handlinger.

§ 17 Offentlig fortegnelse over konsesjoner og meldinger

Datatilsynet skal føre en systematisk fortegnelse over alle behandlinger som er innmeldt etter § 31 eller gitt konsesjon i medhold av § 33. Av fortegnelsen skal det minst fremgå opplysninger som nevnt i § 16 annet ledd.

Fortegnelsen skal være offentlig på den måten Datatilsynet bestemmer.

Kongen kan gi forskrift om fortegnelsen og gjøre slike unntak fra første ledd som er nødvendig ut fra beredskapshensyn eller hensynet til rikets sikkerhet.

§ 18 Den registrertes rett til innsyn

Den registrerte skal på forespørsel få opplyst:

1. hvilke opplysninger om en selv som behandles ved elektroniske hjelpemidler eller som er tatt inn i et manuelt register
2. behandlingens formål
3. hvem opplysningene om en selv blir eller vil bli utlevert til
4. kilden for disse opplysningene
5. hvilke sikkerhetstiltak som er knyttet til behandlingen, dersom innsyn ikke svekker sikkerheten.

Innsyn kan kreves hos den behandlingsansvarlige eller dennes representant som nevnt i § 6. Den registrerte kan kreve at opplysningene skal gis skriftlig.

§ 19 Unntak fra den registrertes rett til innsyn

Innsynsretten etter § 18 gjelder ikke opplysninger som bare brukes til statistikk, forskning eller generelle planleggingsformål dersom behandlingen ikke får noen direkte betydning for den registrerte.

Innsynsretten gjelder ikke opplysninger som det må anses utilrådelig at den registrerte får kjennskap til, av hensyn til vedkommendes helse eller forholdet til personer som står dem nær. Opplysningen kan på anmodning likevel gjøres kjent for en representant for den registrerte når ikke særlige grunner taler mot det.

Den registrerte kan ikke kreve innsyn i opplysninger i dokumenter som er unntatt fra innsyn etter forvaltningsloven § 18. Overfor behandlingsansvarlige som ikke er organ for stat eller kommune kan det ikke kreves innsyn i opplysninger i dokumenter som er utarbeidet for den interne saksforberedelse av

1. den behandlingsansvarlige selv
2. særskilte rådgivere eller sakkyndige, eller
3. annen sammenslutning eller stiftelse innenfor eget konsern eller organisasjon.

Selv om opplysninger er unntatt etter reglene i fjerde ledd, har den registrerte rett til innsyn i faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum. Dette gjelder likevel ikke når den registrerte på annen måte har tilgang til de faktiske opplysningene.

Dersom innsyn kan motvirke muligheten for å få en sak som er under behandling avklart, kan den som kravet om innsyn retter seg mot bestemme at den registrerte ikke skal gis innsyn så lenge undersøkelser pågår.

Kongen kan gi forskrift om unntak fra og vilkår for bruk av innsynsretten.

§ 20 Informasjonsplikt ved innsamling av personopplysninger fra den registrerte

Ved innsamling av personopplysninger fra den registrerte skal den behandlingsansvarlige opplyse den registrerte om hvem som er behandlingsansvarlig, formålet med innsamlingen av opplysningene samt om det er frivillig å levere fra seg opplysningene. Informasjonsplikten gjelder ikke dersom den registrerte må antas allerede å kjenne til dette.

Ytterligere informasjon skal gis dersom det må antas å være nødvendig for at den registrerte skal kunne ivareta egne interesser. Eksempler på slik informasjon er hvem opplysningene kan bli utlevert til, samt i hvilken grad den registrerte kan kreve innsyn, retting eller sletting av opplysningene.

§ 21 Varslingsplikt ved innsamling av personopplysninger fra andre enn den registrerte

Dersom personopplysningene innhentes fra andre enn den registrerte, skal den behandlingsansvarlige gi informasjon som nevnt i § 15 annet ledd til den registrerte når registrering skjer. Dersom opplysningene skal videregis innen rimelig tid, kan varslingen utsettes til første gangs videregivelse av opplysningene.

Første ledd gjelder ikke dersom

1. varslingen er umulig eller uforholdsmessig vanskelig,
2. den registrerte må antas å være kjent med behandlingen, eller
3. det er fastsatt i lov at det er adgang til å registrere eller videreggi opplysningene.

§ 22 Rett til begrunnelse for fullstendig automatiserte avgjørelser

Dersom det foreligger en avgjørelse som definert i § 2 nr 9 som fullt ut er basert på automatisk behandling av personopplysninger, kan den som avgjørelsen retter seg mot kreve å få begrunnet resultatet. I begrunnelsen skal den behandlingsansvarlige redegjøre for regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen.

§ 23 Varlingsplikt ved bruk av personprofiler

Når det treffes enkeltavgjørelser som definert i § 2 nr 9 eller gjøres henvendelser til den registrerte på grunnlag av personprofiler som er ment å beskrive atferd, preferanser, evner eller behov, skal den behandlingsansvarlige opplyse den registrerte om hvem som er behandlingsansvarlig, hvilke opplysningstyper som er anvendt, samt kildene for disse opplysningene.

§ 24 Varlingsplikt ved elektronisk overvåkning

Ved elektronisk overvåkning på offentlig sted eller arbeidssted skal det ved skilting eller på annen måte gjøres tydelig oppmerksom på at stedet blir overvåket og hvem som er behandlingsansvarlig.

"Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet" i Kapittel 4 Retting og sletting mv

§ 25 Plikt til å rette, slette, supplere og sperre mangelfulle personopplysninger

Dersom det er registrert personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å registrere, skal den behandlingsansvarlige sørge for at opplysningene rettes, slettes eller suppleres såframt mangelen kan få betydning for den registrerte. Har mangelen ført til at det er gitt eller brukt slike opplysninger, skal den behandlingsansvarlige såvidt mulig sørge for at feilen ikke får betydning for den registrerte.

Dersom opplysningene på grunn av annen lovgivning ikke kan slettes eller rettes kan Datatilsynet gi pålegg om at opplysningene skal sperres for å forhindre at de blir brukt.

§ 26 Sletting og sperring av personopplysninger

Den behandlingsansvarlige plikter, når det ikke lenger er saklig grunn for oppbevaring, å slette personopplysninger som behandles elektronisk eller som inngår eller skal inngå i et manuelt personregister. Med saklig grunn forstås blant annet at oppbevaring er pålagt i eller i medhold av lov eller at den behandlingsansvarlige behandler opplysningene til det formål de er innsamlet for.

Den registrerte kan, dersom dette ikke strider mot annen lov, likevel kreve slike opplysninger om seg selv sperret eller slettet dersom opplysningene er belastende for den registrerte og sperring eller sletting finnes forsvarlig ut fra en samlet vurdering av andres interesser, personverninteresser, samfunnsmessige interesser og den ressursinnsats som kravet forutsetter. Datatilsynet kan gi pålegg om slik sperring eller sletting. Slikt pålegg går foran bestemmelsene om kassasjon i lov 4 desember 1992 nr 126 om arkiv § 9.

§ 27 Rett til å kreve manuell behandling av personopplysninger

Den som en avgjørelse retter seg mot eller som saken ellers direkte gjelder, kan kreve at personopplysningene behandles manuelt dersom avgjørelsen

1. er en enkeltavgjørelse som definert i § 2 nr 9 eller som på annen måte har vesentlig betydning for vedkommende, og
2. fullt ut er basert på automatisk behandling, og
3. karakteriserer personlige egenskaper.

Retten til å kreve en manuell behandling som nevnt i første ledd gjelder ikke dersom det er truffet tilstrekkelige tiltak for å ivareta vedkommendes personverninteresser, og

1. avgjørelsen er hjemlet i lov, eller
2. avgjørelsen knytter seg til inngåelse eller oppfyllelse av kontrakt.

§ 28 Rett til å kreve sitt navn sperret mot bruk i markedsføringsøyemed

Kongen kan gi forskrift om at det skal opprettes et sentralt reservasjonsregister samt nærmere regler for registeret.

Den registrerte kan kreve sitt navn sperret mot bruk til direkte markedsføring. Sperring kan kreves både i det sentrale reservasjonsregisteret og i markedsførers adresseregister.

En behandlingsansvarlig som markedsfører direkte plikter å oppdatere adresseregisteret i henhold til det sentrale reservasjonsregisteret før første gangs utsendelse og minst to ganger pr år. Kongen kan i forskrift gjøre unntak fra denne plikten.

Mottakere av direkte reklame skal få opplyst hvem som har oppgitt personopplysningene som ligger til grunn for henvendelsen.

Denne bestemmelsen gjelder ikke for markedsføring av egne produkter fra den behandlingsansvarlige hvor den registrerte har et løpende kundeforhold.

"Personregisterloven med forskrifter" i Kapittel 5 Videregivelse av personopplysninger til utlandet

§ 29 Vilkår for videregivelse av personopplysninger til utlandet – hovedregel

Videregivelse av personopplysninger til utlandet kan bare skje dersom staten som mottakeren skal behandle personopplysningene i regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte. Stater som har gjennomført direktiv 95/46/EF oppfyller kravet til tilstrekkelig forsvarlig regulering.

I vurderingen av om stater som ikke har gjennomført direktiv 95/46/EF regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte, skal det bl a legges vekt på opplysningenes art, de planlagte behandlingenes formål og varighet, den aktuelle statens rettsregler om behandling av personopplysninger, regler for god forretningsskikk og sikkerhetsforanstaltninger hos mottakeren. Det skal også legges vekt på om den aktuelle staten har tiltrådt Europarådets konvensjon 28 januar 1981 nr 108.

§ 30 Videregivelse av personopplysninger til stater som ikke regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte

Videregivelse av personopplysninger til utlandet kan skje selv om den aktuelle staten ikke regulerer behandling av personopplysninger på en tilstrekkelig forsvarlig måte dersom

1. den registrerte har gitt sitt samtykke til videregivelsen
2. Norge har plikt til å foreta slik videregivelse etter folkerettslig overenskomst eller som følge av medlemskap i internasjonal organisasjon
3. det er fastsatt i lov at det er adgang til å videreggi opplysningene
4. videregivelsen er nødvendig for å inngå eller oppfylle en kontrakt mellom den registrerte og den behandlingsansvarlige
5. videregivelsen er nødvendig for å inngå eller oppfylle en kontrakt i den registrertes interesse
6. videregivelsen er nødvendig for å beskytte den registrertes vesentlige interesser.

Dersom særlig grunner taler for det, kan Datatilsynet tillate videregivelse selv om vilkårene i første ledd ikke er oppfylt.

Kongen kan gi forskrift om videregivelse av personopplysninger til utlandet.

"Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern" i Kapittel 6 Meldeplikt og konsesjonsplikt m v

§ 31 Meldeplikt

Enhver behandlingsansvarlig som benytter elektroniske systemer for behandling av personopplysninger skal gi melding til Datatilsynet på fastsatt skjema i god tid før behandlingen tar til.

Slik melding skal også sendes ved opprettelse av et manuell personregister dersom det skal inneholde sensitive personopplysninger, jf § 2 nr 8.

Meldeplikten gjelder ikke for behandlinger som utelukkende gjør bruk av allment tilgjengelige personopplysninger.

Kongen kan gi forskrift om at visse typer behandlinger skal være unntatt fra meldeplikten etter første og annet ledd, underlagt en forenklet meldeplikt eller underlagt konsesjonsplikt. For behandlinger som unntas fra meldeplikt kan det gis forskrift om forhold som nevnt i § 35 annet ledd. Det kan også gis forskrift for å begrense de ulemper behandlingen ellers kunne medføre for den enkelte.

§ 32 Meldingens innhold

Meldingen skal inneholde opplysninger om

1. navn og adresse på den behandlingsansvarlige og på dennes eventuelle representant, jf § 6
2. hvem som har det daglige ansvaret for å oppfylle pliktene som hviler på den behandlingsansvarlige
3. behandlingens formål
4. definisjoner og andre beskrivelser av de typer personopplysninger som inngår i behandlingen
5. kildene for personopplysningene
6. grunnlaget for innhenting av opplysningene

7. hvem personopplysningene blir eller vil bli utlevert til
8. planlagt utlevering av personopplysningene til mottakere i andre stater, og
9. hvilke sikkerhetstiltak som er knyttet til behandlingen.

Kongen kan gi forskrift om hvilke opplysninger meldingene skal inneholde, samt regler om gjennomføringen av meldepliktsordningen.

Den behandlingsansvarlige er ansvarlig for at det til enhver tid er innsendt melding som gir riktige opplysninger. Ny melding med oppdaterte opplysninger skal sendes etter 3 år, med mindre det i løpet av denne tiden er sendt endringsmelding. Kongen kan gi forskrift som skal sikre meldingenes kvalitet og kan for enkelte typer av behandlinger fastsette andre regler for når ny melding skal sendes.

§ 33 Konesesjonsplikt

Det kreves samtykke fra Datatilsynet (konesesjon) for å behandle sensitive personopplysninger (jf § 2 nr 8) når formålet med behandlingen er å treffe enkeltavgjørelser som definert i § 2 nr 9.

Kongen kan gi forskrift om at visse typer behandlinger skal være unntatt fra konesesjonsplikten etter første ledd, og i stedet underlagt meldeplikt etter § 31. For slik behandling skal det gis forskrift om forhold som nevnt i § 35 annet ledd. Det kan også gis forskrift for å begrense de ulemper behandlingen ellers kunne medføre for den enkelte.

§ 34 Vurderingen av om konesesjon skal gis

Ved vurderingen av om konesesjon skal gis, skal det innenfor den rammen som er fastsatt i loven kapittel 2, vurderes om behandlingen av de sensitive personopplysningene kan volde ulemper for den registrerte som ikke løses tilfredsstillende av vilkår fastsatt i medhold av § 35 første ledd. Dersom slike ulemper kan oppstå, må det overveies om de blir oppveid av hensyn som taler for at behandlingen kan finne sted.

§ 35 Vilkår for konesesjonspliktige behandlinger

Når det blir gitt samtykke etter § 33, skal det fastsettes nærmere vilkår for behandlingen dersom slike vilkår anses nødvendige for å begrense de ulempene behandlingen ellers kunne medføre.

I vurderingen av om det er nødvendig å sette vilkår etter første ledd bør det blant annet tas i betraktning om

1. det er lagt til rette for at de registrerte kan gjøre nytte av rettighetene etter loven, herunder om de vil bli gitt tilstrekkelig informasjon om sine rettigheter og mulighetene til å gjøre nytte av dem
2. personopplysningene vil bli tilstrekkelig korrekte, dekkende og ajourførte i forhold til formålet med behandlingen, jf § 7
3. personopplysningene vil bli behandlet med den diskresjon som regler om taushetsplikt og formålet med behandlingen gjør nødvendig
4. det er planlagt informasjons- og veiledningstiltak som står i et rimelig forhold til kontrolltiltak
5. det er etablert tilstrekkelig sikkerhet i forhold til formålene med behandlingen av personopplysninger.

*"Europarådets konvensjon og rekommandasjoner om persondataskyttelse" i
Kapittel 7 Tilsyn og sanksjoner*

§ 36 Datatilsynets organisering og oppgaver

Datatilsynet skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Datatilsynet ledes av en direktør som utnevnes av Kongen. Direktøren kan utnevnes for en tidsavgrenset periode.

Kongen kan ikke gi Datatilsynet instruksjoner om håndhevingen av loven, og heller ikke om myndighetsutøvelsen i enkelttilfeller. Datatilsynets enkeltvedtak kan ikke omgjøres av Kongen.

Datatilsynet skal

1. behandle søknader om konsesjoner, motta meldinger og vurdere om det skal gis pålegg der loven gir hjemmel for dette
2. kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet
3. holde seg orientert om den generelle nasjonale og internasjonale utviklingen i behandlingen av personopplysninger og om de problemer som knytter seg til slik behandling, samt gi informasjon om dette
4. identifisere og formulere personverntrusler, og gi råd om hvorledes de kan unngås eller begrenses
5. gi råd og rettleiding i spørsmål om personvern og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder gi bistand i utarbeidelsen av bransjevisse atferdsnormer
6. etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om behandling av personopplysninger, herunder være høringsinstans ved utarbeidelsen av lover og forskrifter som har direkte betydning for personvern
7. gi Kongen eller det departement Kongen fastsetter årlig melding om sin virksomhet.

Alternativt forslag til § 36 første ledd:

Datatilsynet skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Datatilsynet ledes av et styre som skal ha syv medlemmer. Medlemmene blir oppnevnt av Kongen som også fastsetter hvem som skal være styrets leder og nestleder. Datatilsynets direktør kan utnevnes for en tidsavgrenset periode.

§ 37 Personvernemndas oppgaver og organisering

Personvernemnda avgjør klager over Datatilsynets avgjørelser. Nemnda kan bestemme at tre av nemndas medlemmer, herav leder og/eller nestleder kan behandle klager over avgjørelser som etter sin art må avgjøres uten opphold. Nemnda orienterer årlig Kongen om behandlingen av klagesakene.

Personvernemnda skal være et uavhengig forvaltningsorgan administrativt underordnet Kongen og det departement Kongen fastsetter. Paragraf 36 annet ledd gjelder tilsvarende.

Personvernemnda har fem medlemmer som oppnevnes for fire år. Medlemmene blir oppnevnt av Kongen, som også fastsetter hvem som skal være nemndas leder og nestleder. Leder og nestleder skal ha kompetanse som nevnt i domstolloven § 54 annet ledd.

Alternativt forslag til § 37 tredje ledd:

Personvernemnda har syv medlemmer som oppnevnes for fire år. Fem av medlemmene oppnevnes av Kongen. Lederen og nestlederen oppnevnes av Stortinget. Leder og nestleder skal ha kompetanse som nevnt i domstolloven § 54 annet ledd.

§ 38 Tilsynsmyndighetens tilgang til opplysninger m v

Datatilsynet og Personvernemnda kan kreve de opplysningene som trengs for at det kan gjennomføre sine oppgaver.

Datatilsynetilsynet kan kreve å få adgang til de stedene der personregistre, billedopptak som nevnt i § 4, personopplysninger som behandles elektronisk og hjelpemidlene for elektronisk behandling av personopplysninger fins. Tilsynet kan gjennomføre de prøver eller kontroller som det mener er nødvendige og kreve nødvendig bistand fra personalet slike steder for å få utført prøvene eller kontrollene. Beslutninger om stedlig kontroll kan påklages til Personvernemnda.

Datatilsynets rett til å kreve opplysninger og tilgang til lokaler og hjelpemidler er ikke begrenset av taushetsplikt.

Kongen kan gjøre unntak fra første til tredje ledd som er nødvendige av hensyn til rikets sikkerhet. Kongen kan også gi forskrift om dekning av utgiftene ved kontroll. Skyldig bidrag til dekning av utgiftene er tvangsgrunnlag for utlegg.

§ 39 Unntak fra taushetsplikt

Datatilsynets ansatte og medlemmer av Personvernemnda kan uten hinder av lovbestemt taushetsplikt gi opplysninger til utenlandske tilsynsmyndigheter når dette er nødvendig for at tilsynsmyndigheten eller utenlandske tilsynsmyndigheter skal kunne treffe vedtak, eller for å gjennomføre slike vedtak.

Alternativt forslag til § 39:

Datatilsynets ansatte, styremedlemmer og medlemmer av Personvernemnda kan uten hinder av lovbestemt taushetsplikt gi opplysninger til utenlandske tilsynsmyndigheter når dette er nødvendig for at tilsynsmyndigheten eller utenlandske tilsynsmyndigheter skal kunne treffe vedtak, eller for å gjennomføre slike vedtak.

§ 40 Pålegg om opphør av ulovlige behandlinger m v

Datatilsynet kan gi pålegg om at behandling av personopplysninger i strid med denne loven skal opphøre eller stille vilkår som må oppfylles for at behandlingen skal være i samsvar med loven. Pålegg kan påklages til Personvernemnda.

Ved vurderingen av om det skal gis pålegg etter første ledd skal det særlig tas i betraktning forhold som nevnt i § 35 annet ledd nr 1-5.

§ 41 Tvangsmulkt

Dersom pålegg i medhold av §§ 10, 25, 26 eller 40 ikke overholdes, kan Datatilsynet bestemme at den avgjørelsen retter seg mot skal betale en daglig løpende mulkt til staten inntil forholdet rettes.

Mulkten løper ikke før klagefristen er ute. Hvis vedtaket om tvangsmulkt påklages, løper ingen mulkt før vedtak om mulkt treffes av Personvernemnda.

Mulkten er tvangsgrunnlag for utlegg.

§ 42 *Straff*

Med bøter eller fengsel inntil ett år eller begge deler straffes den som forsettlig eller aktløst

1. unnlater å innhente samtykke etter §§ 33 eller 46
2. unnlater å sende melding etter §§ 31 eller 46
3. overtrer vilkår fastsatt etter § 35 eller § 40
4. behandler personopplysninger i strid med §§ 11, 13 eller 28
5. unnlater å varsle etter §§ 20, 21, 23 eller 24
6. unnlater å etterkomme pålegg fra Datatilsynet etter §§ 10, 25, 26 eller 40
7. unnlater å gi opplysninger etter §§ 16 eller 18 jf 19.

Ved særdeles skjerpene omstendigheter kan fengsel inntil to år idømmes. Ved avgjørelsen av om det foreligger særdeles skjerpene omstendigheter skal det blant annet legges vekt på faren for stor skade eller ulempe for den registrerte, den tilsiktede vinning ved overtredelsen, overtredelsens varighet og omfang, utvist skyld, og på om den skyldige tidligere er straffet for overtredelse av tilsvarende bestemmelser.

Medvirkning straffes på samme måte.

I forskrift som gis i medhold av loven, kan det fastsettes at overtredelse av forskriften skal straffes med bøter eller fengsel inntil ett år eller begge deler.

§ 43 *Erstatning*

Har den behandlingsansvarlige eller dennes databehandler behandlet personopplysninger i strid med denne loven eller vedtak gitt i medhold av den, skal den behandlingsansvarlige erstatte det økonomiske tapet som skaden påfører den registrerte. Den behandlingsansvarlige kan fritas for ansvar dersom han godtgjør at tapet ikke skyldes feil eller forsømmelse på den behandlingsansvarliges side.

Kongen kan gi forskrift om objektivt ansvar for virksomheter som formidler personopplysninger (§ 45) og som har meddelt opplysninger som viser seg uriktige eller åpenbart misvisende.

"Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger" i Kapittel 8 Forholdet til andre lover. Ikraftsetting. Overgangsregler, m v

§ 44 *Forholdet til andre lover*

Loven gjelder også for behandling av personopplysninger som er regulert i annen lov i den utstrekning ikke annet følger av hjemmelsloven.

§ 45 *Forskriftsregulering av bestemte former for virksomheter*

Kongen kan gi forskrift om behandling av personopplysninger for særskilte virksomheter og bransjer.

§ 46 *Overgangsregler*

Innehavere av konsesjon etter lov om personregistre mm § 9 som blir meldepliktige eller konsesjonspliktige i medhold av denne lov *"Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern"* i kapittel 6, skal sende melding etter § 31 eller søke konsesjon etter § 33

innen tre år fra loven trer i kraft. Konesjonsvilkårene gjelder i den utstrekning de ikke strider mot denne loven.

Behandlingsansvarlige som ikke har konsesjon etter lov om personregistre mm § 10 og som foretar behandling av personopplysninger som blir meldepliktige eller konsesjonspliktige i medhold av denne lov *"Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern"* i kapittel 6, skal sende melding etter § 31 eller søke konsesjon etter § 33 innen ett år fra loven trer i kraft.

Kongen kan gi forskrift med utfyllende overgangsregler.

§ 47 Ikrafttredelse

Loven trer i kraft fra den tiden Kongen bestemmer. De ulike paragrafene kan settes i kraft til ulik tid.

Vedlegg 1

Summary in English of the Committee's Proposals

Part I of the Report

In *Chapter 2*, the background, authority, composition, and working method of the Committee charged with revising the Personal Data Registers Act (hereinafter, the Committee) are presented. The need for the revision of the Personal Data Registers Act is due in part to technological development, which is steadily creating new possibilities to collect, process, and use personal information, and in part due to Norway's obligation to implement a European Union Directive on data protection.

The notions of privacy and data protection can appear both diffuse and wide-ranging. The Committee has therefore found it prudent to define precisely what meaning it assigns to these notions (see *Chapter 3*). In this way, the important frame of reference for the Committee's work is made apparent.

As mentioned above, the reason for the Committee's mandate is among other things the technological and social developments that have significance for the rules concerning privacy and data protection. *Chapter 4* goes into some of these developments in depth and explains how they are of significance for such protection.

When a law is revised, the law itself marks the starting point for the evaluation. *Chapter 5* gives an overview of the Personal Data Registers Act and its regulations, whereas *Chapter 6* illustrates that privacy and data protection are also fostered through other types of legislation, rules arising from contract, and legal norms which exist independently of statute.

The Committee has considered it important to familiarize itself with international rules and the state of the law in other countries. In *Chapter 7*, the Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data is discussed. In *Chapter 8*, an overview of the EU Directive 95/46 on the protection of individuals with regard to processing of personal data and on the free movement of such data (often called «Data Protection Directive» or «Directive») is given. In *Chapter 9*, a short account of other international rules and certain other countries' data protection legislation is given. A few foundational similarities are found – e.g. statutory rules are often combined with a regulatory agency that monitors compliance with the law. The common starting point, however, disappears due to a range of different regulatory mechanisms from country to country.

Part II of the Report

The Personal Data Registers Act applies to personal registers and the use of personal information in certain activities. The Committee proposes that the concept of register be maintained as a delimitation criterion for manual processing of personal information but that all electronic processing of personal information be covered independently of whether or not the information is part of a personal register. This is an extension of the current Personal Data Registers Act. The change is not very extensive, however, because one can relatively easily recover personal information about the individual which is stored electronically (the requirement of systematic organization of data has no independent significance).

According to the Committee's proposal, the envisaged law applies to the processing of information about *physical/natural* persons. Information about legal per-

sons will also often have a legitimate need for protection. This need will to a large extent, however, be grounded in other considerations than privacy and data protection – e.g. economic interests – and such interests should be taken care of in other legislation. Information about physical/natural persons that is connected to legal persons (e.g. a person is registered as an owner of an enterprise) will be personal information covered by the law. Information about deceased persons is covered to the extent that it is associated with a surviving individual. It is further proposed that the law apply to public and private enterprises, but that processing of personal information for purely personal purposes – as with the current Personal Data Registers Act – is not covered.

In *Chapter 11*, a series of new rights that the proposed law awards the individual are discussed. *The right of access* is extended in relation to the Personal Data Registers Act (see 11.2). In the first place, this implies an extended right to general information about the processing of personal data and an extended right of access to registered information about oneself. Second, a disclosure requirement (when the personal information is collected from the data subject and when personal information is obtained from third parties) is imposed on the party responsible for processing the data (hereinafter «data controller»). Third, the individual is given a claim to the reasoning behind completely automated decisions (the claim to access to the «logic» behind an automated decision, see 11.4).

Further, the Committee proposes certain rules which give the individual a right to oppose certain types of personal data processing (see 11.3). Two rights belong to this group. The right granted by the Personal Data Registers Act to demand that one's name be blocked from use in direct marketing is proposed to be continued in the new law. The Committee supports the Data Inspectorate's proposal to establish a central reservation register to make it easier for an individual to guard against him or herself receiving advertising material. The Committee also proposes to establish a right to demand manual review of certain entirely automatic decisions.

Finally, certain rules are proposed about the deletion of personal information (see 11.5). For the most part, it is proposed to keep the current provisions in the Personal Data Registers Act on amending, deleting, or supplementing incorrect or incomplete information or information which is not allowed to be registered. In addition, a general rule is proposed that personal information shall be deleted when an objective reason for keeping it no longer exists. Such general rules concerning deletion are laid down in the Data Inspectorate's licenses for setting up a personal data register. New in relation to today's regulation is the Committee's proposal that the registered individuals be given an expanded right to demand that information about themselves be deleted or blocked.

In closing, *Chapter 11* discusses some questions connected to deadlines for compliance with demands from the data subjects and costs connected to their rights (see 11.6).

In *Chapter 12*, the Committee proposes a broad spectrum of instruments for safeguarding privacy and data protection in connection with the processing of personal information. The Committee proposes to continue the licensing duty but to make it far less comprehensive than it currently is and to replace it with a series of measures that, among other things, will build on an obligation to submit reports in combination with more supervision from the Data Inspectorate. The Committee proposes in addition that the Data Inspectorate shall give advice to those who plan to process or who already process personal information, plus to carry out subsequent inspections. The proposals contain more rules than exist under the current law, and there will, like today, be the need for control through issuing regulations. Further, there are proposed rules about internal control, and, finally, the Committee

has evaluated the need for sectoral codes of conduct, which are drafted by the data controllers themselves. Examples of new rules in the proposed law are provisions on the requirement to explicitly define the purposes for processing personal information, on the use of personal information for other purposes than those originally considered, on processing of sensitive personal information, and on use of the official personal identification number.

The Personal Data Registers Act regulates the use of personal information in certain types of activities (credit rating activities, data processing activities, addressing and distribution services and opinion polling and marketing surveys) in Chapters 5 – 8 of the Act. The Committee does not propose to continue such distinct regulation in the new law (see *Chapter 13*). Instead, the Committee proposes a series of new rules that will be applied to all types of electronic processing (together with certain types of manual processing). More general rules reduce the need for special rules for certain selected activities. It may be pertinent for the data controller to employ a data processor who processes personal information on behalf of the responsible party by contract. The Committee proposes a provision that restricts the data controller's possession over personal information. If additional need for separate regulation of certain activities is shown, the Committee proposes that this be done through the issuing of regulations. In the Committee's opinion, processing of personal information in credit rating activities should be controlled in greater detail through regulations.

Surveillance that involves electronic processing of personal data is encompassed by the proposed law, and some provisions in the proposed law also apply to other types of surveillance. In *Chapter 14* of the Committee's report, the Committee proposes that current rules concerning video surveillance be continued and supplemented on two counts. First, the Committee recommends that video surveillance resulting in actual picture recording be covered by a duty to report. Second, the Committee proposes that the Data Inspectorate be given the power to intervene and stop video surveillance and taping in connection with surveillance when it is commenced illegally, e.g. because the surveillance is not objectively justified. Finally, it is proposed that section 390 b of the Penal Code regarding the duty to warn about video surveillance of public places and work places be moved from the Code to the proposed new law on data protection.

In *Chapter 15*, the security of personal information is treated, i.e. the attempt to ensure that personal information is processed in accordance with the law. While the legal rules make demands as to how personal information shall and can be used, it is the safety measures' organizational and technical requirements that shall safeguard that the legal rules are followed. The Committee gives an account of earlier studies and initiatives in the field, together with current law. A premise for the Committee's considerations is that there is a great need for systematic measures to ensure compliance with the rules on the processing of personal information. And such attempts are a necessary part of the future regulation of the field of privacy and data protection. The Committee proposes more specifically that a statutory duty be created to establish and apply methods for information and data security for certain types of personal data processing.

Chapter 16 deals with transfer of personal information to foreign countries. The Committee first gives an account of existing law and international regulations in the area. A premise for the Committee's considerations is that it should be easier to transfer personal information to states that have implemented the EU Directive on data protection. Regarding transfer to states that have not implemented the EU Directive, it is decisive whether or not the actual state has an adequate level of data

protection. If the receiving state does not have an adequate protection level, the transfer can take place if certain other specified conditions are met.

The rules regarding the treatment of personal information must take into account freedom of expression, *see Chapter 17*. The Committee proposes that a general exception be made from parts of the bill where it is necessary to find a reasonable balance between freedom of expression and protection of privacy. The term «freedom of expression,» is not only intended to refer to superior rules such as section 100 of the Constitution and Articles 8 and 10 of the European Convention on Human Rights, but also to freedom of expression as an interest in itself. In this chapter, the Committee gives a number of examples of the balancing of freedom of expression with privacy and data protection.

Chapter 18 deals with the regulatory agency's organization, placement and tasks.

Concerning the Data Inspectorate's tasks, it is proposed that great emphasis be placed on giving advice and controlling that the law is followed. Processing license applications will take less time and resources than it currently does.

The Committee unanimously advocates that the Data Inspectorate be independent of the government and the Ministries (except regarding administrative matters). This involves that the government and Ministries shall not be able to instruct the Data Inspectorate on the interpretation of the law and the exercise of discretion either generally or in individual cases, and that the Ministry of Justice shall no longer handle complaints about the Data Inspectorate's decisions. Complaints shall, according to the proposal, be handled by a newly created organization, the Data Protection Tribunal. This Tribunal shall also be independent of the Ministry of Justice (except regarding administrative matters). In other respects, the Committee advocates that both the Data Inspectorate and the Data Protection Tribunal shall administratively fall under the government and the Ministry the king appoints (currently the Ministry of Justice).

The Committee is not unanimous on all the issues associated with the organization and placement of the regulatory agency. The Chairman of the Committee as well as Committee members Apenes, Kristiansen, Meinich and Schartum advocate that with the new organization of the regulatory agency there will no longer be a need for a board of directors in the Data Inspectorate, whereas members Bredengen, Gundersen, Hestnes, Håøy and Koch believe that today's board arrangement should be continued. Concerning the appointment of members to the Data Protection Tribunal, the majority of the Committee's members made up of Bredengen, Gundersen, Hestnes, Håøy, Koch, Kristiansen and Meinich, advocate that the Tribunal should have five members and that all of them should be appointed by the King. A minority in the Committee, made up of the Chairman and members Apenes and Schartum, are of the opinion that the Tribunal should have seven members and that two of these should be appointed by the Parliament, whereas the rest should be appointed by the King.

Chapter 19 deals with which sanctions can be used if the law is broken. Criminal responsibility continues with some minor changes, inter alia, that violation of the law, under extremely aggravating circumstances, may result in a jail sentence of up to two years. Criminal responsibility for corporations should be regulated by the current provisions of the Penal Code. Moreover, the Committee recommends introducing a general liability for breaking the law when the breach results in economic loss and the tortfeasor cannot show that he or she was not responsible for the damage. The Committee does not advocate the right to indemnification for non-economic loss (reparation) but proposes instead that a duty be placed on the tortfeasor to ensure that the violation of the law has the least possible consequences for the

data subject (a duty of restoration). The Committee proposes further that the Data Inspectorate should be able to impose enforcement damages if the statutory duties are not followed.

In *Chapter 20*, the economic and administrative consequences of the Committee's proposals are explained. For the *Ministry of Justice*, the proposals will mean that it will no longer have to use resources on handling complaints about the Data Inspectorate's decisions. The Ministry must, however, see to it that a Data Protection Tribunal is established and set aside funding for it. For the *Data Inspectorate*, the proposals allow it to use resources that are currently needed for processing license applications for work on advising and law enforcement. The Data Inspectorate will have a need for much greater resources than today, especially in the initial stages of establishing the new regulatory regime. For the *data controller*, the proposal involves some costs that follow from an increased number of individual rights and from the requirements to take security measures, etc. Exactly how great the costs will be is hard to identify beforehand due to the fact that they depend on, among other things, how many will take advantage of the rights the proposed law gives.

Vedlegg 2

Lov av 9. juni 1978 nr. 48 om personregistre m.m. og forskrifter gitt i medhold av denne

"Sammendrag av personregisterlovutvalgets utredning" i Kapittel 1 Lovens område

§ 1. Loven gjelder for personregistre og for annen bruk av personopplysninger i visse typer virksomhet.

Med personopplysninger er ment opplysninger og vurderinger som direkte eller indirekte kan knyttes til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser. Med personregistre er ment registre, fortegnelser m.m. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen.

Loven gjelder for personregistre og bruk av personopplysninger i organ for stat eller kommune og i privat næringsvirksomhet, foreninger eller stiftelser.

Kongen kan bestemme at loven ikke skal gjelde for visse typer personregistre.

"Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte" i Kapittel 2 Datatilsynet

§ 2. Det blir opprettet et datatilsyn. Datatilsynet skal være et frittstående organ underordnet Kongen og det departement Kongen fastsetter.

Datatilsynet blir ledet av et styre, som skal ha 7 medlemmer. Medlemmene blir oppnevnt av Kongen, som også fastsetter hvem som skal være styrets formann og nestformann.

§ 3. Uttalelse fra Datatilsynet skal være innhentet før det blir gjort vedtak som i loven her er lagt til Kongen. Dette gjelder likevel ikke vedtak etter § 2.

Datatilsynet skal ellers:

1. holde seg orientert om den generelle utvikling i bruken av personregistre og om de problemer som knytter seg til slike registre, samt sørge for informasjon i denne forbindelse
2. gi råd og rettleiing om spørsmål om personvern og datasikring til dem som planlegger å opprette personregistre
3. kontrollere at de lover, forskrifter og regler som gjelder for personregistre, blir fulgt, og at feil eller mangler blir rettet
4. etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om bruk av personregistre eller i generelle spørsmål som gjelder bruk av personopplysninger.

Kongen kan gi Datatilsynet ytterligere oppgaver som gjelder bruk m.m. av personregistre eller bruk av personopplysninger ellers.

§ 4. Datatilsynet skal føre en systematisk fortegnelse over personregistre som er gitt konsesjon etter § 9. Fortegnelsen skal henviser til de regler som er fastsatt etter § 11. Et eksemplar av reglene skal oppbevares ved Datatilsynet.

Fortegnelsen og reglene skal være tilgjengelige for alle.

Kongen kan gi nærmere regler om fortegnelsen og gjøre slike unntak fra første ledd som er nødvendige ut fra beredskapshensyn eller hensynet til rikets sikkerhet.

§ 5. Datatilsynet kan kreve de opplysningene som trengs for at det kan gjennomføre sine oppgaver. Tilsynet kan kreve å få adgang til de stedene der personreg-

istre, billedopptak som nevnt i "*Oversikt over andre internasjonale reguleringer og andre lands rett*" i kapittel 9 a og tekniske hjelpemidler fins, og til å gjennomføre de prøver eller kontroller som det mener er nødvendige. Tilsynet kan kreve nødvendig bistand fra personalet slike steder for å få utført prøvene eller kontrollene.

Datatilsynets rett til å kreve opplysninger er ikke begrenset av bestemmelser om taushetsplikt.

Kongen kan gjøre slike unntak fra første og annet ledd som er nødvendige av hensyn til rikets sikkerhet. Kongen kan også gi forskrift om dekning av utgiftene ved kontroll. Skyldig bidrag til dekning av utgiftene er tvangsgrunnlag for utlegg.

"Hva er personvern?" i Kapittel 3 Alminnelige regler om personregistre

§ 6. Registrering av personopplysninger skal være saklig begrunnet ut fra hensynet til administrasjon og virksomhet i det organ eller foretak som foretar registreringen.

Uten at det er nødvendig, må det ikke registreres

1. opplysninger om rase, eller politisk eller religiøs oppfatning
2. opplysninger om at en person har vært mistenkt, tiltalt eller dømt for straffbart forhold
3. opplysninger om helseforhold eller misbruk av rusmidler
4. opplysninger om seksuelle forhold
5. andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

§ 7. Alle har rett til å få opplyst hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler. Denne innsynsretten gjelder likevel ikke registre som bare brukes til statistikk, forskning eller generelle planleggingsformål. Innsynsretten gjelder heller ikke opplysninger som det må anses utilrådelig at vedkommende får kjennskap til, av hensyn til deres helse eller forholdet til personer som står dem nær.

For personregistre i organ for stat eller kommune gjelder innsynsretten, slik den er avgrenset i første ledd, også for opplysninger som ikke lagres eller bearbeides ved elektroniske hjelpemidler. Den registrerte kan likevel ikke kreve å få se dokumenter som regnes som interne etter forvaltningslovens § 18.

For personregistre i organ for stat eller kommune har alle dessuten rett til å få opplyst hvilke typer opplysninger som er tatt inn i registeret.

Kongen kan ved forskrift bestemme at det som er fastsatt i annet og tredje ledd, også skal anvendes på personregistre i privat næringsvirksomhet, foreninger eller stiftelser, eller for visse slike registre.

Kongen kan ved forskrift eller for det enkelte register fastsette flere unntak fra innsynsretten og fastsette nærmere regler eller vilkår for bruken av retten.

§ 8. Dersom et personregister inneholder uriktige eller ufullstendige opplysninger, opplysninger som det ikke er adgang til å ta inn i registeret, eller opplysninger som ikke lenger har betydning, skal opplysningene rettes, slettes eller suppleres såframnt mangelen kan få betydning for den registrerte. Har mangelen ført til at det er gitt eller brukt uriktige eller ufullstendige opplysninger, skal det sørges for at feilen så vidt mulig ikke får betydning for den registrerte.

Når det foreligger feil som nevnt i første ledd, kan Datatilsynet gi pålegg om retting, sletting eller supplerings av registeret og om tiltak etter første ledd annet punktum.

§ 8 a. En person kan kreve sitt navn sperret i et personregister mot bruk til utsending av direkte reklame og liknende publikasjoner.

§ 8 b. Kongen kan ved forskrift eller enkeltvedtak gi regler for sikring av personopplysninger.

"Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet" i Kapittel 4 Plikt til å søke samtykke til å opprette personregistre

§ 9. Det kreves samtykke fra Kongen (konsesjon) for å opprette personregistre som skal gjøre bruk av elektroniske hjelpemidler. Slikt samtykke kreves også for å opprette andre personregistre dersom de skal inneholde

1. opplysninger om rase, eller politisk eller religiøs oppfatning
2. opplysninger om at en person har vært mistenkt, tiltalt eller dømt for straffbart forhold
3. opplysninger om helseforhold eller misbruk av rusmidler
4. opplysninger om seksuelle forhold, eller
5. andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

Kongen kan bestemme at visse typer personregistre skal være unntatt fra konsesjonsplikten etter første ledd. For slike registre kan det fastsettes forskrifter om forhold som er nevnt i § 11. Det kan også fastsettes andre forskrifter for å begrense de problemer registeret ellers kunne medføre for den enkelte, bl.a. regler om at registeret skal kontrolleres av Datatilsynet og tas med i fortegnelsen etter § 4.

Kongens myndighet etter første og annet ledd kan bare delegeres til departementet eller til Datatilsynet.

Første ledd gjelder ikke for personregistre som opprettes av Riksrevisjonen som ledd i dens kontrollvirksomhet. Slike personregistre skal slettes straks kontrollen er utført.

§ 10. Ved avgjørelsen av om samtykke skal gis, skal det – innenfor den rammen som er fastsatt i § 6 – vurderes om opprettelse og bruk av personregisteret kan volde problemer for den enkelte som ikke kan løses tilfredsstillende ved regler etter § 11. Dersom slike problemer kan oppstå, må det overveies om de blir oppveid av hensyn som taler for at registeret blir opprettet.

§ 11. Når det blir gitt samtykke etter § 9, skal det fastsettes regler for personregisteret som angir hvilke typer opplysninger registeret kan inneholde, og hva registeret kan brukes til.

I reglene kan det dessuten fastsettes slike vilkår som har betydning for bruken av registeret eller kan begrense de ulempene opprettelsen og bruken av registeret ellers kunne medføre. Særlig bør det overveies å fastsette regler om

1. innsamling og kontroll av de opplysninger registeret kan inneholde
2. behandling og lagring av disse opplysningene
3. adgangen til samkjøring med andre personregistre (kobling)
4. bruk av fødselsnummer (fødselsdato og personnummer)
5. utlevering av opplysninger, bl.a. om opplysninger kan overføres til andre registre
6. omfanget og innholdet av den informasjon som skal gis ved meldinger eller andre henvendelser til den registrerte
7. den enkeltes rett til å kreve opplysninger etter § 7
8. retting av opplysninger og rutiner i registeret
9. ajourføring av registeret
10. sletting eller ikke-bruk av opplysninger etter en viss tid, og eventuelt overføring av registeret til arkivverket

Reglene skal dessuten peke ut det organ eller foretak eller den person som har ansvar for at reglene blir gjennomført.

§ 12. Regler som er fastsatt etter § 11, kan ikke fravikes uten at det er innhentet samtykke fra det organet som fastsetter reglene, eller – når reglene bestemmer det – fra departementet eller Datatilsynet.

"Personregisterloven med forskrifter" i Kapittel 5 Kreditt- og personopplysningsvirksomhet

§ 13. Med kredittopplysningsvirksomhet menes i kapitlet her virksomhet som består i å gi meddelelser som belyser kredittverdighet eller økonomisk vederheftighet (kredittopplysning). Kapitlet gjelder ikke bruk av opplysninger innen et foretak, og heller ikke i forhold til foretak innen samme konsern med mindre opplysningene blir gitt av et foretak som driver kredittopplysningsvirksomhet. Det gjelder heller ikke avgivelse av opplysninger til annet kredittopplysningsforetak som loven gjelder for, forutsatt at opplysningene skal brukes i dette foretakets kredittopplysningsvirksomhet.

Kongen kan gi utfyllende forskrift om hva som skal reknes som kredittopplysningsvirksomhet. For visse typer foretak kan Kongen ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i kapitlet.

Foretak som driver kredittopplysningsvirksomhet, kan ikke uten samtykke fra Kongen drive annen personopplysningsvirksomhet.

§ 14. Et foretak kan ikke sette i gang kredittopplysningsvirksomhet før Kongen har gitt samtykke til det.

Ved avgjørelsen av om det skal gis samtykke, skal det legges vekt på om virksomheten kan forutsettes å ville bli drevet på en redelig og forsvarlig måte. Innenfor rammen av bestemmelsene i denne lov kan det settes slike vilkår for konsesjonen som er egnet til å fremme disse formål, bl.a. om sikkerhet for ansvar. For foretak som utenlandske interesser har bestemmende innflytelse over, kan det settes vilkår som gjelder etableringsformen og sammensetningen av selskapets ledelse.

§ 15. Kredittopplysningsforetaket skal påse at de opplysninger som brukes i kredittopplysningsøyemed, så vidt mulig er fullstendige, og at det ikke brukes opplysninger som kan danne grunnlag for ugrunnet eller urimelig avvisende holdning til den opplysningene gjelder.

En opplysning som ved kalenderårets utgang vil være 3 år gammel eller mer, kan bare brukes dersom det er åpenbart at forholdet fortsatt har vesentlig betydning for vurderingen av den opplysningene gjelder.

§ 16. Foretaket kan ikke som ledd i kredittopplysningsvirksomhet bruke

1. opplysninger om rase, eller politisk eller religiøs oppfatning
2. opplysninger om at en person har vært mistenkt, tiltalt eller dømt for straffbart forhold
3. opplysninger om helseforhold eller misbruk av rusmidler
4. opplysninger om seksuelle forhold
5. andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

Kongen kan likevel gi samtykke til at opplysninger som nevnt i første ledd nr 2 og 3 samles inn og meddeles i visse tilfelle.

§ 17. Kredittopplysning må ikke gis når det etter det som foreligger, går fram at bestilleren ikke har saklig behov for den.

§ 18. Kredittopplysning skal vanligvis meddeles skriftlig. Den kan gis muntlig dersom den ikke inneholder noe som kan bli anført mot den opplysningen gjelder,

eller kredittopplysningen av praktiske grunner må gis uten opphold. Blir en kredittopplysning gitt muntlig, skal opplysningens innhold samt bestillerens navn og adresse noteres og oppbevares minst et halvt år. Inneholder den noe som kan bli anført mot den opplysningen gjelder, skal den bekreftes skriftlig.

Kredittopplysningen kan gis ved utsending av publikasjoner eller lister, forutsatt at publikasjonen eller listen bare inneholder opplysninger om næringsdrivende, og at opplysningene er gitt i summarisk form. Slike publikasjoner kan bare sendes til medlemmer og abonnenter.

Anmodning om kredittopplysning som går ut på at bestilleren skal få vite det kredittopplysningsforetaket blir kjent med i framtiden eller i et bestemt tidsrom, kan bare omfatte opplysninger om næringsdrivende.

§ 19. Når kredittopplysning om noen som ikke er næringsdrivende blir gitt eller bekreftet skriftlig, skal kredittopplysningsforetaket samtidig vederlagsfritt sende gjenpart, kopi eller annen melding om innholdet til den det er bestilt opplysninger om.

§ 20. Alle har rett til å få opplyst hva foretaket har lagret om dem selv til bruk i kredittopplysningsøyemed, og til å få opplyst hvilke kredittopplysninger som er gitt om dem de siste seks måneder. Foretaket plikter også å opplyse hvem som har bestilt opplysningene, og hvem det har mottatt opplysningene fra. Svar skal gis skriftlig om ikke vedkommende har samtykket i at det blir gitt på annen måte. Blir opplysning om hva et register inneholder gitt i form av et sammendrag, eller har foretaket lagret opplysninger som ikke gjengis fullstendig, skal dette sies i svaret. Den opplysningene gjelder, kan kreve å få gjennomgå alle dokumenter m.m. ved henvendelse til foretaket.

Foretaket kan beregne seg en rimelig godtgjørelse når opplysning etter første ledd første punktum blir gitt skriftlig. Kongen kan ved forskrift eller enkeltvedtak gi nærmere regler om beregning av godtgjørelsen.

§ 21. Kongen kan ved forskrift fastsette at § 14 om konsesjonsplikt skal gjelde også for andre foretak som driver personopplysningsvirksomhet. I konsesjonen kan det settes vilkår om innsamling, lagring og bruk av opplysningene, samt om kontroll, om innsynsrett for den opplysningene gjelder og om rett til å kreve seg slettet av register.

"Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern" i Kapittel 6 Databehandlingsforetak

§ 22. Virksomhet som består i å bearbeide personopplysninger for andre ved elektroniske hjelpemidler, må ikke settes i gang før Kongen har gitt samtykke til det. § 14 annet ledd gjelder tilsvarende.

Første ledd gjelder ikke dersom bearbeidelsen utelukkende skjer for andre foretak innen samme konsern.

Kongen kan gi utfyllende forskrifter om hva som skal reknes som databehandlingsforetak ved anvendelse av første ledd, og kan ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i dette kapitlet.

§ 23. Foretak som må ha konsesjon etter § 22 første ledd, må ikke uten avtale med oppdragsgiveren anvende opplysningene til andre formål enn det oppdraget gjelder. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.

§ 24. Foretaket skal treffe de sikringstiltak som trengs. Kongen kan ved forskrift eller for det enkelte foretak gi bestemmelser om de sikringstiltak som skal gjennomføres.

*"Europarådets konvensjon og rekommandasjoner om persondatabeskyttelse" i
Kapittel 7 Adresserings- og distribusjonsvirksomhet*

§ 25. Virksomhet som består i å selge eller på annen måte tilby adresser for grupper av personer, eller i å utføre oppdrag for utsending av reklame og andre meddelelser til slike grupper, kan ikke settes i gang før Kongen har gitt samtykke til det. § 14 annet ledd gjelder tilsvarende.

Kongen kan gi utfyllende forskrift om hvilke foretak som er konsesjonspliktige etter første ledd, og kan ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i kapitlet.

§ 26. Et register til bruk for virksomhet som er nevnt i § 25 første ledd, kan ikke inneholde

1. opplysninger om rase, eller politisk eller religiøs oppfatning
2. opplysninger om at en person har vært mistenkt, tiltalt eller dømt for straffbart forhold
3. opplysninger om helseforhold eller misbruk av rusmidler
4. opplysninger om seksuelle forhold
5. andre opplysninger om familieforhold enn slike som gjelder slektskap eller familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

Kongen kan ved forskrift eller enkeltvedtak ytterligere begrense foretakets adgang til å registrere personopplysninger, og regulere bruken av registrerte opplysninger.

§ 27. Uten hinder av bestemmelsene i § 26 kan foretaket sende meldinger på grunnlag av kunde- og medlemsregistre som stilles til rådighet av oppdragsgiveren. Slike registre må bare nyttes til å sende meldinger om oppdragsgiverens varer eller tjenester o.l., og de kan ikke overlates til andre.

§ 28. Foretaket skal i sine registre slette enhver som ber om det. En registrert kan kreve å få opplyst hvem som er foretakets kilde for registreringen.

Gjelder kravet om sletting slikt register som er nevnt i § 27, skal kravet sendes til oppdragsgiveren, som plikter å påse at vedkommende blir strøket som adressat ved seinere bruk av registeret. Den som har satt fram kravet, skal underrettes om videresendingen og om oppdragsgiverens navn.

§ 29. Kongen kan ved forskrift eller for det enkelte foretak gi bestemmelser med sikte på å hindre at personopplysninger blir brukt i strid med § 26 og § 27 og for å sikre gjennomføringen av reglene i § 28.

§ 30. Kongen kan ved forskrift bestemme

1. at § 26, § 27, § 28 skal gjelde tilsvarende for foretak som i enkeltstående tilfeller påtar seg oppdrag som er nevnt i § 25 første ledd,
2. at visse typer opplysninger ikke skal kunne anvendes for utvalg av adressater ved utsending av meldinger for foretakets egne varer og tjenester o.l., samt at § 28 skal gjelde tilsvarende for slike adresselister.

"Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger" i Kapittel 8 Opinions- og markedsundersøkelser

§ 31. Virksomhet som består i å utføre opinions- eller markedsundersøkelser for andre, kan ikke settes i gang før Kongen har gitt samtykke til det. § 14 annet ledd gjelder tilsvarende.

Kongen kan gi utfyllende forskrift om hvilke foretak som er konsesjonspliktige etter første ledd, og kan ved forskrift eller enkeltvedtak gjøre unntak fra de enkelte bestemmelser i dette kapitlet.

§ 32. Personopplysninger som noen gir under opinions- eller markedsundersøkelser, må ikke meddeles videre i en slik form at opplysningen kan henføres til en enkelt person.

Opplysninger som er mottatt for opinions- og markedsundersøkelser, må ikke brukes for andre formål.

§ 33. Uten samtykke fra den opplysningene gjelder, må opplysning om navn, fødselsdato, fødselsnummer eller liknende ikke innføres i register som bearbeides ved elektroniske hjelpemidler. Heller ikke må slike opplysninger innføres i et annet register som er særskilt utformet med sikte på at opplysningene skal være lett tilgjengelige og anvendelige.

Uten samtykke fra den opplysningen gjelder, må innsamlete opplysninger ikke lagres i mer enn et halvt år i slik form at de kan henføres til en enkelt person.

§ 34. Kongen gir nærmere forskrifter om slik virksomhet som er nevnt i § 31. Forskriftene kan bl.a. inneholde bestemmelser om innhenting av opplysninger, om lagring av innhentete opplysninger, og andre bestemmelser som skal sikre at innsamlete personopplysninger ikke nyttes på urett måte eller kommer på urette hender.

§ 35. Kongen kan ved forskrift bestemme at § 32, § 33, § 34 skal gjelde også for foretak som i enkeltstående tilfelle påtar seg slike oppdrag som er nevnt i § 31 første ledd, og for foretak som setter i verk slike undersøkelser for sin egen administrasjon og virksomhet.

"Oversikt over andre internasjonale reguleringer og andre lands rett" i Kapittel 9 Overføring til utlandet, m.m.

§ 36. Register som omfattes av § 9 første ledd må ikke overføres til utlandet uten samtykke av Kongen.

Personopplysninger som er innsamlet her i riket, må ikke overføres til utlandet uten samtykke av Kongen når formålet er å innføre opplysningene i et register som nevnt i § 9 første ledd.

Kongen kan ved forskrift gjøre unntak fra første og annet ledd. Det kan fastsettes at disse bestemmelser ikke skal gjelde i forhold til enkelte andre land.

§ 37. Kongen kan gi forskrift om samarbeid mellom Datatilsynet og tilsynsmyndigheter i andre land. I slik forskrift kan det fastsettes særlige regler om meldeplikt for registre og om kontroll med eller tilintetgjøring av registre.

"Oversikt over andre internasjonale reguleringer og andre lands rett" i Kapitel 9 a Fjernsynsovervåkning

§ 37 a. Fjernsynsovervåkning og billedopptak i forbindelse med slik overvåkning er bare tillatt dersom det er saklig begrunnet ut fra hensynet til virksomheten i det organ eller foretak som foretar overvåkingen. Ved overvåkning av sted hvor en begrenset krets av personer jevnlig ferdes, er overvåkingen likevel bare tillatt dersom det ut fra hensynet til virksomheten er et særskilt behov for overvåkingen.

Billedopptakene skal slettes når det ikke lenger er saklig grunn for oppbevaring.

Med fjernsynsovervåkning menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller liknende apparat.

Kapitlet her gjelder ikke for billedopptak som er å anse som personregistre. Kongen kan i tvilstilfelle bestemme når billedopptak som er gjort ved fjernsynsovervåkning, skal anses som personregistre etter § 1 annet ledd.

§ 37 b. Billedopptak gjort ved fjernsynsovervåkning kan bare utleveres til noen utenfor det foretak eller organ som har foretatt opptaket, dersom den som er avbildet samtykker eller utleveringsadgangen følger av lov. Hvis ikke lovbestemt taushetsp-

likt er til hinder for utlevering, kan billedopptak likevel utleveres til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker. Kongen kan i forskrift eller i det enkelte tilfelle fastsette at billedopptak kan utleveres utover det som er bestemt i første og annet punktum.

Kongen kan i forskrift fastsette nærmere regler om sikring, bruk, utlevering og sletting av billedopptak gjort ved fjernsynsovervåkning. Kongen kan også fastsette forskrift om innsynsrett for den som er overvåket, i de deler av billedopptakene hvor han eller hun er avbildet.

Dersom billedopptak ikke slettes i samsvar § 37a annet ledd eller forskrift fastsatt i medhold av annet ledd i paragrafen her, kan Datatilsynet gi pålegg om sletting.

"Lovens saklige og geografiske virkeområde" i Kapittel 10 Straff og erstatning

§ 38. Med bøter eller fengsel inntil ett år eller begge deler straffes den som forsettlig eller aktløst

1. unnlater å innhente samtykke etter § 9, § 13 tredje ledd, § 14, § 22, § 25, § 31 eller § 36
2. overtrer regler eller vilkår fastsatt etter § 11, § 14, § 22, § 25, § 31, § 36 eller § 37 b
3. bruker opplysninger i strid med reglene i § 16, § 18, § 23, § 26, § 27, § 32, § 33 eller § 37 b
4. unnlater å etterkomme krav fra Datatilsynet etter § 5, § 8 eller § 37 b
5. unnlater å etterkomme krav om opplysninger etter § 7, § 20 eller § 37 b eller krav om sletting etter § 28 eller § 37 b
6. unnlater å gi melding etter § 19 til den opplysningen gjelder.

Medvirkning straffes på samme måte.

I forskrift som gis i medhold av loven, kan det fastsettes at overtredning av forskriften skal straffes med bøter eller fengsel inntil ett år eller begge deler.

§ 39. (Opphevet ved lov 20 juli 1991 nr 66)

§ 40. Har foretak som driver virksomhet som nevnt i § 13, meddelt opplysninger i strid med bestemmelser gitt i eller i medhold av loven her, eller meddelt opplysninger som viser seg uriktige eller åpenbart misvisende, skal foretaket erstatte det tap som påføres den opplysningene gjelder. Dette gjelder uten hensyn til om det er utvist skyld fra noen som har opptrådt på vegne av eller i tjeneste hos foretaket.

"Individuelle personverngarantier" i Kapittel 11 Forholdet til andre lover. Ikraftsetting. Overgangsregler

§ 41. Konesjonsplikten etter § 9 jfr. § 10 gjelder ikke for personregistre i organ for stat eller kommune som er opprettet ved egen lov. Også for slike registre skal det likevel fastsettes regler som nevnt i § 11, i den utstrekning det ikke er fastsatt noe annet i eller i medhold av heimelsloven. Også de andre bestemmelsene i loven gjelder for slike registre i den utstrekning ikke annet følger av hjemmelsloven.

§ 42. Loven trer i kraft den dag Kongen bestemmer.

For personregistre som er opprettet før loven trer i kraft, og som omfattes av § 9, skal det søkes om samtykke innen en frist som Kongen fastsetter. Forutsatt at søknad er kommet inn innen fristen, kan personregisteret brukes uendret inntil det er fastsatt regler etter § 11.

Reglene i annet ledd gjelder tilsvarende når det kreves samtykke etter "*Personregisterloven med forskrifter*" i kapitlene 5 til 9.

§ 43. Fra loven trer i kraft gjøres følgende endringer i andre lover: – – –

FORSKRIFTER I MEDHOLD AV LOV OM PERSONREGISTRE M.M.

Gitt av Justisdep 21 des 1979 i medhold av kgl.res av 21 desember 1979, sist endret 2 desember 1996.

"Sammendrag av personregisterlovutvalgets utredning" i Kap. 1 Om innsynsretten.

(personregisterloven § 7 fjerde og femte ledd).

§ 1-1.

Svar på henvendelser som nevnt i personregisterlovens § 7 første ledd skal gis snarest mulig og senest innen en måned.

Svaret skal gis skriftlig dersom ikke den som benytter innsynsretten samtykker i at svaret gis muntlig eller på annen måte.

§ 1-2.

Svar på henvendelser som nevnt i personregisterloven § 7 annet ledd skal gis snarest mulig og senest innen en måned. Dersom innsynsretten kan motvirke muligheten for å få en sak som er under behandling avklart, kan institusjonen fastsette at vedkommende ikke skal ha adgang til opplysningene så lenge undersøkelser pågår, (jfr forvaltningsloven § 20 første ledd).

Den registeransvarlige bestemmer ellers, ut fra hensynet til forsvarlig saksbehandling, hvordan dokumentene eller opplysningene skal gjøres tilgjengelige for vedkommende. På anmodning skal vedkommende gis skriftlig svar ved utskrift eller avskrift fra registeret.

§ 1-3.

Svar på henvendelser som nevnt i personregisterlovens § 7 tredje ledd skal gis umiddelbart.

Svaret skal gis skriftlig dersom ikke den som benytter innsynsretten samtykker i at svaret gis muntlig eller på annen måte.

§ 1-4.

Datatilsynet gis myndighet som nevnt i personregisterlovens § 7 femte ledd til ved enkeltvedtak å fastsette unntak fra innsynsretten. Datatilsynet kan også ved enkeltvedtak fastsette nærmere regler eller vilkår for bruk av retten, herunder unntak fra reglene i dette kapittel.

§ 1-5.

Innsynsrett etter lovens § 7 annet ledd i opplysninger som ikke lagres eller bearbeides ved elektroniske hjelpemidler, skal også gjelde for de registre over nåværende eller tidligere ansatte, personale eller representanter som finnes i privat næringsvirksomhet, foreninger eller stiftelser, jfr lovens § 7 fjerde ledd.

Som interne dokumenter som etter § 7 annet ledd kan unntas fra innsyn, skal i denne sammenheng regnes alle dokumenter arbeidsgiver selv utarbeider for sin interne saksforberedelse samt dokumenter som er utarbeidet for den interne saks-

forberedelse av særskilte rådgivere eller sakkyndige, eller av annen sammenslutning eller stiftelse innenfor eget konsern eller organisasjon.

Også dokumenter om å innhente dokumenter nevnt i denne bestemmelse kan unntas fra innsyn.

Selv om dokument er unntatt etter annet og tredje ledd bør vedkommende ha rett til å gjøre seg kjent med de deler av dokumentet som inneholder faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum. Dette gjelder likevel ikke faktiske opplysninger som finnes i annet dokument som vedkommende har innsyn i.

"Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte" i Kap. 2 Unntak fra konsesjonsplikt (personregisterloven § 9 annet ledd).

§ 2-1. Unntak fra konsesjonsplikt

Personregistre som omfattes av dette kapitlet er unntatt fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Konsesjonsfrihet er betinget av at kravene til registerets innhold m.m. i kapitlet her følges, og at bestemmelsene i *"Hva er personvern?"* i kapittel 3 overholdes.

§ 2-2. Foreningers medlemsregistre

Foreningers medlemsregistre unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register menes en oversikt over en forenings nåværende og tidligere medlemmer, og som ikke inneholder andre personopplysninger enn:

1. navn
2. adresseopplysninger (bosteds-, arbeids-, adviserings-, tilskriver-, elektronisk adresse m.v.)
3. anropsnummer for teletjenester
4. fødselsdato
5. fødselsnummer, dersom dette er pålagt i lov eller forskrift gitt med hjemmel i lov
6. utdanning, stilling, arbeidsgiver
7. inntekt
8. sivil status
9. kjønn
10. statsborgerskap
11. spesielle interesser i tilknytning til foreningen etter samtykke fra den registrerte
12. medlemsnummer
13. medlemskoder (opplysninger om type medlemskap o.l.)
14. tillitsverv
15. data for distribusjon av trykksaker, publikasjoner o.l.
16. kurs, utdanning o.l. innen foreningen eller i tilknytning til denne
17. kontingentopplysninger
18. utlånte eiendeler
19. resultater fra idrettskonkurranser o.l.
20. foresattes navn, adresse og anropsnummer for teletjenester.

Registeret kan bare brukes som ledd i foreningens administrasjon eller interne virksomhet. Annen bruk kan fastsettes av foreningens høyeste organ eller i foreningens vedtekter.

§ 2-3. Kunde-, abonnent- og leverandørregistre

Kunde-, abonnent- og leverandørregistre unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register menes en oversikt over kunder, abonnenter eller leverandører, som ikke inneholder andre personopplysninger enn:

1. navn
2. adresseopplysninger
3. anropsnummer for teletjenester
4. fødselsdato
5. organisasjonsnummer
6. kontaktnummer og kontaktperson
7. konsernopplysninger
8. kontonummer bank/ post og andre opplysninger i den sammenheng
9. rubriseringsdata (så som kategori kunde/ leverandør, distrikt, type varer, kontonummer i regnskap, kunde-/ leverandørnummer, andre opplysninger til bruk i statistikk og annen bedriftsintern avregning og andre opplysninger som ikke angår fysiske personer eller personlige forhold)
10. inkasso- og utbetalingsopplysninger
11. saldoinformasjon
12. kredittgrense
13. betalingsbetingelser
14. aldersfordeling av saldoposter
15. purringsstatus.

Registeret kan bare brukes til administrasjon og gjennomføring av kontraktsforpliktelser. Dette er ikke til hinder for at opplysninger benyttes i adressemekling av et adresserings- eller distribusjonsforetak som har konsesjon etter loven § 25 når dette skjer etter avtale med registerets eier.

§ 2-4. Kunderegistre i banker og finansinstitusjoner

Kunderegistre i banker som omfattes av

- lov 1. mars 1946 nr. 3 om Den Norske Stats Husbank
- lov 15. juli 1949 nr. 1 om Norges Kommunalbank
- lov 24. mai 1961 nr. 1 om sparebanker
- lov 24. mai 1961 nr. 2 om forretningsbanker
- lov 5. februar 1965 nr. 2 om Statens Landbruksbank
- lov 28. april 1972 nr. 22 om Statens Fiskarbank
- lov 5. juni 1992 nr. 51 om Norges Postbank

og kunderegistre i finansinstitusjon, jf. lov 10. juni 1988 nr. 40 om finansieringsvirksomhet § 1-3, som etableres i forbindelse med institusjonens finansieringsvirksomhet unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

I det enkelte kunderegister kan det ikke registreres andre personopplysninger enn:

1. Kundeopplysninger

Med kundeopplysninger menes personopplysninger om bankens kunder, kausjonister og andre som banken har saklig behov for opplysninger om på grunn av deres forhold til kunden (jf. personregisterloven § 6 første ledd). Følgende kundeopplysninger kan registreres:

- a) navn
- b) adresseopplysninger

- c) anropsnummer for teletjenester
- d) fødselsnummer
- e) organisasjonsnummer
- f) kjønn
- g) statsborgerskap
- h) antall konti (egne, kausjonist, garantist o.l.)
- i) sivilstand
- j) stillingsbetegnelse
- k) notatfelt med rent administrative opplysninger om kundeforholdet (disposisjonsforhold, sperringer o.l.). Personopplysninger som nevnt i personregisterloven § 6 annet ledd tillates ikke registrert i notatfeltet
- l) kundetype og kundehode
- m) formues- og inntektsforhold, og beløpsangivelse for beregnet kredittverdighet, samt kredittopplysninger
- n) kundedataopplysninger (opprettelse, avslutning o.l.)
- o) henvisninger til andre som banken har saklig behov for å registrere på grunn av deres forhold til kunden (kausjonister, garantister, konsern, datterselskap, arbeidsgiver e.l.)
- p) firmaattest
- q) andre opplysninger om kundens ektefelle/ samboer/ registrert partner enn de som kan registreres etter litra o) ovenfor, når denne har gitt samtykke til registreringen.

2. Konto- og oppdragsopplysninger

Med konto- og oppdragsopplysninger menes opplysninger om de enkelte konti eller oppdrag. Følgende konto- og oppdragsopplysninger kan registreres:

- a) kontonummer og oppdragsnummer
- b) andre numre i tilknytning til kontoen (depotnummer, disponentnummer, bankkortnummer, kausjonistnummer, betalingskontonummer, aksjenummer m.v.)
- c) åpnings-, endrings-, avslutningsdato og andre datoopplysninger vedrørende kontoen eller oppdraget
- d) rente-, dekort-, provisjonsbetingelser og gebyrer
- e) saldi, gebyrbeløp, rentebeløp debet/ kredit, omkostninger, provisjoner, agio og andre statusopplysninger
- f) avdrags-, termin- og forfallsopplysninger
- g) opplysninger om purringer, overtrekk og inkasso
- h) disposisjonsopplysninger, stikkord
- i) innvilgede lån
- j) opplysninger om stillet sikkerhet (prioritet, takst, utløpsdatoer o.l.)
- k) henvisningsopplysninger av betydning for disponeringen av kontoen eller oppdraget
- l) notatfelt med rent administrative opplysninger om kontoen eller oppdraget (disposisjonsforhold, sperringer o.l.). Personopplysninger som nevnt i personregisterloven § 6 annet ledd tillates ikke registrert i notatfeltet
- m) kontoanalysedata
- n) betalingsmottakeres/ kreditorers kontonummer, navn, adresse og fødselsnummer
- o) opplysninger som er nødvendige for å hindre uttak på sperret konto.

3. Transaksjonsopplysninger

Med transaksjonsopplysninger menes opplysninger som registreres i forbin-

delse med bruk av kontoen, inklusive transaksjoner som tilføres automatisk slik som renter, provisjoner o.l.

Følgende transaksjonsopplysninger kan registreres:

- a) transaksjonsbeløp og valutasort
- b) arkivreferanse og terminalidentifikasjon
- c) ID-nummer (ikke fødselsnummer), bilagsnummer, sjekknnummer o.l.
- d) tekstkode, tekst og annen beløpsidentifikasjon
- e) bokføringsdato, valuteringsdato og andre tidsbestemmelser av transaksjonsforløpet
- f) henvisninger til motpost
- g) førings- og behandlingkoder.

4. Administrative opplysninger og interne referanser

I tilknytning til opplysninger som nevnt i punkt (1) til og med (3) ovenfor, kan det registreres administrative opplysninger som systemet må benytte for at det skal kunne arbeide i samsvar med de kunde-, konto-, oppdrags- og transaksjonsopplysninger som er nevnt. Dessuten kan det registreres interne referanser som bare benyttes for å vise til andre rutiner eller registre, og som ellers ikke har behandlingmessige konsekvenser.

5. Statistikk

Felter for klassifikasjon og koding av opplysninger til å utarbeide offentlig og intern statistikk for personopplysninger som tillates registrert etter punkt (1) til og med (3) ovenfor. Statistikk må ikke utarbeides i en slik form at opplysningene direkte eller indirekte kan føres tilbake til den enkelte konto eller kunde.

Kunderegistre i banker og kunderegistre i andre finansinstitusjoner som etableres i forbindelse med institusjonens finansieringsvirksomhet, kan bare benyttes i forbindelse med innlån, utlån, betalingsformidling, inkasso, forvaltning og andre ordinære bank- og finanstjenester. Dette er ikke til hinder for at opplysninger benyttes i adressemekling av et adresserings- eller distribusjonsforetak som har konsesjon etter loven § 25 når dette skjer etter avtale med registerets eier.

§ 2-5. Katalogfirmaregistre

Registre som opprettes for utgivelse av katalog, bok e.l. unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd, så langt det ikke registreres sensitive opplysninger, jf. personregisterloven § 6 annet ledd, og den registrerte har hatt anledning til å verifisere opplysningene.

Registeret kan bare brukes for utgivelse av katalog, bok e.l.

§ 2-6. Leietaker- og sameieregistre

Leietaker- og sameieregistre unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register menes en oversikt over registreierens leietakere eller sameiere i et boligsameie, som ikke inneholder andre personopplysninger enn:

1. navn
2. adresseopplysninger
3. anropsnummer for teletjenester
4. fødselsnummer, dersom dette er pålagt i lov eller i forskrift gitt med hjemmel i lov
5. medlemsnummer i borettslag
6. ansiennitetsopplysninger til bruk ved tildeling av leilighet

7. medlemskontingentbeløp
8. leilighetsnummer og adresse
9. leilighetstype og størrelse
10. leilighetens alder
11. leilighetens verdi (takst) ved omsetning
12. leilighetens omsetningsform
13. leiebeløp/ sameieavgift fordelt på art (husleie, garasje, fyring etc.)
14. medlemmets/ sameierens/ beboerens tilknytning til leilighet (eier, fremleier, leietaker etc.)
15. dato for innflytning
16. betaling/ restansedata for kontingentinnkreving
17. betaling/ restansedata for innkreving av leie, sameieavgift, fellesavgifter, m.v.
18. oversikt over tidligere leietakere til bruk ved fordeling av ligningsmessig underskudd/ overskudd i borettslag
19. gjeld/ formue
20. kontonummer for automatisk belastning av leie på konto
21. andre rent administrative opplysninger.

Registeret kan bare brukes til administrasjon og gjennomføring av leie-/sameieforholdet.

Paragrafen gjelder tilsvarende for boligaksjeselskaper.

§ 2-7. Registre for utsendelse av trykksaker o.l. (salgsstøtteregistre)

Registre over juridiske og fysiske personer, for utsendelse av publikasjoner/trykksaker o.l. vedrørende egen virksomhet unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Et slikt register over fysiske personer kan bare inneholde følgende opplysninger:

1. navn
2. adresseopplysninger
3. anropsnummer for teletjenester
4. fødselsår.

Registeret kan bare brukes for utsendelse av egne publikasjoner/ trykksaker o.l.

§ 2-8. Katalog-, låner- og utlånsregistre

Katalog-, låner- og utlånsregistre i bibliotek og liknende registre unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et katalogregister menes et register over titler som brukes som et hjelpemiddel og som kun inneholder bibliografiske personopplysninger.

Med et lånerregister menes en oversikt over samtlige lånere som ikke inneholder andre personopplysninger enn:

1. lånenummer
2. navn
3. adresseopplysninger
4. anropsnummer for teletjenester
5. fødselsdato
6. arbeidssted
7. dato for utsendelse av lånekortet
8. opplysninger om utlånte (ikke tilbakeleverte) gjenstander og uoppgjorte tjenester.

Med et utlånsregister menes en fortegnelse over hver enkelt utlånt gjenstand (så som bok, film, video e.l.) og som kun inneholder personopplysninger som er nødvendige for utleien.

Katalog-, låner- og utlånsregister kan bare brukes for administrasjon av virksomheten og kundeforholdet og for å sikre at utlånte gjenstander blir tilbakelevert.

§ 2-9. Advokaters, revisorers og fonds- og eiendomsmegleres klientregistre

Personregistre som opprettes i forbindelse med virksomhet som nevnt i lov 13. august 1915 nr. 5 "*Individuelle personverngarantier*" i kapittel 11 om advokater, lov 14. mars 1964 nr. 2 om revisorer, lov 14. juni 1985 nr. 61 om fondsmeglere og lov 16. juni 1988 nr. 53 om eiendomsmegling unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med et slikt register menes en fortegnelse over tidligere og nåværende klienter og motparter, samt andre med tilknytning til disse.

Registeret kan bare brukes innenfor rammene av lovgivning som nevnt i første ledd.

§ 2-10. Legers, tannlegers, psykologers og annet godkjent helsepersonells registre

Godkjent helsepersonells pasientregistre som ikke gjør bruk av elektroniske hjelpemidler unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Registeret kan bare brukes i behandlingen og oppfølgingen av den enkelte pasient samt til utarbeidelse av statistikk.

§ 2-11. Aksjeeierregistre

Aksjeeierregistre opprettet i medhold av lov 4. juni 1976 nr. 59 om aksjeselskaper § 3-8 unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd, dersom det ikke inneholder slike opplysninger som nevnt i § 6 annet ledd.

Registeret kan bare brukes for å ivareta de forpliktelser aksjelovgivningen pålegger det enkelte selskap.

§ 2-12. Personalregistre

Register over arbeidsgivers nåværende eller tidligere ansatte, personale, representanter, innleid arbeidskraft samt søkere til en stilling, unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd dersom

1. registeret ikke gjør bruk av elektroniske hjelpemidler, og ikke inneholder personopplysninger som nevnt i personregisterloven § 6 annet ledd, med mindre opplysningene er knyttet til arbeidsforholdet.
2. registeret gjør bruk av elektroniske hjelpemidler og ikke inneholder andre opplysninger enn:
 1. navn
 2. adresseopplysninger
 3. statsborgerskap/ bostedland
 4. anropsnummer for teletjenester
 5. fødselsnummer og annet nummer knyttet til person (rullenummer/ arbeidstakernummer)
 6. rubriseringsdata, (såsom kategori, type ansatt/ representant, distrikt, type varer, kontonummer i regnskap, representantkategori, andre opplysninger til bruk i statistikk og annen bedriftsintern avregning)
 7. kjønn

8. nærmeste pårørende
9. sivilstand
10. antall barn og barnas fødselsår
11. stillingsbetegnelse
12. yrkesopplysninger som etter overenskomst eller tariffavtale som har betydning for lønns- og arbeidsvilkår
13. opplysninger om utdanning og praksis
14. lønns- og provisjonsopplysninger
15. kontonummer
16. pensjonsopplysninger
17. trekk- og skatteopplysninger
18. ansettelses- og sluttdato (permisjoner e.l.)
19. sluttårsak
20. fraværsgang, type fravær og varighet. Angivelse av sykdommens art tillates ikke registrert utover det som er pålagt ved lov 4. februar 1977 nr. 4 om arbeidervern og arbeidsmiljø m.v. § 20
21. dødsdato
22. firmabil e.l.
23. utlånte eiendeler
24. lån til ansatte eller garanti for lån
25. opplysning om den ansatte er mobiliseringsdisponert (ja/nei), evt. militært løpenummer, grad og rulleførende avdeling.

Andre opplysninger kan registreres dersom det er pålagt i lov eller gjennom avtale mellom partene i arbeidslivet.

Personalregisteret kan bare brukes til personaladministrasjon, for eksempel administrering av lønn, utvikling og opplæring, stillingsevaluering, erstatningsplanlegging, karriereplanlegging, budsjettmessige formål, velferdstiltak og til behandling av disiplinærsaker.

§ 2-13. Forlagenes personregistre for utgivelse av leksika

Forlagenes personarkiver/ registre til bruk ved utgivelse av biografiske leksika, konversasjonsleksika og fagleksika unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

§ 2-14. Dags- og ukepressens personregistre

Dags- og ukepressens personregister til bruk i journalistisk virksomhet unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

§ 2-15. Register over offentlige representanter

Register over valgte eller oppnevnte representanter i organ opprettet i medhold av lov 25. september 1992 nr. 107 om kommuner og fylkeskommuner eller lov 19. desember 1952 nr. 7 om Den norske kirkes ordning unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Det samme gjelder for registre over Stortingets representanter eller medlemmer av Stortingets komiteer.

§ 2-16. Protokollføring av mekling

Registre ved føring av meklingsprotokoll pålagt etter lov 8. april 1981 nr. 7 (barneloven) og lov 4. juli 1991 nr. 47 (ekteskapsloven) unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Med slike registre menes manuelle eller elektronisk førte meklingsprotokoller, som ikke inneholder andre opplysninger enn:

1. navn/ eventuelt tidligere navn
2. fødselsnummer
3. adresseopplysninger
4. meklingsinstansens navn
5. meklers navn
6. dato for innkommet begjæring om mekling
7. dato for innkalling
8. hvem har begjært mekling
9. hjemmel for innkalling
10. dato for møter
11. dato for fremmøte, sammen/ hver for seg
12. fremgangsmåte for innkalling
13. dato for utstedt meklingsattest
14. dato for avsluttet mekling uten meklingsattest.

Registeret kan bare brukes til kontroll av at mekling har funnet sted, evaluering og planlegging av meklingsordningen og som grunnlag for statistiske analyser.

§ 2-17. Forskningsregistre

Registre som opprettes i forbindelse med et forskningsprosjekt unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd, så langt

- a) prosjektet baserer seg på frivillig deltagelse fra de registrerte, og
- b) førstegangskontakt opprettes gjennom faglig ansvarlig person ved den institusjon respondenten er registrert, og
- c) respondenten har gitt skriftlig samtykke til alle deler av undersøkelsen, og
- d) det innsamlede materialet anonymiseres eller slettes ved prosjektavslutning, og
- e) prosjektet har en fastsatt prosjektavslutning innen 5 år fra prosjektstart.

Registeret kan bare brukes i samsvar med prosjektets formål og den registrertes samtykke. Dersom prosjektet innebærer kobling av registre kreves særskilt tillatelse fra Datatilsynet for dette.

§ 2-18. Domstolenes registre

Personregistre som opprettes i forbindelse med domstolenes virksomhet (herunder registrerings- og notarialforretninger og lignende som utføres ved et dommerkontor) unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Registrene må bare brukes innenfor rammene av domstolenes virksomhet.

§ 2-19. Elektroniske arkiv

Elektroniske arkiv ført i lukket edb-system unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Elektronisk arkiv i delt edb-system unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd dersom det ikke inneholder opplysninger som nevnt i

personregisterloven § 6 annet ledd. Med delt edb-system menes et edb-system som er tilgjengelig, eller kan være tilgjengelig for uvedkommende.

Elektronisk arkiv omfatter i denne sammenheng elektronisk ført postjournal, arkivkatalog, korrespondansearkiv og dokumentasjonsarkiv i den grad disse utgjør et personregister i henhold til personregisterloven § 1 annet ledd. Med elektronisk postjournal menes en oversikt over inn- og utgående post, og annen dokumentasjon som det anses formålstjenlig å arkivere. Med elektroniske dokumentasjonsarkiv og korrespondansearkiv menes elektroniske arkiv over dokumentasjon som ligger lagret i fulltekst. Med elektroniske arkivkataloger menes en oversikt over arkivert materiale og tilhørende opplysninger om arkivskapere.

Elektronisk postjournal og arkivkatalog som inneholder sensitive opplysninger og som benyttes av flere instanser (delt edb-system) unntas likevel fra konsesjonsplikten så fremt det enkelte organ kun får tilgang til opplysninger i egne saker.

Arkivet kan bare brukes til å ivareta de oppgaver foretaket/ institusjonen har, herunder å sikre bevaring av arkiver i tråd med lov 4. desember 1992 nr. 126 (arkivloven).

§ 2-20. Aktivitetslogg i et edb-system eller datanett

Register over aktiviteter (hendelser) internt i et edb-system eller datanett, samt register over disposisjoner til ressurser internt i systemet unntas fra konsesjonsplikten etter personregisterloven § 9 første ledd.

Registeret kan bare brukes til administrasjon av systemet, og til å avdekke/ oppklare brudd på sikkerheten i edb-systemet.

§ 2-21. Personregistre som utleveres elektronisk

Dersom det i konsesjonen til et personregister er gitt tillatelse til å utlevere personregisteret elektronisk, unntas det utleverte registeret fra konsesjonsplikten etter personregisterloven § 9 første ledd.

"Hva er personvern?" i Kapittel 3 Nærmere om personregistre unntatt fra konsesjonsplikt

(personregisterloven §§ 9 annet ledd og 8b)

§ 3-1. Formål

Personregistre som er unntatt fra konsesjonsplikt kan bare benyttes til de formål som følger av § 2-2 til § 2-21.

§ 3-2. Registeransvarlig

Virksomhetens ledelse er ansvarlig for at bestemmelsene i personregisterloven og denne forskrift blir fulgt (registeransvar).

Den registeransvarlige plikter å føre oversikt over hvilke personregister som vedkommende har registeransvaret for. Oversikten skal vise hvilke typer opplysninger registeret kan inneholde og hva det kan brukes til, og være offentlig tilgjengelig.

§ 3-3. Sikring

Den registeransvarlige må sørge for nødvendig sikring av konfidensialitet, kvalitet og tilgjengelighet for personopplysninger og registre.

Den registeransvarlige skal godkjenne alle brukere av registeret, samt drifts- og vedlikeholdspersonale. Enhver bruker av et elektronisk register skal entydig identifiseres og autentiseres av registersystemet før tilgang til registeret.

Datatilsynet kan gi pålegg som ansees nødvendige for å oppnå forsvarlig sikring. For organ i staten vises for øvrig til Beskyttelsesinstruksen, Sikkerhetsinstruksen

med utfyllende bestemmelser og Datasikkerhetsdirektivet. Denne paragrafen gjelder ikke for registre som nevnt i § 2-15.

§ 3-4. Utlevering

Personopplysninger må ikke utleveres fra registeret til utenforstående, unntatt når utleveringen skjer

- a) med samtykke fra den opplysningen gjelder,
- b) med hjemmel i lov, eller i forskrift gitt med hjemmel i lov,
- c) som ledd i betalingsinnkreving,
- d) som ledd i regnskap- og revisjonsbehandling,
- e) med hjemmel i avtale mellom partene i arbeidslivet,
- f) til annen sammenslutning eller stiftelse innenfor eget konsern (jf. lov 4. juni 1976 nr. 59 om aksjeselskaper § 1-2 og lov 21. juni 1985 nr. 83 om ansvarlige selskaper og kommandittselskaper § 1-2 (2)) når utleveringen ikke strider mot registerets formål eller lovbestemt taushetsplikt,
- g) fra registre som nevnt i § 2-4 til annen bank eller finansinstitusjon, etter beslutning fra styret eller noen som har fullmakt fra styret til å avgjøre spørsmål om utlevering,
- h) fra registre som nevnt i § 2-2 og § 2-12 som nødvendig ledd i opprettelse og administrasjon av kollektive forsikringsordninger,
- i) fra registre som nevnt i § 2-12 til registre for utarbeidelse av lønnsstatistikk som har konsesjon etter personregisterloven § 9, dersom ikke annet er bestemt i avtale mellom partene i arbeidslivet,
- j) fra registre som nevnt i § 2-12 til utarbeidelse av kataloger eller lister over arbeidstakers interne telefonnummer, besøksadresse og stillingsbenevnelse,
- k) fra medlemsregistre som nevnt i § 2-2 dersom dette er tillatt i henhold til vedtak fra foreningens høyeste organ eller fastsatt i foreningens vedtekter.

Fødselsnummer må ikke benyttes utenpå postsendinger.

Oppbevaring eller behandling av personopplysninger i databehandlingsforetak som har konsesjon etter loven § 22, i adresserings- eller distribusjonsforetak som har konsesjon etter loven § 25 eller foretak som har konsesjon til å drive opinions- og markedsundersøkelsesvirksomhet etter loven § 31, regnes ikke som utlevering når dette skjer etter oppdrag fra registerets eier.

Denne paragrafen gjelder ikke for personregistre som nevnt i § 2-11, § 2-13, § 2-14 og § 2-15.

§ 3-5. Kobling

Selv om personregistre er unntatt fra konsesjon etter "*Utvalgets bakgrunn, sammensetning, mandat og arbeidsmåte*" i kapittel 2, kreves det likevel konsesjon (tillatelse) fra Datatilsynet når slike registre kobles, unntatt når:

- a) koblingen skjer med hjemmel i lov, eller
- b) koblingen har hjemmel i avtale mellom partene i arbeidslivet, eller
- c) utlevering er tillatt i henhold til forskriften § 3-4, og resultatet av koblingen ikke skal benyttes til kontrollformål eller til å treffe beslutninger rettet mot enkeltpersoner. Koblingen kan ikke skje i strid med registrenes formål.

Med kobling menes i forskriften her elektronisk samkjøring av to eller flere personregistre slik at det opprettes et nytt register eller at et eksisterende register tilføres nye opplysninger. Enkeltvise oppslag regnes ikke som kobling.

§ 3-6. Sletting

Med mindre annen lovgivning er til hinder for det, kan enhver som ber om det kreve seg slettet fra registre som nevnt i § 2-2, § 2-3, § 2-4, § 2-5, § 2-6, § 2-7 og § 2-17. Dette gjelder ikke for § 2-2, § 2-3, § 2-4 og § 2-6 dersom registreringen er en forutsetning for medlemskap, leie- eller kundeforhold.

Opplysninger om forbindelsen mellom låntaker/ bruker, som nevnt i § 2-8 (katalog-, låner- og utlånsregistre), og den tjenesten som har vært benyttet, skal av eget tiltak slettes straks den utlånte gjenstanden er tilbakelevert eller tjenesten er opphørt/oppgjort.

"Noen teknologiske og samfunnsmessige utviklingstrekk med spesiell betydning for personvernet" i Kapittel 4 Konesjon for kreditt- og personopplysningsvirksomhet. (Personregisterloven § 13 andre ledd og § 17 andre ledd.)

§ 4-1.

Følgende virksomheter regnes ikke som kredittopplysningsvirksomhet:

1. meldinger fra offentlige registre om rettigheter og heftelser i fast eiendom eller løsøre.
2. meldinger fra banker (jfr lov av 23 april 1892 om Norges Bank, lov av 1 mars 1946 nr 3 om Den Norske Stats Husbank, lov av 10 desember 1948 nr 2 om Norges Postsparebank, lov av 15 juli 1949 nr 1 om Norges Kommunalbank, lov av 24 mai 1961 nr 1 om sparebanker, lov av 24 mai 1961 nr 2 om forretningsbanker, lov av 5 februar 1965 nr 2 om Statens Landbruksbank, lov av 28 april 1972 nr 22 om Statens Fiskarbank og lov av 25 mars 1977 nr 14 om Den Norske Industribank A/ S) og fra finansieringsselskaper (jfr lov av 4 juni 1976 nr 71 om finansieringsvirksomhet) som gjelder dekningskontroll for sjekk eller annet uttak fra konto, diskontering av vekslere og avbetalingskontrakter. Det samme gjelder når slike meldinger formidles for bank eller finansieringsselskap av et utenforstående foretak.
3. meldinger til den opplysningene gjelder.
4. utgivelse av ligningsdata.

§ 4-2.

Følgende virksomheter unntas fra konsesjonsplikten etter personregisterlovens § 14:

1. banker, jfr lov av 24 mai 1961 nr 2 om forretningsbanker og lov av 24 mai 1961 nr 1 om sparebanker
2. finansieringsvirksomhet i medhold av lov av 4 juni 1976 nr 71 om finansieringsvirksomhet

3. statsbanker opprettet ved egen lov.

§ 4-3.

Fødselsnummer må ikke benyttes utenpå postsendinger.

§ 4-4.

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre unntak som nevnt i personregisterloven § 13 annet ledd annet punktum.

§ 4-5.

Datatilsynet gis myndighet til ved enkeltvedtak å gi slike regler som nevnt i personregisterloven § 17 annet ledd.

"Personregisterloven med forskrifter" i Kapittel 5 Konesjon for databehandlingsforetak.

(Personregisterloven § 22 tredje ledd og § 24 annet ledd.)

§ 5-1.

Et forvaltningsorgan (jfr forvaltningsloven § 1) som bare bearbeider personopplysninger for andre over-, under- eller sideordnede organer i samme etat, regnes ikke som databehandlingsforetak etter personregisterloven § 22 første ledd.

Det samme gjelder når et forvaltningsorgan bearbeider opplysninger for kollegiale organer, sakkyndige eller tilsynsførere m.v. som er tilknyttet etaten, eller for private som er engasjert for å løse oppgaver for etaten.

§ 5-2.

Et forvaltningsorgan som bearbeider personopplysninger som det har mottatt fra andre forvaltningsorganer, regnes ikke som databehandlingsforetak etter personregisterloven § 22 første ledd dersom bearbeidingen hovedsakelig skjer ut fra organets eget behov, eller for slike organer som nevnt ovenfor i § 5-1. Dette gjelder selv om bearbeidede opplysninger sendes tilbake til det organ som forvaltningsorganet mottok opplysningene fra.

§ 5-3.

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre unntak fra de enkelte bestemmelser i personregisterlovens kap 6, jfr lovens § 22 tredje ledd.

§ 5-4.

Datatilsynet gis myndighet til ved enkeltvedtak å gi bestemmelser som nevnt i personregisterloven § 24 annet ledd.

"Annen lovgivning som gjelder behandling og registrering av personopplysninger. Ulovfestet og avtalefestet personvern" i Kapittel 6 Konesisjon for adresserings- og distribusjonsvirksomhet.

(Personregisterloven §§ 25, 26 og 29.)

§ 6-1.

Reglene i kap 7 i personregisterloven gjelder ikke for virksomhet drevet av forvaltningsorganet (jfr forvaltningsloven § 1).

§ 6-2.

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre slike unntak som nevnt i personregisterloven § 25 annet ledd.

§ 6-3.

Datatilsynet gis myndighet til ved enkeltvedtak å gi regler som nevnt i personregisterloven § 26 annet ledd.

§ 6-4.

For å gjennomføre reglene i personregisterloven § 28 må foretaket opprette et eget register over eller på annen måte anmerke de personer som etter lovens § 28 krever seg slettet blant de adresser foretaket tilbyr eller benytter, slik at de som har krevd seg slettet ikke lenger står som adressat på de utskrifter som foretaket tilbyr eller benytter til distribusjon.

Når foretaket har mottatt krav om sletting, skal det bare oppbevare de opplysninger om vedkommende som er nødvendige for å hindre at vedkommende kommer med i en adresseutskrift.

Tiltak etter første og annet ledd skal foretas innen en frist som fastsettes ved den enkelte konsesjon.

§ 6-5.

Datatilsynet gis myndighet til ved enkeltvedtak å gi slike regler som nevnt i personregisterloven § 29.

§ 6-6.

I medhold av personregisterloven § 30 nr 1 bestemmes at lovens § 28 skal gjelde også for foretak som i enkeltstående tilfeller påtar seg oppdrag som nevnt i lovens § 25 første ledd.

I medhold av personregisterloven § 30 nr 2 bestemmes at lovens § 28 skal gjelde også for adresselister til bruk for utsending av et foretaks egne varer og tjenester o.l.

"Europarådets konvensjon og rekommandasjoner om persondatubeskyttelse" i Kapittel 7 Konesisjon for opinions- og markedsundersøkelser.

(Personregisterloven §§ 31 og 35.)

§ 7-1.

Et forvaltningsorgan (jfr forvaltningslovens § 1) som utfører opinions- eller markedsundersøkelser for andre over-, under- eller sideordnede organer i samme etat, trenger ikke konsesjon etter personregisterloven § 31 første ledd.

Det samme gjelder når et forvaltningsorgan utfører opinions- eller markedsundersøkelser for kollegiale organer, sakkyndige eller tilsynsførere m.m som er tilknyttet etaten, eller for private som er engasjert for å løse oppgave for etaten.

§ 7-2.

Et forvaltningsorgan som utfører opinions- eller markedsundersøkelser ved hjelp av opplysninger det har mottatt fra andre forvaltningsorganer, trenger ikke konsesjon etter personregisterloven § 31 første ledd dersom undersøkelsen hovedsakelig skjer ut fra organets egne behov, eller for slike organer som nevnt ovenfor i § 7-1. Dette gjelder selv om bearbejdede opplysninger sendes tilbake til det organ som forvaltningsorganet mottok opplysningene fra.

§ 7-3.

Datatilsynet gis myndighet til ved enkeltvedtak å gjøre unntak fra de enkelte bestemmelser i personregisterloven kap 8, jfr lovens § 31 annet ledd.

§ 7-4.

I henhold til personregisterloven § 35 bestemmes at lovens § 32, § 33, § 34 også skal gjelde for foretak som i enkeltstående tilfeller påtar seg slike oppdrag som nevnt i lovens § 31 første ledd, og for foretak som setter i verk slike undersøkelser for sin egen administrasjon og virksomhet.

"Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger" i Kapittel 8 Samtykke til overføring til utlandet.

(Personregisterloven § 36 tredje ledd.)

§ 8-1.

Dersom register eller opplysning som nevnt i lovens § 36 første og annet ledd overføres til utlandet, behøves ikke slikt samtykke som nevnt i § 36. Overføringen må meldes til Datatilsynet på fastsatt skjema i god tid før overføringen finner sted. Datatilsynet kan nekte overføring eller sette vilkår for overføringen.

Overføring behøves ikke meldes når Norge har plikt til å foreta slik overføring etter folkerettslig overenskomst eller som følge av medlemskap i internasjonal organisasjon.

"Oversikt over andre internasjonale reguleringer og andre lands rett" i Kapittel 9 Straffebestemmelser.

(Personregisterloven § 38 tredje ledd.)

§ 9-1.

Den som forsettlig eller aktløst unnlater å følge reglene i denne forskrift § 1-1, § 1-2, § 1-3, "*Hva er personvern?*" i kapittel 3, § 4-3 eller § 8-1, straffes med bøter eller fengsel inntil ett år eller begge deler.

Medvirkning straffes på samme måte.

FORSKRIFT OM BRUK AV BILLEDOPPTAK GJORT VED FJERNSYNS-OVERVÅKNING.

Fastsatt av Justisdepartementet ved kgl. res. 1. juli 1994 med hjemmel i lov 9. juni 1978 nr. 48 om personregistre m.m. § 37 b andre ledd.

§ 1. Virkeområde – definisjon

Forskriften gjelder bruk av billedopptak i organ for stat eller kommune og i privat næringsvirksomhet, foreninger eller stiftelser når opptaket er gjort ved fjernsynsovervåkning. Med fjernsynsovervåkning menes vedvarende eller regelmessig gjentatt personovervåkning ved hjelp av fjernbetjent eller automatisk virkende fjernsynskamera, fotografiapparat eller liknende apparat.

§ 2. Sikring av billedopptakene

Billedopptakene skal lagres på en forsvarlig måte, slik at ikke noen får tilgang til dem uten å ha rett til eller krav på billedopptakene.

Innenfor det foretak eller organ som er i besittelse av billedopptakene, skal bare de personer som foretaket eller organet utpeker, ha tilgang til billedopptakene. Bare de personer som har saklig grunn til slik tilgang i sitt arbeid eller virke i virksomheten, skal utpekes.

§ 3. Bruk av billedopptak

Billedopptak kan bare brukes til de formål de er innhentet for. Politiet kan uten hinder av første punktum bruke billedopptak det måtte være i besittelse av, i forbindelse med forebygging eller etterforskning av straffbare handlinger, som bevis i straffesaker, eller i forbindelse med oppklaring av ulykker.

§ 4. Utlevering av opptakene

Billedopptak gjort ved fjernsynsovervåkning kan bare utleveres til noen utenfor det foretak eller organ som har foretatt opptaket, dersom den som er avbildet samtykker eller utleveringsadgangen følger av lov. Hvis ikke lovbestemt taushetsplikt er til hinder for utlevering, kan billedopptak likevel utleveres til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker.

§ 5. Sletting

Billedopptak skal slettes når det ikke lenger er saklig grunn for oppbevaring.

Billedopptak skal senest slettes 7 dager etter at opptakene er gjort. Slettingsplikten etter forrige punktum gjelder likevel ikke dersom det er sannsynlig at billedopptaket vil bli utlevert til politiet etter § 4 andre punktum. I slike tilfeller kan billedopptakene oppbevares inntil 30 dager.

Billedopptak gjort i post- og banklokaler skal senest slettes 3 måneder etter at opptakene er gjort.

Slettingsplikten etter andre og tredje ledd gjelder ikke

- a) for billedopptak som politiet er i besittelse av,
- b) for billedopptak som Forsvaret er i besittelse av i saker som kan være av betydning for rikets sikkerhet, eller
- c) hvor den som er avbildet samtykker i at billedopptakene oppbevares lenger.

Hvor slettingsplikten etter første ledd oppstår for billedopptak som politiet er i besittelse av, men som er utlevert til politiet fra andre, kan politiet tilbakelevere opptaket til vedkommende, som snarest skal slette det dersom fristen etter andre og tredje ledd er gått ut.

Dersom det foreligger et særlig behov for oppbevaring i lengre tid enn fastsatt i andre og tredje ledd, kan Justisdepartementet gjøre unntak fra disse bestemmelsene.

§ 6. Innsynsrett

Den som det er gjort billedopptak av, kan kreve innsyn i de deler av billedopptakene hvor han eller hun er avbildet, dersom billedopptakene oppbevares ut over 7 dager. Innsynsretten gjelder ikke i forhold til billedopptak som politiet er i besittelse av, eller som Forsvaret er i besittelse av i saker som kan være av betydning for rikets sikkerhet.

§ 7. Straff

Den som forsettlig eller aktløst unnlater å følge reglene i forskriften § 2, § 3, § 4, § 5 andre til sjette ledd eller § 6, straffes med bøter eller fengsel inntil ett år eller begge deler.

Medvirkning straffes på samme måte.

§ 8. Ikraftsetting

Forskriften trer i kraft 15. oktober 1994.

FORSKRIFT OM UNNTAK FRA KONSESJONSPLIKT FOR FINANSINSTITUSJONER MV'S PERSONREGISTRE I SAKER OM HVITVASKING AV PENGER

Fastsatt av Justisdepartementet 23.3.1995 med hjemmel i lov 9. juni 1978 nr 48 om personregistre mm, § 9 annet ledd og § 7 femte ledd, jf kgl res 21. desember 1979.

§ 1 Unntak fra konsesjonsplikt

Denne forskriften gjelder for institusjoner som er regulert av finansieringsvirksomhetsloven § 2-17, jf. § 2-1.

Institusjoners personregistre til bruk i forbindelse med pålagt undersøkelses- og rapporteringsplikt etter finansieringsvirksomhetsloven § 2-17, jf. forskrift 7. februar 1994 nr. 118 om legitimasjonskontroll og tiltak mot hvitvasking av penger § 8 femte ledd, unntas fra konsesjonsplikt etter personregisterloven § 9 første ledd. Registeret skal bare inneholde opplysninger som fremkommer ved institusjonens undersøkelser etter finansieringsvirksomhetsloven § 2-17.

§ 2 *Bruk av registeret*

Registeret må ikke brukes til andre formål enn det som følger av finansieringsvirksomhetsloven § 2-17 og tilhørende forskrifter. Annen bruk av registeret krever samtykke fra den opplysningen gjelder eller hjemmel i lov.

§ 3 *Registeransvarlig*

Det skal utpekes en registeransvarlig i hver institusjon. Den registeransvarlige bør i alminnelighet være den særlig utpekte person som etter forskrift 7. februar 1994 nr. 118 om legitimasjonskontroll og tiltak mot hvitvasking av penger § 8 sjettede ledd skal påse at kontroll- og kommunikasjonsrutiner er etablert og blir fulgt.

Den registeransvarlige er ansvarlig for at reglene i personregisterloven og i denne forskrift blir fulgt.

§ 4 *Innsynsrett*

Innsynsretten etter personregisterloven § 7 gjelder ikke for registre opprettet i medhold av denne forskrift.

§ 5 *Sikring*

Ingen skal ha tilgang til personopplysninger i registeret uten å være autorisert til det. Autorisasjonen skal spesifisere hvilke typer rådighet (lese-, skrive-, endre-, sletterådighet m.v.) vedkommende er gitt. Autorisasjon kan bare gis den som har tjenestlige behov for det. Autorisasjonen skal bare gjelde de funksjoner vedkommende har tjenestlig behov for.

Autorisert personell skal undertegne særskilt taushetserklæring. Erklæringen skal oppbevares av den registeransvarlige.

Den registeransvarlige skal etablere og oppfølge følgende sikringsregler:

1. *Tilgangskontroll.* Det skal gjennomføres tilgangskontroll overfor brukere av registeret. Kontrollen skal avvise forsøk på tilgang fra uautoriserte brukere. Enhver tilgang eller forsøk på tilgang til registeret skal logges. Registeret skal ikke føres i et EDB-system som også brukes av personer uten lovlig tilgang til registeret.

2. *Datakvalitet.* Det skal etableres rutiner for kontroll av opplysninger og relasjoner mellom opplysninger som skal sikre at data er korrekte, komplette og aktuelle.

3. *Tilgjengelighet.* Det skal gjennomføres tiltak som sikrer at registre og opplysninger er tilgjengelige når det er behov for dem. Kopi av opplysninger og annet nødvendig materiale skal sikres med tanke på rekonstruksjon etter tap av data.

§ 6 *Utlevering*

Personopplysninger kan bare utleveres til ØKOKRIM og til Kredittilsynet for ivaretagelse av tilsynspliktene etter lov 7. desember 1956 nr. 1 om tilsynet for kredittinstitusjoner, forsikringselskaper og verdipapirhandel m.v. (Kredittilsynet).

Den registeransvarlige skal påse at all kommunikasjon med ØKOKRIM og Kredittilsynet skjer på betryggende måte.

Ved oversendelse pr. post skal postsendingen være registrert. Ved elektronisk overføring av opplysninger, herunder oversendelse med telefaks, skal opplysningene krypteres. Når saken haster, kan oversendelse uten kryptering likevel skje dersom det følges betryggende rutiner slik at bare autorisert personell kan sende og motta opplysningene.

All oversendelse av opplysninger må logges og det skal opprettes rutiner som bekrefter at opplysningene er kommet frem og at de er sendt av autorisert personell.

§ 7 Kobling

Elektronisk samkjøring av registeret med andre personregistre i eller utenfor finansinstitusjonen er ikke tillatt uten når dette har hjemmel i lov.

§ 8 Anonymisering eller sletting

Den registeransvarlige har ansvaret for at personopplysninger som ikke lenger har betydning blir anonymisert eller slettet, jf. personregisterloven § 8.

For opplysninger som er oversendt ØKOKRIM, gjelder forskrift 7. februar 1994 nr. 118 om legitimasjonskontroll og tiltak mot hvitvasking av penger § 12 første ledd tilsvarende.

§ 9 Straff

Med bøter eller fengsel inntil ett år eller begge deler straffes den som forsettlig eller uaktsomt overtrer denne forskrift.

Medvirkning straffes på samme måte.

FORSKRIFT OM ÅRSAVGIFT FOR FORETAK SOM ER KONSESJONS- PLIKTIGE ETTER PERSONREGISTERLOVEN

Fastsatt av Justisdepartementet 12.12.1988 i medhold av lov om personregistre 9 juni 1978 nr 48 § 5 fjerde ledd, jf kgl res 21 desember 1979.

I

Foretak som er meddelt konsesjon av Datatilsynet i medhold av lov om personregistre §§ 14, 22, 25 og 31, skal betale et årlig gebyr til Datatilsynet på kr 3.000,-. Gebyret skal også betales av foretak som meddeles konsesjon i løpet av året.

Gebyret forfaller 31 januar hvert år. For foretak som får konsesjon i løpet av året, forfaller gebyret en måned etter at konsesjonen er meddelt. Innbetalingen skjer etter nærmere bestemmelse fastsatt av Justisdepartementet.

Gebyr som ikke batles innen forfall forhøyes til kr 5.000,-. Dersom gebyret ikke betales senest 3 måneder etter forfall, kan konsesjonen trekkes tilbake.

II

Forskriften trer i kraft 1 januar 1989.

Vedlegg 3

Europa-parlamentets og rådets direktiv 95/46/EF af 24. Oktober 1995

om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR –
under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 100 A,

under henvisning til forslag fra Kommissionen,
under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg,
i henhold til fremgangsmåden i traktatens artikel 189 B, stk. 3,

og

ud fra følgende betragtninger:

1. Fællesskabets målsætninger, der er nedfældet i traktaten, som ændret ved traktaten om Den Europæiske Union, er at gennemføre en stadig snævrere sammenlutning mellem de europæiske folk, at skabe snævrere forbindelser mellem de stater, som det forener, gennem fælles handling at sikre økonomiske og sociale fremskridt ved at fjerne de skranker, der deler Europa, stadig at forbedre dets folks levevilkår, at bevare og styrke freden og friheden samt at fremme demokratiet på grundlag af de grundlæggende rettigheder, der er anerkendt i medlemsstaternes forfatninger og love, samt i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder;
2. databehandlingssystemer er til for menneskets skyld; de skal være i overensstemmelse med de grundlæggende rettigheder og frihedsrettigheder, der gælder for fysiske personer, uanset statsborgerskab og bopæl, herunder retten til privatlivets fred, og bidrage til at sikre økonomiske og sociale fremskridt og til at fremme samhandelen og det enkelte menneskes velfærd;
3. det indre markeds oprettelse og funktion, som i henhold til traktatens artikel 7 A indebærer fri bevægelighed for varer, personer, tjenesteydelser og kapital, forudsætter ikke blot, at personoplysninger kan cirkulere frit fra én medlemsstat til en anden, men også, at det enkelte menneskes grundlæggende rettigheder beskyttes;
4. personoplysninger benyttes stadig hyppigere inden for de forskellige områder at det økonomiske liv og samfundslivet i Fællesskabet; fremskridtene på det informationsteknologiske område gør det betydeligt nemmere at behandle og udveksle sådanne oplysninger;
5. den økonomiske og sociale integration, der er en følge af det indre markeds oprettelse og funktion efter traktatens artikel 7 A, vil uvægerligt medføre en kraftig vækst i strømmen af personoplysninger på tværs af landegrænserne mellem alle aktører i medlemsstaternes økonomiske liv og samfundslivet, både inden for den private og den offentlige sektor; udvekslingen af personoplysninger mellem virksomheder i de forskellige medlemsstater kan ikke undgå at tage til omfang; medlemsstaternes myndigheder vil som led i gennemførelsen af fællesskabsretten skulle samarbejde og udveksle personoplysninger indbyrdes for at kunne varetage deres opgaver og udføre hverv på vegne af en anden medlemsstats myndighed inden for det område uden indre grænser, som det indre marked indebærer;

6. udbygningen af det teknisk-videnskabelige samarbejde og den koordinerede etablering af nye telekommunikationsnet i Fællesskabet gør det endvidere nødvendigt og nemmere at udveksle personoplysninger på tværs af landegrænserne;
7. forskellen i den beskyttelse af personers rettigheder og frihedsrettigheder, og navnlig retten til privatlivets fred, som de enkelte medlemsstater yder i forbindelse med behandling af personoplysninger, kan forhindre, at oplysninger af denne art videregives fra én medlemsstats område til en anden medlemsstats område; denne forskel kan derved udgøre en hindring for udøvelsen af en række økonomiske aktiviteter på fællesskabsplan, virke konkurrencefordrejende og hindre at de nationale myndigheder i at udføre de opgaver, som påhviler dem i henhold til fællesskabsretten; denne forskel i beskyttelsesniveauet hidrører fra forskellene i de nationale love og administrative bestemmelser;
8. for at hindringerne for udveksling af personoplysninger kan fjernes, skal beskyttelsen af det enkelte menneskes rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysninger være ensartet i alle medlemsstaterne; denne målsætning er af grundlæggende betydning for det indre marked, men kan ikke realiseres af medlemsstaterne alene, navnlig på grund af omfanget af de nuværende forskelle mellem de nationale love på området, og fordi det er nødvendigt at samordne medlemsstaternes lovgivninger, så udveksling af personoplysninger på tværs af landegrænserne underlægges et samlet regelsæt, der er i overensstemmelse med målsætningen om det indre marked som fastsat i traktatens artikel 7 A; det er derfor nødvendigt, at Fællesskabet tager skridt til at gennemføre en indbyrdes tilnærmelse af lovgivningerne;
9. med den ensartede beskyttelse, som vil følge af den indbyrdes tilnærmelse af de nationale lovgivninger, vil medlemsstaterne ikke længere under henvisning til det enkelte menneskes rettigheder og frihedsrettigheder, navnlig retten til privatlivets fred, kunne lægge hindringer i vejen for den frie udveksling af personoplysninger medlemsstaterne imellem; medlemsstaterne vil få en manøvrermargen, som erhvervslivet og arbejdsmarkedets parter kan benytte sig af i forbindelse med direktivets gennemførelse; de vil således i deres nationale lovgivning kunne fastsætte de generelle betingelser for lovlig behandling af personoplysninger; medlemsstaterne skal derved tilsigte en forbedring af den beskyttelse, som deres nuværende lovgivning sikrer; indenfor rammerne af denne manøvrermargen og i overensstemmelse med fællesskabsretten kan der forekomme forskelle i gennemførelsen af direktivet, og dette kan få konsekvenser for udvekslingen af oplysninger såvel inden for den enkelte medlemsstat som på fællesskabsplan;
10. medlemsstaternes lovgivning om behandling af personoplysninger skal sikre overholdelsen af de grundlæggende rettigheder og frihedsrettigheder, navnlig den ret til privatlivets fred, der er fastslået i artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og i fællesskabsrettens generelle principper; af denne grund må en indbyrdes tilnærmelse af lovgivningerne ikke medføre en forringelse af den beskyttelse, disse yder, men skal tværtimod have til formål at sikre et højt beskyttelsesniveau overalt i Fællesskabet;
11. dette direktivs princip om beskyttelse af personers rettigheder og frihedsrettigheder, og navnlig retten til privatlivets fred, er en præcisering og udvidelse af principperne i Europarådets konvention af 28. Januar 1981 om beskyttelse af det enkelte menneske i forbindelse med databehandling af personoplysninger;
12. principperne om beskyttelse skal finde anvendelse på enhver behandling af per-

- sonoplysninger, foretaget af en person, hvis aktiviteter falder ind under fællesskabsrettens anvendelsesområde; en fysisk persons behandling af oplysninger som led i rent personlige eller familiemæssige aktiviteter som f.eks. korrespondance og føring af en adressefortegnelse, bør dog ikke være omfattet;
13. aktiviteterne i afsnit V og VI i traktaten om Den Europæiske Union vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område hører ikke under fællesskabsrettens anvendelsesområde, uden at dette berører de forpligtelser, der påhviler medlemsstaterne i henhold til traktatens artikel 56, stk. 2, artikel 57 og artikel 100 A; den behandling af personoplysninger, som kræves for at beskytte statens økonomiske interesser, er ikke omfattet af dette direktiv, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed;
 14. der gøres for tiden betydelige fremskridt inden for informationssamfundet med hensyn til udvikling af metoder til at registrere, udsende, bearbejde, lagre, opbevare og videresende oplysninger om fysiske personer via lyd og billede, og det er derfor nødvendigt, at dette direktiv finder anvendelse på behandling af sådanne oplysninger;
 15. behandling af sådanne oplysninger er kun omfattet af dette direktiv, hvis den foregår ved hjælp af elektronisk databehandling, eller hvis de pågældende oplysninger er indeholdt i eller skal indgå i et register, der er struktureret efter bestemte kriterier vedrørende personerne for at lette adgangen til de pågældende personoplysninger;
 16. behandling af lyd- og billeddata, som f.eks. i forbindelse med video-overvågning, er ikke omfattet af dette direktiv, hvis den iværksettes med henblik på den offentlige sikkerhed, forsvar, statens sikkerhed eller statens aktiviteter på det strafferetlige område eller andre aktiviteter, der ikke falder ind under fællesskabsretten;
 17. med hensyn til behandling af lyd- og billeddata, der finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, navnlig på det audio-visuelle område, finder direktivets principper begrænset anvendelse i henhold til bestemmelserne i artikel 9;
 18. for at forhindre, at en person unddrages den beskyttelse, der sikres ved dette direktiv, skal enhver behandling af personoplysninger inden for Fællesskabet være i overensstemmelse med lovgivningen i en af medlemsstaterne; med henblik herpå bør enhver behandling af oplysninger være underkastet lovgivningen i den medlemsstat, hvor den registeransvarlige, under hvis myndighed behandlingen udføres, er etableret;
 19. ved etablering på en medlemsstats område forstås faktisk udøvelse af aktiviteter gennem en mere permanent struktur; den pågældende strukturs retlige form, hvad enten det blot er en filial eller et datterselskab med status som juridisk person, har ikke afgørende betydning i denne forbindelse; en registeransvarlig, som er etableret på flere medlemsstats områder, især i form af datterselskaber, skal, navnlig for at undgå omgåelse, sikre sig, at hver enkelt struktur opfylder kravene i den gældende nationale lovgivning;
 20. den omstændighed, at den registeransvarlige er etableret i et tredjeland, må ikke hindre personer i at nyde den beskyttelse, der fastsættes ved dette direktiv; den pågældende behandling bør i så fald underkastes lovgivningen i den medlemsstat, hvor de hjælpemidler, der benyttes til behandlingen, befinder sig, og der bør stilles garanti for, at de rettigheder og forpligtelser, der følger af dette direktiv, også overholdes;
 21. dette direktiv berører ikke de territorialbestemmelser, der gælder i straffesager;
 22. medlemsstaterne fastsætter i deres lovgivning eller i de bestemmelser i øvrigt,

- der vedtages til gennemførelse af dette direktiv, nærmere bestemmelser om, på hvilke generelle betingelser en behandling er lovlig; især artikel 5 giver i forbindelse med artikel 7 og 8 medlemsstaterne mulighed for uafhængigt af de generelle regler at fastsette særlige betingelser for databehandling på specifikke områder og med hensyn til de særlige kategorier af oplysninger, der omhandles i artikel 8;
23. medlemsstaterne er bemyndigede til at gennemføre beskyttelsen af personer såvel ved en generel lov om beskyttelse af personer i forbindelse med behandling af personoplysninger som ved særlove, f.eks. for statistikinstitutter;
 24. dette direktiv berører ikke national lovgivning, der beskytter juridiske personer i forbindelse med behandlingen af oplysninger, som vedrører dem;
 25. principperne om beskyttelse skal dels afspejles i de forskellige forpligtelser, der påhviler personer, offentlige myndigheder, virksomheder, organer eller andre databehandlingsansvarlige, navnlig for så vidt angår oplysningernes pålidelighed, den tekniske sikkerhed, anmeldelse til tilsynsmyndigheden og de omstændigheder, hvorunder behandlingen må udføres, og dels i de rettigheder, der tilkommer de personer, hvis personoplysninger gøres til genstand for behandling; bl.a. retten til at blive underrettet om en behandling, til indsigt, til at kunne kræve oplysninger berigtiget, men også til under visse omstændigheder at gøre indsigelse mod en behandling;
 26. beskyttelsesprincipperne skal gælde enhver oplysning om en identificeret eller identificerbar person; for at afgøre om en person er identificerbar tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person; beskyttelsesprincipperne gælder ikke oplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke længere kan identificeres; adfærdskodekser i henhold til artikel 27 kan være et nyttigt instrument til at angive måder, hvorpå oplysningene kan gøres anonyme og opbevares i en sådan form, at den registrerede ikke længere kan identificeres;
 27. fysiske personer skal beskyttes såvel i forbindelse med elektronisk databehandling af oplysninger som i forbindelse med ikke elektronisk behandling; omfanget af beskyttelsen må i praksis ikke afhænge af de anvendte teknikker, da der ellers vil være alvorlig risiko for omgåelse; for så vidt angår manuel behandling omfatter dette direktiv dog kun registrere og ikke sagsmapper, der ikke er struktureret efter bestemte kriterier vedrørende personer for at lette adgangen til personoplysningerne; i overensstemmelse med definitionen i artikel 2, litra c), kan de forskellige kriterier for adgang til denne samling af oplysninger defineres af hver enkelt medlemsstat; sagsmapper eller samlinger af sagsmapper eller deres forsider, som ikke er struktureret efter bestemte kriterier, hører under ingen omstændigheder ind under dette direktivs anvendelsesområde;
 28. enhver behandling af personoplysninger skal udføres rimeligt og lovligt i forhold til de registrerede; oplysninger, der behandles, skal være tilstrækkelige, relevante og nødvendige i forhold til behandlingsformålene; behandlingsformålene skal være udtrykkeligt angivet, legitime og skal fastlægges ved indsamlingen af oplysningerne; behandlingsformål, der fastlægges senere end indsamlingen, må ikke være uforenelige med de oprindeligt angivne formål;
 29. senere behandling af personoplysninger navnlig i historisk, statistisk eller videnskabeligt øyemed er generelt ikke uforenelig med de formål, som den tidligere indsamling af oplysningerne havde, såfremt medlemsstaterne giver de fornødne garantier; disse garantier skal især udelukke, at oplysningerne bliver anvendt til at underbygge foranstaltninger eller afgørelser, der træffes over for

- en bestemt person;
30. for at være lovlig skal en behandling af personoplysninger desuden bero på den registreredes samtykke eller være nødvendig med henblik på indgåelse eller opfyldelse af en kontrakt, der har bindende virkning for den registrerede, eller være begrundet i et lovkrav, i udførelsen af opgaver i almenhedens interesse, i udøvelsen af embedsmyndighed eller i en persons legitime interesse, medmindre den registreredes interesser, grundlæggende rettigheder og frihedsrettigheder går forud herfor; med særligt henblik på at tilgodese de involverede interesser ligeligt og samtidig sikre en effektiv konkurrence kan medlemsstaterne fastsætte nærmere bestemmelser om, på hvilke betingelser anvendelse og videregivelse af personoplysninger til tredjemand kan finde sted i forbindelse med legitime aktiviteter udøvet af virksomheder og andre organer som led i den daglige drift; de kan ligeledes fastsætte nærmere bestemmelser om, på hvilke betingelser videregivelse af personoplysninger til tredjemand kan finde sted i forbindelse med markedsføring eller markedsundersøgelser, der udføres af velgørende organisationer eller andre sammenslutninger eller stiftelser, f.eks. af politisk karakter, under overholdelse af bestemmelser, som har til formål at give den registrerede mulighed for uden begrundelse og udgifter at gøre indsigelse mod, at sådanne oplysninger behandles;
 31. behandling af personoplysninger, der har til formål at beskytte et hensyn af fundamental betydning for den registreredes liv, anses ligeledes for lovlig;
 32. medlemsstaterne træffer afgørelse om, hvorvidt den registeransvarlige, der udfører en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, skal være en offentlig myndighed eller en anden offentligretlig eller privatretlig person, f.eks. faglig sammenslutning;
 33. oplysninger, som ifølge deres art kan krænke de grundlæggende frihedsrettigheder eller privatlivets fred, må ikke gøres til genstand for behandling uden den registreredes udtrykkelige samtykke; der skal dog udtrykkeligt gives mulighed for undtagelse fra dette forbud for at imødekomme visse behov, navnlig i sådane tilfælde, hvor databehandlingen udføres med bestemte sundhedsmæssige formål og af personer, der er underkastet tavshedspligt, eller i forbindelse med visse foreningers eller stiftelsers legitime aktiviteter, hvis formål er at sikre udøvelsen af grundlæggende frihedsrettigheder;
 34. når hensynet til vigtige samfundsmæssige interesser berettiger det, skal medlemsstaterne ligeledes kunne fravige forbudet mot at behandle følsomme kategorier af data på områder som f.eks. folkesundhet og social sikring – navnlig for at sikre kvalitet og rentabiliteten af de procedurer, der anvendes i forbindelse med ansøgninger og ydelser og tjenester inden for en sygesikringsordning – videnskabelig forskning og offentlig statistik; det påhviler imidlertid medlemsstaterne at sørge for de fornødne specifikke garantier for beskyttelsen af det enkelte menneskes grundlæggende rettigheder og privatliv;
 35. offentlige myndigheders behandling af personoplysninger for officielt anerkendte religiøse sammenslutninger for at opfylde mål, der er fastsat i forfatningsretten eller i folkeretten, udføres af hensyn til vigtige samfundsmæssige interesser;
 36. hvis det i forbindelse med afholdelse af valg i visse medlemsstater er nødvendigt, for at det demokratiske system kan fungere, at politiske partier indsamler oplysninger om enkeltpersoners politiske holdning, kan behandling af sådanne oplysninger tillades af hensyn til varetagelsen af vigtige samfundsmæssige interesser, forudsat, at der fastsættes bestemmelser om de fornødne garantier;
 37. det bør fastsættes undtagelser fra eller begrænsninger af visse bestemmelser i dette direktiv i forbindelse med behandling af personoplysninger i journalistisk

øjemed eller med henblik på kunstnerisk eller litterær virksomhed, navnlig på det audiovisuelle område, for så vidt sådanne undtagelser er nødvendige for at forene det enkelte menneskes grundlæggende rettigheder med ytringsfriheden, herunder retten til at modtage og give oplysninger, som fastslået bl.a. i artikel 10 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder; det påhviler derfor medlemsstaterne med henblik på afvejning mellem de grundlæggende rettigheder at fastsætte de nødvendige undtagelser og begrænsninger for så vidt angår de generelle foranstaltninger vedrørende lovligheden af behandling af oplysninger, foranstaltningerne til overførsel af oplysninger til tredjelande samt tilsynsmyndighedernes beføjelser. Dette må dog ikke føre til, at medlemsstaterne fastsætter undtagelser fra de foranstaltninger, der tager sigte på at garantere behandlingssikkerheden. Der bør endvidere gives den kontrolmyndighed, der er ansvarlig for dette område, i det mindste visse efterfølgende beføjelser, som f.eks. beføjelsen til med jævne mellemrum at offentliggøre en rapport eller at indbringe sager for de retslige myndigheder;

38. en rimelig behandling af oplysninger forudsætter, at de registrerede kan få kendskab til en behandlings eksistens og, når der indsamles oplysninger hos dem, kan få nøjagtig og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen;
39. visse behandlinger vedrører oplysninger, som den ansvarlige ikke har indsamlet direkte hos den registrerede; endvidere kan der berettiget videregives oplysninger til tredjemand, selv om dette ikke var hensigten, da oplysningerne blev indsamlet hos den registrerede; i disse tilfælde skal den pågældende underrettes, når oplysningerne registreres, eller senest når oplysningerne første gang videregives til tredjemand;
40. det er imidlertid ikke nødvendigt at pålægge en sådan underretningspligt, hvis den registrerede allerede er bekendt med de registrerede oplysninger, eller hvis registreringen eller videregivelsen udtrykkeligt er fastsat i loven, eller hvis det viser sig umuligt eller uforholdsmæssigt vanskeligt at underrette den pågældende, hvilket kan være tilfældet i forbindelse med behandlinger i historisk, statistisk eller videnskabeligt øjemed; i denne forbindelse kan der tages hensyn til antallet af registrerede, oplysningernes alder samt de kompensatoriske foranstaltninger, der kan træffes;
41. enhver skal have ret til indsigt i de oplysninger om sig selv, som gøres til genstand for behandling, så den pågældende kan forvise sig om oplysningernes rigtighed og behandlingens lovlighed; af samme årsag skal enhver have ret til at kende den logik, der ligger bag edb-behandlingen af oplysningerne om sig selv, i det mindste i forbindelse med edb-baserede afgørelser, som omhandlet i artikel 15, stk. 1; denne ret må ikke krænke forretningshemmeligheden eller den intellektuelle ejendomsret, navnlig den ophavsret, som programmerne er beskyttet af; dette må dog ikke resultere i, at den registrerede nægtes alle oplysninger;
42. medlemsstaterne kan af hensyn til den registreredes interesser eller med henblik på at beskytte andres rettigheder og frihedsrettigheder begrænse retten til indsigt og til underretning; de kan f.eks. fastsætte, at adgang til medicinske oplysninger kun kan finde sted via en person, der udøver profession inden for sundhedsvæsenet;
43. medlemsstaterne kan ligeledes indskrænke retten til indsigt og underretning samt visse af den registeransvarliges forpligtelser, såfremt dette er nødvendigt af hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed eller væsentlige økonomiske og finansielle interesser i medlemsstaten eller Unionen

- samt efterforskning og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerende erhverv; undtagelser og begrænsninger bør omfatte kontrol-, tilsyns- og reguleringsopgaver, der er nødvendige på de tre sidstnævnte områder vedrørende den offentlige sikkerhed, de økonomiske og finansielle interesser og retsforfølgning i straffesager; dette berører ikke det berettigede i undtagelser og begrænsninger af hensyn til statens sikkerhed eller forsvaret;
44. medlemsstaterne kan i medfør af fællesskabsrettens bestemmelser blive nødt til at fravige bestemmelserne i dette direktiv vedrørende indsigt, underretning af de registrerede og oplysningernes kvalitet for at sikre visse af ovenstående mål;
 45. hvor behandling af personoplysninger kan foregå fuldt lovligt i almenvellets interesse, af hensyn til offentlig myndighedsudøvelse eller i en persons legitime interesse, bør enhver ikke desto mindre være berettiget til, hvis han på grund af egne særlige forhold har tungtvejende og legitime grunde hertil, at gøre indsigelse mod, at oplysningerne om ham selv gøres til genstand for behandling; medlemstaterne har imidlertid mulighed for at vedtage nationale bestemmelser om det modsatte;
 46. beskyttelsen af de registreredes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger forudsætter, at der træffes de fornødne tekniske og organisatoriske foranstaltninger både under selve udformingen og under iværksættelsen af en behandling, navnlig for at varetage sikkerheden og derved forhindre enhver form for ubeføjet behandling; det påhviler medlemsstaterne at søge for, at de registeransvarlige overholder disse foranstaltninger; disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, der skal beskyttes;
 47. når en meddelelse, der indeholder personoplysninger, fremsendes via telekommunikations- eller elektronisk posttjeneste, hvis eneste formål er at sende meddelelser af denne type, er det den person, som er ophavsmand til meddelelsen, og ikke den person, der tilbyder tjenesten, der normalt vil blive betragtet som ansvarlig for behandlingen af de personoplysninger, der er indeholdt i meddelelsen; de personer, som udbyder disse tjenester, vil dog normalt blive betragtet som ansvarlige for behandlingen af de supplerende personoplysninger, der er nødvendige for tjenestens udførelse;
 48. anmeldelsesprocedurerne tager sigte på at gøre en behandlingsformål samt dens vigtigste karakteristika offentlig kendt med henblik på kontrol af behandlingens overholdelse af de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv;
 49. for at undgå overføldige administrative formaliteter kan medlemsstaterne fastsætte fritagelser for og lempelser af anmeldelsespligten for behandlinger, der ikke vil kunne krænke de registreredes rettigheder og frihedsrettigheder, og som er i overensstemmelse med en retsakt, der er udstedt af en medlemsstat, og som fastsætter begrænsningerne herfor; medlemsstaten kan ligeledes give mulighed for forenklet anmeldelse eller fritagelse for anmeldelse, hvor en person med ansvar for databeskyttelse, der udpeges af den registeransvarlige, har kunnet fastslå, at den foretagne behandling ikke vil kunne krænke de registreredes rettigheder og frihedsrettigheder; den person, der har ansvar for databeskyttelse, skal, uanset om han er ansat hos den registeransvarlige eller ej, være i stand til at udøve sit hverv i fuld uafhængighed;
 50. der kan fastsættes fritagelse for anmeldelse eller forenklet anmeldelse i forbin-

- delse med behandlinger, hvis eneste formål er at føre registre, som er udarbejdet i henhold til national ret med henblik på at stille oplysninger til rådighed for offentligheden eller for personer, der kan godtgøre en legitim interesse heri;
51. den omstændighed, at den registeransvarlige er omfattet af den forenklede anmeldelsespligt eller fritaget for anmeldelsespligt, fritager ikke den registeransvarlige for de øvrige forpligtelser, der følger af dette direktiv;
 52. efterfølgende kontrol fra myndighedernes side skal i den forbindelse generelt betragtes som tilstrækkelig;
 53. dog vil visse behandlinger på grund af deres art, omfang eller formål kunne indebære en særlig risiko for at krænke de registreredes rettigheder og frihedsrettigheder, f.eks. behandlinger, der har til formål at udelukke den registrerede fra at udøve en ret, modtage en ydelse eller opnå en kontrakt, eller som indebærer anvendelse af ny teknologi; medlemsstaterne må, hvis de ønsker det, præcisere denne risiko i deres lovgivning;
 54. i forhold til alle de behandlinger, der iværksættes i samfundet, skulle det antal behandlinger, der indebærer en særlig risiko, være meget begrænset; medlemsstaterne skal fastsætte bestemmelser om, at tilsynsmyndigheden eller den person, der har ansvar for databeskyttelse, i samråd med tilsynsmyndigheden skal foretage en kontrol af disse behandlinger, inden de iværksættes; tilsynsmyndigheden kan, efter at kontrollen er foretaget, og i overensstemmelse med den nationale lovgivning udtale sig om eller give tilladelse til den pågældende behandling; den forudgående kontrol kan også foretages som led i udarbejdelsen af en lov, der vedtages af det nationale parlament, eller af en anden foranstaltning med hjemmel i en sådan lov, som fastlægger karakteren af behandlingen og fastsætter de fornødne garantier;
 55. krænker den registeransvarlige en registrerets rettigheder, skal der i medlemsstaternes lovgivning gives adgang til at indbringe sagen for en retsinstans; personer, som lider skade som følge af en ulovlig behandling, skal have ret til erstatning fra den registeransvarlige; denne kan fritages for erstatningsansvar, hvis det bevises, at han ikke er skyld i den forvoldte skade, navnlig hvis der kan henvises til en fejl fra den registreredes side eller et tilfælde af force majeure; der skal iværksættes sanktioner over for såvel privatretlige som offentlige personer, der overtræder nationale bestemmelser vedtaget med henblik på gennemførelsen af dette direktiv;
 56. strømmen af personoplysninger på tværs af landegrænserne er nødvendig af hensyn til udbygningen af den internationale samhandel; den beskyttelse, der ved dette direktiv garanteres personer inden for Fællesskabet, er ikke til hinder for, at der videregives personoplysninger til tredjelande, for så vidt disse sikrer et tilstrækkeligt beskyttelsesniveau; vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, skal foretages på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger;
 57. hvis et tredjeland derimod ikke sikrer et tilstrækkeligt beskyttelsesniveau, skal videregivelse af personoplysninger til det pågældende land forbydes;
 58. der skal dog kunne undtages fra dette forbud under bestemte omstændigheder, hvor den registrerede har meddelt sit samtykke, hvor videregivelsen er nødvendig i forbindelse med en kontrakt eller en retssag, hvor beskyttelsen af væsentlige samfundsinteresser kræver det, f.eks. ved international udveksling af oplysninger mellem skatte- eller toldforvaltninger eller mellem socialsikringsmyndigheder, eller hvor videregivelsen sker fra et register, der er oprettet ved lov, og som offentligheden eller personer med en legitim interesse heri skal kunne konsultere; en sådan videregivelse bør ikke omfatte alle oplys-

- ningerne eller hele kategorier af oplysninger i dette register; når et register er beregnet til at blive konsulteret af personer, der har en legitim interesse heri, bør videregivning kun ske på anmodning af disse personer, eller hvis de selv er modtageren;
59. der kan træffes særlige foranstaltninger til at afhjælpe et utilstrækkeligt beskyttelsesniveau i et tredjeland, hvis den registeransvarlige stiller de fornødne garantier; endvidere skal det fastsættes bestemmelser om forhandlingsprocedurer mellem Fællesskabet og de pågældende tredjelande;
 60. videregivelse til tredjelande må under alle omstændigheder kun finde sted under fuld overholdelse af de bestemmelser, som medlemsstaterne vedtager i medfør af dette direktiv, særlig artikel 8;
 61. medlemsstaterne og Kommissionen skal inden for deres respektive kompetenceområder opfordre de berørte erhvervskredse til at udarbejde adfærdskodekser med henblik på, under hensyn til de særlige former for behandling, der udføres i bestemte sektorer, at fremme iværksættelsen af dette direktiv under overholdelse af de bestemmelser, medlemsstaterne har truffet til gennemførelse deraf;
 62. oprettelsen af en uafhængig tilsynsmyndighed i hver medlemsstat har afgørende betydning for beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger;
 63. denne myndighed skal tildeles de fornødne beføjelser til at varetage denne opgave, herunder undersøgelses- og interventionsbeføjelser, navnlig når det drejer sig om klager, samt beføjelse til at indbringe sager for en retsinstans; myndigheden skal bidrage til at tilvejebringe gennemsigtighed i de databehandlinger, der udføres i den medlemsstat, hvorunder den hører;
 64. tilsynsmyndighederne i de enkelte medlemsstater skal yde hinanden bistand i forbindelse med varetagelsen af deres opgaver for at sikre, at beskyttelsesreglerne overholdes fuldt ud overalt i Den Europæiske Union;
 65. der skal på fællesskabsplan nedsættes en arbejdsgruppe om beskyttelse af personer i forbindelse med behandling af personoplysninger; gruppen skal være fuldt uafhængig i udøvelsen af sine funktioner; i kraft af denne uafhængighed skal den rådgive Kommissionen og navnlig bidrage til, at de nationale regler, der vedtages til gennemførelse af dette direktiv, anvendes ensartet;
 66. for så vidt angår videregivelse af oplysninger til tredjelande, er det nødvendigt at tillægge Kommissionen beføjelse til at udstede gennemførelsesbestemmelser og indføre en procedure i henhold til retningslinjerne i Rådets afgørelse nr. 87/373/EØF for at kunne anvende dette direktiv;
 67. Europa-Parlamentet, Rådet og Kommissionen nåede den 20. december 1994 til enighed om en modus vivendi vedrørende gennemførelsesforanstaltningerne til retsakter vedtaget efter fremgangsmåden i artikel 189 B i EF-traktaten;
 68. de principper om beskyttelse af personers rettigheder og frihedsrettigheder, og navnlig retten til privatlivets fred, i forbindelse med behandling af personoplysninger, som opstilles i dette direktiv, vil for visse sektors vedkommende kunne suppleres med eller præciseres i særregler, der skal være i overensstemmelse med disse principper;
 69. der bør gives medlemsstaterne en frist på højst tre år regnet fra datoen for ikrafttrædelsen af de nationale foranstaltninger, der træffes til gennemførelse af dette direktiv, for at de gradvis kan bringe de nye nationale bestemmelser i anvendelse på samtlige behandlinger, der allerede er iværksat; af hensyn til en omkostningsbevidst gennemførelse indrømmes der medlemsstaterne en yderligere periode, der udløber 12 år efter datoen for vedtagelsen af dette direktiv, til at sikre, at eksisterende ikke-elektroniske registre bringes i overensstemmelse med visse af direktivets bestemmelser; data, der er indeholdt i disse registre, og

som behandles manuelt i denne udvidede overgangsperiode, skal dog på det tidspunkt, hvor de er genstand for en sådan yderligere behandling, være bragt i overensstemmelse med disse bestemmelser;

70. den registrerede skal ikke på ny give sit samtykke, for at den registeransvarlige efter ikrafttrædelsen af de nationale bestemmelser i forbindelse med gennemførelsen af dette direktiv kan fortsætte behandlingen af følsomme oplysninger, når denne er nødvendig for udførelsen af en kontrakt, der er indgået på grundlag af frit og informeret samtykke inden ikrafttrædelsen af ovennævnte bestemmelser;
71. dette direktiv er ikke til hinder for, at en medlemsstat vedtager regler for markedsføring, der henvender sig til forbrugere, der er bosiddende på dens område, for så vidt sådanne regler ikke berører beskyttelsen af personer i forbindelse med behandling af personoplysninger;
72. dette direktiv giver mulighed for, at der i gennemførelsen af dets bestemmelser kan tages hensyn til princippet om aktindsigt i offentlige dokumenter -

UDSTEDT FØLGENDE DIREKTIV:

KAPITTEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Direktivets formål

1. Medlemsstaterne sikrer i overensstemmelse med dette direktiv beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger.

2. Medlemsstaterne må ikke af grunde, der har forbindelse med den i stk. 1 foreskrevne beskyttelse, indskrænke eller forbyde fri udveksling af personoplysninger mellem medlemsstaterne.

Artikel 2

Definitioner

I dette direktiv forstås ved:

- a) «personoplysninger», enhver form for information om en identificeret eller identificerbar fysisk person («den registrerede»); ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet;
- b) «behandling af personoplysninger» («behandling»), enhver operation eller række af operationer – med eller uden brug af elektronisk databehandling – som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring samt blokering, sletning eller tilintet-

- gørelse;
- c) «register med personoplysninger» («register»), enhver strukturert samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag;
 - d) «den registeransvarlige», den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; er formålet med og hjælpemidlerne ved behandlingen fastlagt ved nationale love eller forskrifter eller på fællesskabsplan, kan den registeransvarlige, eller de specifikke kriterier for udpegelse af denne, angives i den pågældende nationale ret eller fællesskabsretten;
 - e) «registerfører», den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler personoplysninger på den registeransvarliges vegne;
 - f) «tredjemand», enhver anden fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ end den registrerede, den registeransvarlige, registerføreren og de personer under den registeransvarliges eller registerføreren direkte myndighed, der er beføjet til at behandle oplysningerne;
 - g) «modtager», den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, hvortil oplysningerne meddeles, uanset om der er tale om en tredjemand; myndigheder, som vil kunne få meddelt oplysninger som led i en isoleret forespørgsel, betragtes ikke som modtagere;
 - h) «den registreredes samtykke», enhver frivillig, specifik og informeret vilje til kendeigivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Artikel 3

Anvendelsesområde

1. Dette direktivs bestemmelser anvendes på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger.

2. Dette direktiv gælder ikke for sådan behandling af personoplysninger,
- som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten, som f.eks. de aktiviteter, der er fastsat i afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interesser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafretlige område
 - som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.

Artikel 4

Gældende national ret

1. Medlemsstaterne anvender de nationale bestemmelser, de vedtager til gennemførelse af dette direktiv, på behandling af personoplysninger;

- a) der foretages som led i en virksomheds eller et organs aktiviteter inden for den medlemsstats område, hvor den registeransvarlige er etableret; en registeransvarlig, som er etableret på flere medlemsstats områder, skal træffe de nødvendige foranstaltninger til at sikre, at hver af disse virksomheder eller organer opfylder kravene i den gældende nationale lovgivning
 - b) der foretages af en registeransvarlig, der ikke er etableret på den pågældende medlemsstats område, men på et sted, hvor dens nationale lovgivning gælder i henhold til folkeretten
 - c) der foretages af en registeransvarlig, der ikke er etableret på Fællesskabets område, og som med henblik på behandling af personoplysninger anvender midler, der være sig elektroniske eller ikke-elektroniske, som befinder sig på den pågældende medlemsstats område, medmindre disse midler kun benyttes med henblik på forsendelse gennem Det Europæiske Fællesskabs område.
2. I det i stk. 1, litra c), omhandlede tilfælde udpeger den registeransvarlige en repræsentant, der er etableret på den pågældende medlemsstats område, uden at dette i øvrigt berører eventuelle retslige skridt mod den registeransvarlige selv.

KAPITTEL II

ALMINDELIGE BETINGELSER FOR LOVLIG BEHANDLING AF PERSONOPLYSNINGER

Artikel 5

Medlemsstaterne præciserer i henhold til bestemmelserne i dette kapitel, på hvilke betingelser behandling af personoplysninger er lovlig.

AFDELING I

PRINCIPPER VEDRØRENDE OPLYSNINGERNES PÅLIDELIGHED

Artikel 6

1. Medlemsstaterne fastsætter bestemmelser om, at personoplysninger

- a) skal behandles rimeligt og lovligt
- b) skal indsamles til udtrykkeligt angivne og legitime formål, samt at senere behandling heraf ikke må være uforenelig med disse formål; senere behandling af oplysninger i historisk, statistisk eller videnskabeligt øjemed anses ikke for at være uforenelig med disse formål, såfremt medlemsstaterne giver de fornødne garantier
- c) skal være relevante og tilstrækkelige og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles
- d) skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt til at slette eller berigtige oplysninger, der er urigtige eller ufuldstændige i forhold til det formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt
- e) ikke må opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål,

hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt. Medlemsstaterne fastsætter de fornødne garantier for personoplysninger, der i historisk, statistisk eller videnskabeligt øjemed opbevares længere en i ovennævnte periode.

2. Det påhviler den registeransvarlige at sikre, at bestemmelserne i stk. 1 overholdes.

AFDELING II

PRINCIPPER VEDRØRENDE GRUNDLAGET FOR BEHANDLING AF OPLYSNINGER

Artikel 7

Medlemsstaterne fastsætter bestemmelser om, at behandling af personoplysninger kun må finde sted hvis:

- a) der ikke hersker tvivl om, at den registrerede har givet sit samtykke, eller
- b) behandlingen er nødvendig af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på dennes anmodning forud for indgåelsen af en sådan kontrakt, eller
- c) behandlingen er nødvendig for at overholde en retlig forpligtelse, som gælder for den registeransvarlige, eller
- d) behandlingen er nødvendig for at beskytte den registreredes vitale interesser, eller
- e) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndigheds udøvelse, som den registeransvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller
- f) behandlingen er nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til artikel 1, stk. 1, i dette direktiv, går forud herfor.

AFDELING III

SÆRLIGE KATEGORIER AF BEHANDLINGER

Artikel 8

Behandlinger, der vedrører særlige kategorier af oplysninger

1. Medlemsstaterne forbyder behandling af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsforhold og seksuelle forhold.

2. Stk. 1 finder ikke anvendelse, hvis

- a) den registrerede udtrykkeligt har givet sit samtykke til en sådan behandling, medmindre det i medlemsstatens lovgivning fastsættes, at det i stk. 1 omhan-

- d) lede forbud ikke kan hæves ved den registreredes samtykke, eller
- b) behandlingen er nødvendig for overholdelsen af den registeransvarliges arbejdsretlige forpligtelser og specifikke rettigheder, for så vidt den er tilladt ifølge nationale lovbestemmelser, som fastsætter de fornødne garantier, eller
 - c) behandlingen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke, eller
 - d) behandlingen foretages af en stiftelse, en forening eller et andet almennyttigt organ, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, som led i organets legitime aktiviteter og med de fornødne garantier, på betingelse af, at behandlingen alene vedrører organets medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at oplysningerne ikke videregives til tredjemand uden den registreredes samtykke, eller
 - e) behandlingen vedrører oplysninger, som klart offentliggøres af den registrerede, eller er nødvendig for, at et retskrav kan fastslægges, gøres gældende eller forsvares.

3. Stk. 1 finder ikke anvendelse, hvis behandlingen af oplysningerne er nødvendig med henblik på forebyggende medicin, medicinsk diagnose, sykepleje eller patientbehandling eller forvaltning af læge og sundhetstjenester, og hvis behandlingen af disse oplysninger foretages af en erhvervsudøvende i sundhedssektoren, der i henhold til den nationale lovgivning eller til regler, der er fastsat af kompetente nationale organer, har tavshedspligt, eller af en anden person med tilsvarende tavshedspligt.

4. Med forbehold af, at der gives tilstrækkelige garantier, kan medlemsstaterne af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, fastsætte andre undtagelser end dem, der er nævnt i stk. 2, enten ved national lovgivning, eller ved en afgørelse truffet af tilsynsmyndigheden.

5. Behandling af oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger må kun foretages under kontrol af en offentlig myndighed, eller hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning med forbehold af de undtagelser, som medlemsstaten kan fastsætte på grundlag af nationale lovbestemmelser, hvorefter der gives tilstrækkelige, specifikke garantier. Et fuldstændigt register over straffedomme må dog kun føres under kontrol af en offentlig myndighed.

6. Undtagelser fra stk. 1 som omhandlet i stk. 4 og 5 meddeles til Kommissionen.

7. Medlemsstaterne bestemmer, på hvilke betingelser et nationalt identifikationsnummer eller andre almene midler til identifikation kan gøres til genstand for behandling.

Artikel 9

Behandling af personoplysninger og ytringsfriheden

Medlemsstaterne fastsætter i forbindelse med behandling af personoplysninger, der udelukkende finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed, kun fritagelser eller undtagelser fra bestemmelserne i dette kapitel og i kapitel IV og VI, for så vidt som de er nødvendige for at forene retten til privatlivets fred med reglerne for ytringsfrihed.

*AFDELING IV**OPLYSNINGSPLIGT OVER FOR DEN REGISTREREDE**Artikel 10**Oplysningspligt ved innsamling af oplysninger hos den registrerede*

Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige eller dennes repræsentant skal give den person, hos og om hvem der innsamles oplysninger, mindst følgende informationer, medmindre den pågældende allerede er bekendt hermed, og for så vidt som disse yderligere informationer, under hensyn til de særlige omstændigheder hvorunder oplysningerne innsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne:

- a) den registeransvarliges og eventuelt dennes repræsentants identitet
- b) formålene med den behandling, hvortil oplysningerne er bestemt
- c) alle yderligere informationer som f.eks.
 - modtagerne eller kategorierne af modtagere
 - om det er obligatorisk eller frivilligt at besvare spørgsmålene samt mulige følger af ikke at svare
 - hvorvidt der gives ret til at få innsigt i og foretage berigtigelse af de oplysninger, der vedrører den registrerede.

*Artikel 11**Oplysningspligt, når oplysningerne ikke er innsamlet hos den registrerede*

1. Når oplysningerne ikke er innsamlet hos den registrerede, fastsætter medlemsstaterne bestemmelser om, at den registeransvarlige eller dennes repræsentant allerede ved registreringen af oplysningerne, eller senest når oplysningerne første gang videregives til tredjemand, skal give den registrerede mindst følgende informationer, medmindre den pågældende allerede er bekendt hermed, og for så vidt som disse yderligere informationer, under hensyn til de særlige omstændigheder hvorunder oplysningerne innsamles, er nødvendige for at sikre den registrerede en rimelig behandling af oplysningerne:

- a) den registeransvarliges og eventuelt dennes repræsentants identitet
- b) formålene med behandlingen
- c) alle yderligere informationer som f.eks.
 - hvilken type oplysninger det drejer sig om
 - modtagerne eller kategorierne af modtagere
 - hvorvidt der gives ret til at få innsigt i og foretage berigtigelse af de oplysninger, der vedrører den registrerede.

2. Bestemmelserne i stk. 1 finder ikke anvendelse, navnlig ikke når behandlingen foretages i statistisk øjemed eller til historiske eller videnskabelige forskningsformål, hvis underretning af den registrerede viser sig umulig eller er uforholdsmæssig vanskelig, eller registreringen eller vidergivelsen af oplysningerne er udtrykkeligt fastsat ved lov. I sådanne tilfælde fastsætter medlemsstaterne de fornødne garantier.

*AFDELING V**DEN REGISTREREDES RET TIL INDSIGT**Artikel 12**Ret til innsigt*

Medlemsstaterne sikrer enhver registreret ret til hos den registeransvarlige

- a) frit og uhindret, med rimelige mellemrum og uden større ventetid eller større udgifter
 - at få oplyst, om der behandles personoplysninger om den pågældende selv, samt mindst formålene med behandlingen, hvilken type oplysninger det drejer sig om, og modtagerne eller kategorierne af modtagere af oplysningerne
 - at få meddelt letforståelig information om, hvilke oplysninger der er omfattet af behandlingerne, samt enhver tilgængelig information om, hvorfra disse oplysninger stammer
 - at få at vide, hvilken logik der ligger bag edb-behandlingen af oplysningerne om den pågældende, i det mindste i forbindelse med edb-baserede afgørelser som omhandlet i artikel 15, stk. 1
- b) efter omstændighederne at få oplysninger, som ikke er blevet behandlet i overensstemmelse med dette direktiv, berigtiget, slettet eller blokeret, navnlig hvis de er ufuldstændige eller urigtige;
- c) at få udvirket, at tredjemand, til hvem sådanne oplysninger er blevet videregivet, underrettes om enhver berigtigelse, sletning eller blokering, der er foretaget i overensstemmelse med litra b), medmindre underretning viser sig umulig eller er uforholdsmæssig vanskelig.

*AFDELING VI**UNDTAGELSER OG BEGRÆNSNINGER**Artikel 13**Undtagelser og begrænsninger*

1. Medlemsstaterne kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 6, stk. 1, artikel 10, artikel 11, stk 1, samt artikel 12 og 21, hvis en sådan begrænsning er en nødvendig foranstaltning af hensyn til:

- a) statens sikkerhed
- b) forsvaret
- c) den offentlige sikkerhed
- d) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerende erhverv
- e) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender

- f) en kontrol-, tilsyns- eller reguleringsopgave, selv af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i litra c), d) og e) nævnte områder
- g) beskyttelsen af den registreredes interesser eller andres rettigheder og frihedsrettigheder.

2. Medlemsstaterne kan med forbehold af de fornødne lovhjemlede garantier, navnlig for at oplysningerne ikke anvendes til at træffe foranstaltninger eller afgørelser vedrørende bestemte personer, i tilfælde, hvor der klart ikke er nogen risiko for, at den registreredes ret til privatlivets fred krænkes, ved lov begrænse de i artikel 12 omhandlede rettigheder, hvis oplysningerne udelukkende behandles med videnskabelig forskning for øje eller kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker.

AFDELING VII

DEN REGISTREREDES INDSIGELSESRET

Artikel 14

Den registreredes indsigelsesret

Medlemsstaterne indrømmer den registrerede ret til

- a) i det mindste i de i artikel 7, litra e) og f), omhandlede tilfælde af vægtige legitime grunde, der vedrører den pågældendes særlige situation, til enhver tid at gøre indsigelse mod, at personoplysninger om ham selv gøres til genstand for behandling, medmindre andet er bestemt i den nationale lovgivning; i tilfælde af berettiget indsigelse må den af den registeransvarlige iværksatte behandling ikke længere omfatte de pågældende oplysninger;
- b) efter anmodning og uden udgifter at modsætte sig en behandling af personoplysninger, der vedrører den pågældende, og som den registeransvarlige agter at foretage med henblik på markedsføring, eller at blive underrettet, inden personoplysningerne første gang videregives til tredjemand eller anvendes på tredjemands vegne med henblik på markedsføring, og udtrykkelig få tilbud om uden udgifter at gøre indsigelse mod en sådan videregivelse eller anvendelse.

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de registrerede er bekendt med den i litra b), første afsnit omhandlede ret.

Artikel 15

Edb-behandlede individuelle afgørelser

1. Medlemsstaterne indrømmer enhver person ret til ikke at være undergivet afgørelser, der har retsvirkning for ham, eller som berører ham i væsentlig grad, og som alene er truffet på grundlag af edb-behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, såsom erhversevne, kreditværdighed, pålidelighed, adfærd osv.

2. Uden at dette berører de øvrige bestemmelser i dette direktiv, fastsætter medlemsstaterne bestemmelser om, at en person kan undergive en afgørelse af den art, der er omhandlet i stk. 1 når:

- a) den pågældende afgørelse træffes som led i indgåelsen eller opfyldelsen af en kontrakt, såfremt den registreredes anmodning om indgåelse eller opfyldelse af kontrakten er blevet efterkommet, eller der findes passende foranstaltninger til at beskytte den registreredes legitime interesser, som f.eks. mulighed for denne til at gøre sit synspunkt gældende, eller når
- b) den pågældende afgørelse er hjemlet i en lov, der indeholder bestemmelser til beskyttelse af den registreredes legitime interesser.

AFDELING VIII

FORTROLIGHED OG BEHANDLINGSSIKKERHED

Artikel 16

Behandlingernes fortrolige karakter

Enhver, der udfører arbejde under den registeransvarlige eller registerføreren, herunder registerføreren selv, og som får adgang til personoplysninger, må kun behandle disse efter instruks fra den registeransvarlige, bortset fra tilfælde der er fastsat i lovgivningen.

Artikel 17

Behandlingssikkerhed

1. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling.

Disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes.

2. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige, hvis oplysninger behandles for dennes regning, skal vælge en registerfører, som frembyder den fornødne garanti med hensyn til de tekniske sikkerhedsforanstaltninger og organisatoriske foranstaltninger, der skal træffes, og skal påse, at disse foranstaltninger overholdes.

3. Gennemførelse af en behandling ved en registerfører skal ske i henhold til en kontrakt eller et andet retligt bindende dokument mellem registerføreren og den registeransvarlige, hvori det navnlig fastsættes

- at registerføreren alene handler efter instruks fra den registeransvarlige
- at forpligtelserne i henhold til stk. 1, som fastlagt i lovgivningen i den medlemsstat, hvor registerføreren er etableret, ligeledes påhviler denne.

4. Med henblik på opbevaring af beviserne skal de dele i kontrakten eller det retlige dokument, der vedrører beskyttelse af oplysninger, og de krav, der vedrører de i stk. 1 omhandlede foranstaltninger, foreligge skriftligt eller i en anden tilsvarende form.

AFDELING IX

ANMELDELSE

Artikel 18

Anmeldelsespligt over for tilsynsmyndigheden

1. Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige eller dennes eventuelle repræsentant forud for iværksættelsen af en behandling, der helt eller delvis udføres ved brug af elektronisk databehandling, eller en række sådanne behandlinger, hvis formål er identiske eller indbyrdes relaterede, skal foretage anmeldelse til den i artikel 28 omhandlede tilsynsmyndighed.

2. Medlemsstaterne må kun give mulighed for forenklet anmeldelse eller fritagelse for anmeldelse i følgende tilfælde og på følgende betingelser:

- medlemsstaterne anfører for de typer behandling, hvor det i betragtning af de behandlede oplysninger ikke er sandsynligt, at de registreredes rettigheder eller frihedsrettigheder krænkes, behandlingens formål, hvilke oplysninger eller typer oplysninger der behandles, hvilke registrerede eller kategorier af registrerede der er tale om, til hvilke modtagere eller kategorier af modtagere oplysningerne videregives, samt hvor længe oplysningerne opbevares, og/eller
- de registeransvarlige udpeger i overensstemmelse med den nationale lovgivning, som de er underlagt, en person med ansvar for beskyttelse af personoplysninger, som bl.a. har til opgave
 - i fuld uafhængighed at sikre den interne anvendelse af de nationale bestemmelser, der er truffet i medfør af direktivet
 - at føre et register over de behandlinger, der gennemføres af den registeransvarlige, og som omfatter de i artikel 21, stk. 2, omhandlede oplysninger for på denne måde at sikre at det er ikke sandsynligt, at de registreredes rettigheder og frihedsrettigheder vil kunne krænkes om følge af behandlingen.

3. Medlemsstaterne kan fastsætte, at stk. 1 ikke finder anvendelse på behandlinger, hvis eneste formål er at føre et register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden, og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri.

4. Medlemsstaterne kan fritage de behandlinger, der er omhandlet i artikel 8, stk. 2, litra d), for anmeldelsespligt eller fastsætte en forenklet anmeldelse.

5. Medlemsstaterne kan bestemme, at ikke-elektroniske behandlinger af personoplysninger eller nogle af disse behandlinger skal anmeldes, eller foreskrive forenklet anmeldelse af sådanne behandlinger.

Artikel 19

Anmeldelsens indhold

1. Medlemsstaterne præciserer, hvilke oplysninger anmeldelsen skal indeholde. Anmeldelsen skal mindst indeholde følgende oplysninger:
 - a) navn og adresse på den registeransvarlige og dennes eventuelle repræsentant
 - b) behandlingens formål
 - c) en beskrivelse af kategorien eller kategorierne af registrerede og af de oplysninger eller typer af oplysninger, der vedrører dem
 - d) de modtagere eller kategorier af modtagere, som oplysningerne kan videregives til
 - e) påtænkte overførsler af oplysninger til tredjelande
 - f) en generel beskrivelse, der giver mulighed for foreløbigt at vurdere, om foranstaltningerne med henblik på behandlingssikkerheden i henhold til artikel 17 er passende.
2. Medlemsstaterne præciserer, efter hvilke procedurer ændringer i de i stk. 1 omhandlede oplysninger skal anmeldes til tilsynsmyndigheden.

Artikel 20

Forudgående kontrol

1. Medlemsstaterne præciserer, hvilke behandlinger der kan indebære særlige risici for personers rettigheder og frihedsrettigheder, og sikrer, at disse behandlinger kontrolleres, inden de iværksettes.
2. En sådan forudgående kontrol foretages af tilsynsmyndigheden efter modtagelsen af anmeldelsen fra den registeransvarlige, eller den foretages af den person, der har ansvar for databeskyttelse, som i tilfælde skal høre tilsynsmyndigheden.
3. Medlemsstaterne kan også gennemføre en sådan kontrol som led i udarbejdelsen af en foranstaltning, der vedtages af det nationale parlament, eller af en anden foranstaltning med hjemmel i en sådan lov, som fastlægger karakteren af behandlingen og fastsætter de fornødne garantier.

Artikel 21

Behandlingernes offentlige tilgængelighed

1. Medlemsstaterne træffer foranstaltninger til at sikre, at behandlingerne er offentligt tilgængelige.
2. Medlemsstaterne fastsætter bestemmelser om, at tilsynsmyndigheden fører et register over de behandlinger, der er anmeldt i henholdt il artikel 18.

Registret omfatter mindst de oplysninger, der er anført i artikel 19, stk. 1, litra a)-e).

Registret er offentligt tilgængeligt.
3. For så vidt angår behandlinger, som ikke er omfattet af anmeldelsespligt, fastsætter medlemsstaterne bestemmelser om, at de registeransvarlige eller enhver anden myndighed, som medlemsstaterne udpeger, på passende måde mindst skal

stille de i artikel 19, stk. 1, litra a)-e), omhandlede oplysninger til rådighed for enhver person, der anmoder herom.

Medlemsstaterne kan fastsætte, at denne bestemmelse ikke finder anvendelse på behandlinger, hvis eneste formål er at føre et register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri.

KAPITTEL III

RETSMIDLER, ANSVAR OG SANKTIONER

Artikel 22

Klageadgang

Uden at foregribe muligheden for at iværksætte administrativ klage, herunder for den tilsynsmyndighed, der er nævnt i artikel 28, inden forelæggelse for retsinstanter, fastsætter medlemsstaterne bestemmelser om, at enhver har ret til for en domstol at indbringe en klage over krænkelse af de rettigheder, der garanteres i henhold til de nationale love, der gælder for den pågældende behandling.

Artikel 23

Ansvar

1. Medlemsstaterne fastsætter bestemmelser om, at enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenelig med de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, har ret til erstatning for den forvoldte skade fra den registeransvarlige.

2. Den registeransvarlige kan helt eller delvis fritages for erstatningsansvar for skade, hvis han beviser, at han ikke er skyld i den begivenhed, der medførte skaden.

Artikel 24

Sanktioner

Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at dette direktiv gennemføres i fuldt omfang, og de fastsætter bl.a. de sanktioner, der skal finde anvendelse i tilfælde af overtrædelse af de bestemmelser, der vedtages til dette direktivs gennemførelse.

KAPITTEL IV

VIDEREGIVELSE AF PERSONOPLYSNINGER TIL TREDJELANDE

Artikel 25

Prinsipper

1. Medlemsstaterne fastsætter bestemmelser om, at videregivelse til et tredjeland af personoplysninger, der gøres til genstand for behandling, eller som skal gøres til genstand for behandling efter videregivelsen, kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, og forudsat at de nationale bestemmelser, der vedtages til gennemførelse af direktivets øvrige bestemmelser, overholdes.

2. Vurderingen af, om beskyttelsesniveauet i et tredjeland er tilstrækkeligt, sker på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger; til grund for vurderingen lægges navnlig oplysningernes art, den eller de påtænkte behandligers formål og varighed, oprindelseslandet og det endelige bestemmelsesland, de retsregler – almindelige regler eller sektorregler – der er i kraft i det pågældende tredjeland, samt de regler for god forretningskik og de sikkerhedsforanstaltninger, der gælder i landet.

3. Medlemsstaterne og Kommissionen underretter gensidigt hinanden, hvis de mener, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med stk. 2.

4. Konstaterer Kommissionen efter proceduren i artikel 31, stk. 2, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2, træffes medlemsstaterne de foranstaltninger, der er nødvendige for at hindre enhver videregivelse af oplysninger af samme art til det pågældende tredjeland.

5. Kommissionen indleder på det rette tidspunkt forhandlinger med henblik på at afhjælpe den situation, der opstår som følge af en konstatering efter stk. 4.

6. Kommissionen kan efter proceduren i artikel 31, stk. 2, fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med denne artikels stk. 2, på grundlag af dets nationale lovgivning eller dets internationale forpligtelser med henblik på at beskytte privatlivet og personers grundlæggende rettigheder og frihedsrettigheder, herunder de forpligtelser, der er indgået efter de i stk. 5 nævnte forhandlinger.

Medlemsstaterne træffer de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

Artikel 26

Undtagelser

1. Som undtagelse fra bestemmelserne i artikel 25, fastsætter medlemsstaterne, medmindre andet er bestemt i deres nationale lovgivning, at videregivelse eller en type videregivelse af personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2, kan finde sted, hvis

a) der ikke hersker tvivl om, at den registrerede har givet sit samtykke, eller

- b) videregivelsen er nødvendig af hensyn til opfyldelsen af en kontrakt mellem den registrerede og den registeransvarlige eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan kontrakt, eller
- c) videregivelsen er nødvendig af hensyn til indgåelsen eller udførelsen af en kontrakt, der i den registreredes interesse er indgået mellem den registeransvarlige og tredjemand, eller
- d) videregivelsen er nødvendig eller følger af lov eller bestemmelser fastsat med hjemmel i lov for at beskytte en vigtig samfundsinteresse eller for, at et retskrav kan fastlægges, gøres gældende eller forsvares, eller
- e) videregivelsen er nødvendig for at beskytte den registreredes vitale interesser, eller
- f) videregivelsen finder sted fra et offentligt register, der ifølge love eller administrative bestemmelser er beregnet til at informere offentligheden og som er tilgængeligt for offentligheden generelt eller for personer, der kan godtgøre at have en legitim interesse heri, i det omfang de ved lov fastsatte betingelser for offentlig tilgængelighed er opfyldt i det specifikke tilfælde.

2. Med forbehold af stk. 1, kan en medlemsstat give tilladelse til videregivelse eller en type videregivelse af personoplysninger til et tredjeland, der ikke sikrer et tilstrækkeligt beskyttelsesniveau i overensstemmelse med artikel 25, stk. 2, hvis den registeransvarlige yder tilstrækkelige garantier for beskyttelse af privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder samt for udøvelsen af de dertil knyttede rettigheder; sådanne garantier kan især fremgå af passende kontraktbestemmelser.

3. Den pågældende medlemsstat underretter Kommissionen og de øvrige medlemsstater om de tilladelser, den giver i henhold til stk. 2.

4. Fastslår Kommissionen efter proceduren i artikel 31, stk. 2, at visse standardkontraktbestemmelser frembyder tilstrækkelige garantier i henhold til stk. 2, træffer medlemsstaterne de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse.

KAPITTEL V

ADFÆRDSKODEKSER

Artikel 27

1. Medlemsstaterne og Kommissionen tilskynder til udarbejdelsen af adfædskodekser, der afhængigt af de særlige forhold i de forskellige sektorer skal bidrage til en korrekt anvendelse af de nationale bestemmelser, medlemsstaterne vedtager til gennemførelse af dette direktiv.

2. Medlemsstaterne fastsætter bestemmelser om, at de brancheforeninger eller andre organer, som repræsenterer andre kategorier af registeransvarlige, som har udarbejdet udkast til nationale adfædskodekser, eller som agter at ændre eller forlænge gældende nationale kodekser, skal kunne forelægge dem for den nationale myndighed til udtalelse.

3. Udkast til EF-kodeks og forslag til ændring eller forlængelse af eksisterende EF-kodekser kan forelægges den i artikel 29 omhandlede gruppe. Denne udtaler sig bl.a. om, hvorvidt de udkast, den har fået forelagt, er i overensstemmelse med de nationale bestemmelser til gennemførelse af dette direktiv. Hvis den finder det nød-

vendigt, indhenter den bemærkninger fra de registrerede eller disses repræsentanter. Kommissionen kan tilse, at de kodekser, som gruppen har godkendt, offentliggøres på passende vis.

KAPITTEL VI

TILSYNSMYNDIGHED SAMT GRUPPE TIL BESKYTTELSE AF PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER

Artikel 28

Tilsynsmyndighed

1. Hver medlemsstat drager omsorg for, at der udpeges en eller flere offentlige myndigheder, der har til opgave på dens område at påse overholdelsen af de bestemmelser, medlemsstaten vedtager til gennemførelse af dette direktiv.

Disse myndigheder udøver i fuld uafhængighed de funktioner, der tillægges dem.

2. Hver medlemsstat drager omsorg for, at tilsynsmyndighederne høres ved udarbejdelsen af administrative foranstaltninger eller retsfor skrifer om beskyttelse af personers rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger.

3. Hver tilsynsmyndighed skal bl.a. kunne:

- a) iværksette undersøgelser og bl.a. have adgang til de oplysninger, der gøres til genstand for en behandling, og til at indsamle alle oplysninger, der er nødvendige for at varetage sine tilsynsopgaver;
- b) gribe effektivt ind ved f.eks. at afgive udtalelser forud for iværksættelsen af behandlingerne i henhold til artikel 20 og sikre en passende offentliggørelse af disse udtalelser, at beordre oplysninger blokeret, slettet eller tilintetgjort, midlertidigt eller definitivt at fobyde en behandling, at udstede en advarsel til den registeransvarlige eller påtale en overtrædelse over for den registeransvarlige eller påtale en overtrædelse over for den registeransvarlige eller ved at høre parlamenter eller andre nationale politiske institutioner;
- c) indbringe overtrædelser af de nationale bestemmelser, som vedtages til gennemførelse af dette direktiv, for retsinstanterne eller gøre retsinstanterne opmærksom på disse overtrædelser.

Afgørelser truffet af tilsynsmyndigheden, som går en involveret part imod, kan indbringes for en retsinstant.

4. Enhver kan, eventuelt repræsenteret ved en sammenslutning, til tilsynsmyndigheden indgive en anmodning om beskyttelse af sine rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger. Den pågældende underrettes om, hvorledes sagen følges op.

Enhver kan til tilsynsmyndigheden især indgive en anmodning om at få kontrolleret en behandlings lovlighed, når de nationale bestemmelser, der er truffet i henhold til artikel 13 i dette direktiv, finder anvendelse. Den pågældende underrettes i alle tilfælde om, at der er blevet foretaget en kontrol.

5. Hver tilsynsmyndighed udarbejder med regelmæssige mellemrum en rapport om sin virksomhed. Denne rapport offentliggøres.

6. Den enkelte tilsynsmyndighed er, uanset hvilken national lov der måtte gælde for den pågældende behandling, kompetent til på sin medlemsstats område at udøve de beføjelser, der tillægges den i overensstemmelse med stk. 3 i denne artikel. Myndigheden kan blive anmodet om at udøve sine beføjelser af en myndighed i en anden medlemsstat.

Tilsynsmyndighederne samarbejder med hinanden i det omfang, det er nødvendigt for at opfylde deres pligter, navnlig ved at udveksle alle nyttige oplysninger.

7. Medlemsstaterne fastsætter bestemmelser i deres lovgivning om, at tilsynsmyndighedernes medlemmer og ansatte også efter deres aktiviteterets ophør har tavshedspligt for så vidt angår de fortrolige oplysninger, de har adgang til.

Artikel 29

Gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger

1. Der nedsættes en gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger, i det følgende benævnt «gruppen».

Denne gruppe er rådgivende og uafhængig.

2. Gruppen består af en repræsentant for den eller de tilsynsmyndigheder, hver medlemsstat har udpeget, og af en repræsentant for den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne, samt af en repræsentant for Kommissionen.

Hvert medlem af gruppen udpeges af den institution eller den eller de myndigheder, det repræsenterer. Når en medlemsstat har udpeget flere tilsynsmyndigheder, udnævner disse en fælles repræsentant. Det samme gælder de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne.

3. Gruppen træffer sine afgørelser med simpelt flertal blandt repræsentanterne for tilsynsmyndighederne.

4. Gruppen vælger selv sin formand. Formandens mandat gælder for en periode af 2 år. Mandatet kan fornyes.

5. Gruppens sekretariatsopgaver varetages af Kommissionen.

6. Gruppen fastsætter selv sin forretningsorden.

7. Gruppen behandler spørgsmål, der sættes på dagsordenen af dens formand, enten på dennes initiativ, efter anmodning fra en repræsentant for tilsynsmyndighederne eller efter anmodning fra Kommissionen.

Artikel 30

1. Gruppen har til opgave:

- a) at undersøge ethvert spørgsmål vedrørende anvendelse af de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, med henblik på at bidrage til en ensartet anvendelse heraf;
- b) at give Kommissionen en udtalelse om beskyttelsesniveauet i Fællesskabet og i tredjelande;
- c) at rådgive Kommissionen om ethvert udkast til ændring af dette direktiv og om, hvilke supplerende eller specifikke foranstaltninger der bør træffes for at sikre fysiske personers rettigheder og frihedsrettigheder for så vidt angår behandling af personoplysninger, samt om ethvert andet udkast til fællesskabsforanstaltninger, der har indvirkning på sådanne rettigheder og frihedsrettigheder;
- d) at afgive udtalelse om de adgærdskodekser, der udarbejdes på fællesskabsplan.

2. Konstaterer gruppen forskelle mellem medlemsstaternes lovgivning eller praksis, der kan være til fare for en ensartet beskyttelse af personer i forbindelse med behandling af personoplysninger inden for Fællesskabet, underretter den Kommissionen herom.

3. Gruppen kan på eget initiativ fremsætte henstillinger om ethvert spørgsmål vedrørende beskyttelsen af personer i forbindelse med behandling af personoplysninger inden for Fællesskabet.

4. Gruppens udtalelser og henstillinger forelægges for Kommissionen og for det i artikel 31 omhandlede udvalg.

5. Kommissionen underretter gruppen om, hvorledes den har taget hensyn til dens udtalelser og henstillinger. Kommissionen udarbejder med henblik herpå en beretning, som også forelægges for Europa-Parlamentet og Rådet. Denne beretning offentliggøres.

6. Gruppen udarbejder en årsberetning om situationen vedrørende beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger inden for Fællesskabet og i tredjelande; den forelægger beretningen for Europa-Parlamentet, Rådet og Kommissionen. Beretningen offentliggøres.

KAPITTEL VII

EF-GENNEMFØRELSESFORANSTALTNINGER

Artikel 31

Udvalget

1. Kommissionen bistås af et udvalg, der består af repræsentanter for medlemsstaternes regeringer, og som har Kommissionens repræsentant som formand.

2. Kommissionens repræsentant forelægger udvalget et udkast til de foranstaltninger, der skal træffes. Udvalget afgiver en udtalelse om dette udkast inden for en frist, som formanden kan fastsætte under hensyn til, hvor meget det pågældende spørgsmål haster.

Udtalelsen afgives med det flertal, som er fastsat i traktatens artikel 148, stk. 2. Ved afstemninger i udvalget tildeles medlemsstaternes stemmer den vægt, som er fastsat i nævnte artikel. Formanden deltager ikke i afstemningen.

Kommissionen vedtager foranstaltninger, der straks finder anvendelse. Hvis de ikke er i overensstemmelse med den afgivne udtalelse, underrettes Rådet dog straks af Kommissionen om disse foranstaltninger. I så fald gælder følgende:

- Kommissionen udsætter gennemførelsen af de foranstaltninger, den har truffet afgørelse om, i et tidsrum på tre måneder regnet fra datoen for underretningen;
- Rådet kan med kvalificeret flertal træffe en anden afgørelse inden for det tidsrum, der er nævnt i ovenstående led.

AFSLUTTENDE BESTEMMELSER

Artikel 32

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv senest tre år efter dets vedtagelse.

Når medlemsstaterne vedtager disse love og administrative bestemmelser, skal de indeholde en henvisning til dette direktiv, eller de skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for denne henvisning fastsættes af medlemsstaterne.

2. Medlemsstaterne påser, at behandlinger, der allerede er iværksat på ikrafttrædelsesdatoen for de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, bringes i overensstemmelse med disse bestemmelser senest tre år efter denne dato. Som en undtagelse fra foregående afsnit kan medlemsstaterne fastsætte, at behandlingen af oplysninger, som allerede findes i manuelle registre, der føres på ikrafttrædelsesdatoen for de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, senest 12 år efter vedtagelsen af direktivet skal bringes i overensstemmelse med direktivets artikel 6, 7 og 8. Medlemsstaterne indrømmer dog den registrerede ret til efter anmodning og navnlig i forbindelse med udøvelse af retten til indsigt at få berigtiget, slettet eller blokeret oplysninger, der er ufuldstændige eller urigtige, eller som opbevares på en måde der er uforenelig med de legitime formål, som den registeransvarlige forfølger.

3. Som en undtagelse fra stk. 2 kan medlemsstaterne, hvis der gives passende garantier, fastsætte, at oplysninger, der kun opbevares med henblik på historisk forskning, ikke skal bringes i overensstemmelse med artikel 6, 7 og 8 i dette direktiv.

4. Medlemsstaterne meddeler Kommissionen teksten til de nationale retsfor skrifter, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 33

Kommissionen forelægger med jævne mellemrum, første gang senest 3 år efter det i artikel 32, stk. 1, nævnte tidspunkt, Europa-Parlamentet og Rådet en beretning om anvendelsen af dette direktiv, eventuelt ledsaget af passende ændringsforlag. Beretningen offentliggøres.

Kommissionen undersøger navnlig direktivets anvendelse på behandling af lyd og billeddata og fysiske personer og forelægger passende forslag, der måtte være nødvendige i betragtning af udviklingen inden for informationsteknologien og informationssamfundet.

Artikel 34

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Luxembourg, den 24 oktober 1995

Tabell 3.1:

For Europa-Parlamentet
K. Hänsch
Formand

For Rådet
L. Atienzaserna
Formand

Vedlegg 4

Europarådets konvensjon 28 Januar 1981 nr 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger

Innledning

Europarådets medlemstater som har undertegnet denne konvensjon,

Som mener at Europarådets formål er å oppnå større enhet mellom sine medlemmer, især på grunnlag av respekt for rettsstaten så vel som menneskerettighetene og de grunnleggende friheter;

Som mener at det er ønskelig å utvide vernet for enkeltpersoners rettigheter og grunnleggende friheter, og særlig retten til respekt for privatlivets fred under hensyn til den økende strøm over landegrensene av personopplysninger som bearbeides ved elektronisk databehandling;

Som på samme tid igjen bekrefter sin forpliktelse til informasjonsfrihet uten hensyn til landegrensener;

Som erkjenner at det er nødvendig å bringe de grunnleggende verdier om respekt for privatlivets fred og den frie strøm av opplysninger mellom nasjoner i samsvar med hverandre,

Er blitt enige om følgende:

"Sammendrag av personregisterlovutvalgets utredning" i Kapittel 1 – Generelle bestemmelser

Artikkel 1

Gjenstand og formål

Denne konvensjons formål er å sikre respekt for enhver enkeltpersons rettigheter og grunnleggende friheter og især retten til privatlivets fred på territoriet til enhver part, uten hensyn til statsborgerskap eller bopel, i forbindelse med elektronisk databehandling av personopplysninger som vedrører ham («datavern»).

Artikkel 2

Definisjoner

I denne konvensjons forstand:

- a) betyr «personopplysning» enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson («datasubjektet»);
- b) betyr «elektronisk dataregister» ethvert sett av opplysninger som blir bearbeidet ved elektronisk databehandling;
- c) omfatter «elektronisk databehandling» følgende operasjoner dersom de utføres helt eller delvis ved hjelp av automatiserte metoder: lagring av opplysninger, utføring av logiske og/eller aritmetiske operasjoner i tilknytning til disse

- opplysninger samt forandring, sletting, gjenfinning eller spredning av dem;
- d) betyr «ansvarlig registerfører» den fysiske eller juridiske person, offentlig myndighet, byrå eller annet organ som i henhold til nasjonal lovgivning har kompetanse til å avgjøre hva som skal være det elektroniske dataregisters formål, hvilke kategorier av personopplysninger som skal lagres og hvilke operasjoner som disse skal undergå.

Artikkel 3

Rekkevidde

1. Partene forplikter seg til å anvende denne konvensjon på elektroniske persondataregistrene og elektronisk databehandling av personopplysninger i den offentlige og den private sektor.

2. Enhver stat kan, på undertegningstidspunktet eller når den deponerer sitt dokument vedrørende ratifikasjon, godkjenning, samtykke eller tiltredelse, eller på ethvert senere tidspunkt, gi underretning ved en erklæring rettet til Europarådets Generalsekretær:

- a) om at den ikke vil anvende denne konvensjon på visse kategorier av elektroniske persondataregistre, oppført i en fortegnelse som vil bli deponert. Denne fortegnelsen skal imidlertid ikke omfatte kategorier av elektroniske persondataregistre undergitt intern lovgivning vedrørende datavern. Den skal følgelig endre denne fortegnelsen ved en ny erklæring hver gang nye kategorier av elektroniske persondataregistre blir undergitt datavernbestemmelser i henhold til dens interne lovgivning;
- b) om at den også vil anvende denne konvensjon på opplysninger som gjelder grupper av personer, foreninger, stiftelser, foretak, selskaper og alle andre organer som direkte eller indirekte består av enkeltpersoner, enten slike organer har rettsevne eller ikke;
- c) om at den også vil anvende denne konvensjon overfor persondataregistre som ikke behandles elektronisk.

3. Enhver stat som har utvidet denne konvensjons rekkevidde ved noen av de erklæringer som er fastsatt i underpunkt 2 b) eller c) ovenfor kan gi underretning i den nevnte erklæring om at slike utvidelser bare skal gjelde for visse kategorier av persondataregistre, oppført i en fortegnelse som vil bli deponert.

4. Enhver part som har utelukket visse kategorier av elektroniske persondataregistre ved en erklæring som fastsatt i underpunkt 2 a) ovenfor kan ikke påberope seg at en part som ikke har utelukket dem, skal anvende denne konvensjonen overfor slike kategorier.

5. På samme måte kan en part som ikke har foretatt en eller flere utvidelser som fastsatt i underpunktene 2 b) og c) ovenfor, ikke gjøre krav på å få anvende denne konvensjon på disse punkter overfor en part som har foretatt slike utvidelser.

6. Erklæringene som fastsatt i punkt 2 ovenfor skal få virkning fra det tidspunkt konvensjonen trer i kraft med hensyn til den stat som har avgitt dem dersom de er blitt avgitt på undertegningstidspunktet eller når den deponerte sitt dokument vedrørende ratifikasjon, godkjenning, samtykke eller tiltredelse, eller tre måneder etter at Europarådets Generalsekretær har mottatt dem dersom de er blitt avgitt på et senere tidspunkt. Disse erklæringene kan helt eller delvis kalles tilbake, ved en underretning rettet til Europarådets Generalsekretær. Slike tilbakekallinger skal få virkning tre måneder etter den dato en slik underretning er mottatt.

Kapittel II – Hovedprinsipper for datavern

Artikkel 4

Partenes plikter

1. Hver part skal treffe de nødvendige tiltak i sin interne lovgivning for å gjennomføre hovedprinsippene for datavern fastsatt i dette kapittel.

2. Disse tiltak skal treffes senest på det tidspunkt denne konvensjon trer i kraft for denne part.

Artikkel 5

Datakvalitet

Personopplysninger som bearbeides ved elektronisk databehandling skal:

- a) innsamles og bearbeides på rettferdig og lovlig vis;
- b) lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formål;
- c) være adekvate, relevante og ikke for omfattende i relasjon til de formål de lagres til;
- d) være nøyaktige og, der det er nødvendig, holdt ajour;
- e) oppbevares på en måte som ikke gir anledning til å identifisere datasubjektene lenger enn nødvendig for det formål som disse opplysningene lagres til.

Artikkel 6

Særkategorier av opplysninger

Personopplysninger som åpenbarer rasemessig opprinnelse, politiske oppfatninger samt religiøs eller annen tro, så vel som personopplysninger vedrørende helse eller seksuell liv, kan ikke behandles elektronisk med mindre intern lovgivning gir tilstrekkelig vern. Det samme skal gjelde for personopplysninger som gjelder domfellelser for straffbare handlinger.

Artikkel 7

Sikring av opplysninger

Formålstjenlige sikringstiltak skal treffes for å verne personopplysninger lagret i elektroniske dataregistre mot tilfeldig eller ikke-autorisert ødeleggelse eller tilfeldig tap så vel som mot ikke-autorisert adgang, forandring eller spredning.

Artikkel 8

Tilleggsvern for datasubjektene

Enhver person skal ha rett til:

- a) å bringe på det rene om det eksisterer et elektronisk persondataregister, dets hovedformål, så vel som den ansvarlige registerførers identitet og faste bopel

- eller hovedkontor.
- b) med rimelige mellomrom og uten ugrunnet opphold eller urimelige utgifter å få bekreftet hvorvidt personopplysninger vedrørende ham selv er lagret i det elektroniske persondataregister og å få seg meddelt disse opplysninger i en forståelig form;
 - c) å få korrigert eller slettet, alt etter omstendighetene, slike opplysninger dersom disse er blitt behandlet i strid med de bestemmelser i intern lovgivning som gjennomfører hovedprinsippene fastsatt i denne konvensjons artikler 5 og 6;
 - d) å klage eller på annen måte bringe saken videre dersom en anmodning om bekreftelse eller, alt etter omstendighetene, meddelelse, korrigerings eller sletting som nevnt i denne artikkels punkter b) og c), ikke etterkommes.

Artikkel 9

Unntak og forbehold

1. Intet unntak fra bestemmelsene i artiklene 5, 6, og 8 i denne konvensjon skal være tillatt, med mindre det faller innenfor de rammer som er definert i denne artikkel.
2. Avvik fra bestemmelsene i denne konvensjons artikler 5, 6 og 8 skal være tillatt når slikt avvik er fastsatt ved partens lovgivning og er et nødvendig tiltak i et demokratisk samfunn av hensyn til:
 - a) beskyttelse av statens sikkerhet, offentlig sikkerhet, statens økonomiske interesser eller bekjempelse av kriminelle handlinger;
 - b) beskyttelse av datasubjektet eller andre rettigheter og friheter.
3. Forbehold vedrørende utøvelsen av de rettigheter som er fastsatt i artikkel 8 punktene b), c) og d) kan fastsettes ved lov når det gjelder elektroniske persondataregister anvendt til statistikk eller til vitenskapelige forskningsformål dersom det åpenbart ikke er noen risiko for at datasubjektenes privatliv krenkes.

Artikkel 10

Sanksjoner og kontrollordninger

Hver part plikter å innføre hensiktsmessige sanksjoner og kontrollordninger for brudd på bestemmelsene i intern lovgivning som gjennomfører hovedprinsippene for datavern fastsatt i dette kapittel.

Artikkel 11

Utvidet vern

Ingen av bestemmelsene i dette kapittel skal tolkes slik at de begrenser eller på annen måte innvirker på en parts muligheter til å innrømme datasubjekter en større grad av vern enn det som er fastsatt i denne konvensjon.

Kapittel III – Overføring av opplysninger over landegrenser

Artikkel 12

Overføring av personopplysninger over landegrenser og intern lovgivning

1. De følgende bestemmelser skal gjelde for overføring over landegrenser av personopplysninger som bearbeides ved elektronisk databehandling eller er innsamlet med sikte på å bli bearbeidet ved elektronisk databehandling, uten hensyn til hvilket overføringsmiddel som nyttes.

2. En part skal ikke, utelukkende med det formål å verne privatlivets fred, forby eller kreve særlig tillatelse for overføring av personopplysninger som går til en annen parts territorium.

3. Likevel skal hver part ha rett til å avvike fra bestemmelsene i punkt 2:

- a) i den grad dens lovgivning inneholder særskilte regler for visse kategorier av personopplysninger eller av elektroniske persondataregistre, på grunn av disse opplysningers eller registres karakter, dersom ikke den annen parts regler gir tilsvarende beskyttelse;
- b) når overføringen blir foretatt fra partens territorium til en ikke-kontraherende stats territorium ved hjelp av mellomledd på en annen parts territorium, for å unngå at slike overføringer fører til omgåelse av lovgivningen i den part som er nevnt i begynnelsen av dette punkt.

Kapittel IV – Gjensidig bistand

Artikkel 13

Samarbeid mellom partene

1. Partene er enige om å yte hverandre gjensidig bistand med sikte på å gjennomføre denne konvensjon.

2. For dette formål:

- a) skal hver part peke ut ett eller flere organer, hvis navn og adresse(r) skal meddeles Europarådets Generalsekretær;
- b) hver part som har utpekt mer enn ett organ skal i sin underretning som nevnt i det foregående underpunkt spesifisere hvert enkelt organs kompetanse.

3. Et organ som er utpekt av en part skal på anmodning av et organ utpekt av en annen part:

- a) skaffe til veie informasjon om sin lovgivning og forvaltningspraksis på datavernområdet.
- b) i samsvar med sin interne lovgivning og utelukkende med det formål å verne privatlivets fred, treffe alle hensiktsmessige tiltak for å skaffe til veie konkret informasjon om nærmere angitt elektronisk databehandling utført på sitt territorium, likevel med unntak av personopplysninger som blir behandlet.

Artikkel 14

Bistand til datasubjekter bosatt i utlandet

1. Hver part skal yte bistand til enhver person bosatt i utlandet slik at han kan utøve de rettigheter han har i medhold av intern lovgivning som gjennomfører prinsippene fastsatt i denne konvensjons artikkel 8.

2. Når en slik person er bosatt på en annen parts territorium skal han selv kunne velge om han vil sette fram sin anmodning gjennom det organ som er utpekt av denne parten som mellomledd.

3. Anmodningen om bistand skal inneholde alle de nødvendige opplysninger, blant annet vedrørende:

- a) navnet, adressen og eventuelle andre relevante opplysninger som identifiserer den person som setter fram anmodningen;
- b) det elektroniske persondataregistret som anmodningen vedrører, eller dets ansvarlige registerfører;
- c) anmodningens formål.

Artikkel 15

Vernetiltak vedrørende bistand gitt av utpekte organer

1. Et organ utpekt av en part som har mottatt opplysninger fra et organ utpekt av en annen part enten sammen med en anmodning om bistand eller som svar på sin egen anmodning om bistand skal ikke nytte disse opplysningene til andre formål enn dem som er spesifisert i anmodningen om bistand.

2. Hver part skal sørge for at de personer som tilhører eller opptrer på vegne av det utpekte organ skal være pålagt nødvendig diskresjons- eller taushetsplikt hva angår disse opplysningene.

3. Ikke i noe tilfelle kan et utpekt organ i henhold til artikkel 14 punkt 2 få tillatelse til å fremsette på eget initiativ og uten uttrykkelig samtykke fra vedkommende person en anmodning om bistand på vegne av et datasubjekt bosatt i utlandet.

Artikkel 16

Avslag på anmodninger om bistand

Et utpekt organ som det blir rettet en anmodning om bistand til i henhold til denne konvensjons artikler 13 eller 14 kan ikke avslå å etterkomme den med mindre:

- a) anmodningen er uforenlig med den myndighet organet som er ansvarlig for å svare, har på datavernområdet;
- b) anmodningen ikke er i samsvar med bestemmelsene i denne konvensjon;
- c) oppfyllelse av anmodningen ville være uforenlig med suverenitet, sikkerhet eller offentlig interesse (ordre public) til den part som utpekte friheter til personer under denne parts jurisdiksjon.

Artikkel 17

Utgifter og fremgangsmåter vedrørende bistand

1. For gjensidig bistand som partene gir hverandre i samsvar med artikkel 13 og for bistand de gir til datasubjekter i utlandet i samsvar med artikkel 14 skal der ikke kreves betaling av noen utgifter eller gebyrer utenom dem som er påløpt for sakkyn-dige og oversettere. De sistnevnte utgifter eller gebyrer skal bæres av den part som har utpekt det organ som setter fram anmodningen om bistand.

2. Datasubjektet kan ikke belastes utgifter eller gebyrer i samband med de skritt som er tatt på hans vegne på den annen parts territorium utenom dem som lovlig skal betales av denne parts innvånere.

3. Andre detaljer vedrørende bistand særlig i tilknytning til de former og fremgangsmåter og de språk som skal nyttes, skal fastsettes direkte mellom vedkom-mende parter.

Kapittel V – Rådgivende komité

Artikkel 18

Komitéens sammensetning

1. En rådgivende komité skal opprettes etter at denne konvensjon er trådt i kraft.

2. Hver part skal utnevne en representant til komitéen og en vararepresentant. Enhver av Europarådets medlemstater som ikke har sluttet seg til konvensjonen skal ha rett til å delta i komitéen som observatør.

3. Den rådgivende komité kan, ved enstemmig vedtak, innby enhver stat som ikke er medlem av Europarådet og som ikke er en part i konvensjonen til å la seg representere med en observatør på et bestemt møte.

Artikkel 19

Komitéens oppgaver

Den rådgivende komité:

- a) kan sette fram forslag med sikte på å tilrettelegge eller bedre anvendelsen av konvensjonen;
- b) kan sette fram forslag om endring av denne konvensjon i samsvar med artikkel 21;
- c) skal utarbeide en uttalelse om ethvert forslag om endring av denne konvensjon som forelegges den i samsvar med artikkel 21, punkt 3;
- d) kan på anmodning avgi en part av uttalelse om ethvert spørsmål som vedrører anvendelsen av denne konvensjon.

Artikkel 20

Forretningsorden

1. Den rådgivende komité skal sammenkalles av Europarådets Generalsekretær. Dens første møte skal holdes innen tolv måneder etter at denne konvensjon er trådt

i kraft. Den skal deretter møte minst en gang hvert annet år og i ethvert tilfelle når en tredjedel av partenes representanter anmoder om at den sammenkalles.

2. Den rådgivende komité's møter er beslutningsdyktige når et flertall av partenes representanter er til stede.

3. Etter hvert av dens møter, skal Den rådgivende komité oversende Europarådets Ministerkomité en rapport om sitt arbeid og om hvordan denne konvensjon virker.

4. I henhold til bestemmelsene i denne konvensjon, skal Den rådgivende komité utarbeide sin egen forretningsorden.

Kapittel VI – Endringer

Artikkel 21

Endringer

1. Endringer til denne konvensjon kan foreslås av en part, av Europarådets Ministerkomité eller av Den rådgivende komité.

2. Europarådets Generalsekretær skal meddele ethvert forslag om endring til Europarådets medlemstater og til enhver stat som ikke er medlem, men som har tiltrådt konvensjonen eller som er blitt innbudt til å tiltre denne konvensjon i samsvar med bestemmelsene i artikkel 23.

3. Enhver endring foreslått av en part eller Ministerkomitéen skal dessuten meddeles Den rådgivende komité som skal avgi sin uttalelse om den foreslåtte endring til Ministerkomitéen.

4. Ministerkomitéen skal behandle den foreslåtte endring og enhver uttalelse som Den rådgivende komité har avgitt, og den kan vedta endringen.

5. Teksten til enhver endring som er vedtatt av Ministerkomitéen i samsvar med denne artikkels punkt 4 skal videresendes partene til godkjenning.

6. Enhver endring som er vedtatt i samsvar med denne artikkels punkt 4 skal tre i kraft på den trettiende dagen etter at alle parter har underrettet Generalsekretæren om sin godkjenning av den.

Kapittel VII – Sluttbestemmelser

Artikkel 22

Ikrafttredelse

1. Denne konvensjon skal være åpen for undertegning av Europarådets medlemstater. Den er gjenstand for ratifikasjon, godkjenning eller samtykke. Dokumenter vedrørende ratifikasjon, godkjenning eller samtykke skal deponeres hos Europarådets Generalsekretær.

2. Denne konvensjon skal tre i kraft på den første dagen i den måneden som etterfølger utløpet av en periode på tre måneder etter den dato fem av Europarådets medlemstater har gitt sitt samtykke til å bli bundet av konvensjonen i samsvar med det foregående punkt.

3. I forhold til en medlemstat som senere gir sitt samtykke til å bli bundet av den, skal konvensjonen tre i kraft på den første dagen i den måneden som etterfølger

utløpet av en periode på tre måneder etter datoen for deponeringen av dokumentet vedrørende ratifikasjon, godkjenning eller samtykke.

Artikkel 23

Tiltredelse av ikke-medlemstater

1. Etter ikrafttredelsen av denne konvensjon, kan Europarådets Ministerkomité innby enhver stat som ikke er medlem av Europarådet til å tiltre denne konvensjon ved en beslutning fattet av flertallet som fastsatt i artikkel 20 d) i Europarådets Vedtekter og ved enstemmighet av representantene for de kontraherende stater som har rett til å sitte i komitéen.

2. I forhold til en tiltredende stat, skal konvensjonen tre i kraft på den første dagen i den måneden som etterfølger utløpet av en periode på tre måneder etter datoen for deponeringen av tiltredelsesdokumentet hos Europarådets generalsekretær.

Artikkel 24

Territorialbestemmelser

1. Enhver stat kan på undertegningstidspunktet eller når den deponerer sitt dokument vedrørende ratifikasjon, godkjenning, samtykke eller tiltredelse, spesifisere det eller de territorier som denne konvensjon skal gjelde for.

2. Enhver stat kan på enhver senere dato, ved en erklæring rettet til Europarådets Generalsekretær, utvide anvendelsen av denne konvensjon til ethvert annet territorium som spesifisert i erklæringen. Med hensyn til et slikt territorium skal konvensjonen tre i kraft på den første dagen i den måneden som etterfølger utløpet av en periode på tre måneder etter den dato en slik erklæring er mottatt av Generalsekretæren.

3. Enhver erklæring avgitt i henhold til de to foregående punkter kan med hensyn til ethvert territorium nevnt i en slik erklæring, tilbakekalles ved en meddelelse adressert til Generalsekretæren. En slik tilbakekalling skal tre i kraft på den første dag i den måned som følger etter utløpet av et tidsrom på seks måneder etter den dato da Generalsekretæren mottok den.

Artikkel 25

Forbehold

Intet forbehold kan tas med hensyn til bestemmelsene i denne konvensjon.

Artikkel 26

Oppsigelse

1. Enhver part kan til enhver tid si opp denne konvensjon ved en underretning rettet til Europarådets Generalsekretær.

2. Slik oppsigelse skal få virkning på den første dagen i den måneden som etterfølger utløpet av en periode på seks måneder etter den dato underretningen er mottatt av Generalsekretæren.

Artikkel 27

Underretninger

1. Europarådets Generalsekretær skal underrette Rådets medlemstater og enhver stat som har tiltrådt denne konvensjon om:

- a) enhver undertegning;
- b) deponeringen av ethvert dokument vedrørende ratifikasjon, godkjenning, samtykke eller tiltredelse;
- c) enhver ikrafttredelsesdato for denne konvensjon i samsvar med artiklene 22, 23 og 24;
- d) enhver annen handling, underretning eller meddelelse vedrørende denne konvensjon.

Til bevitnelse herav har undertegnede, dertil behørig bemyndiget, undertegnet denne konvensjon.

Utferdiget i Strasbourg den 28. dag i januar 1981, i engelsk og fransk tekst, som begge har samme gyldighet, i ett eksemplar som skal oppbevares i Europarådets arkiv. Europarådets generalsekretær skal oversende bekreftede kopier til hver av Europarådets medlemsstater og til enhver stat som er innbudt til å tiltre denne konvensjon.

Vedlegg 5

Den konstitusjonelle adgang til å legge vedtaksmyndighet til «uavhengige» organer

av professor, dr.juris Eivind Smith, Universitetet i Oslo

Jeg viser til muntlige kontakter og til brev av 17.9.1996, 6.12.1996 og 4.1.1997, der mitt oppdrag er skissert.

1 INNLEDNING

Ifølge sitt mandat skal Personregisterlovutvalget vurdere «hvilken stilling Datatilsynet bør ha i forhold til regjeringen og departementet, herunder regjeringens og departementets instruksjons- og kontrollmyndighet». I denne sammenheng skal det særskilt vurderes «hvilke løsninger som kan/bør velges» under EF-direktiv 95/46 om personopplysninger.

Av særlig interesse som bakgrunn for de følgende bemerkninger er bestemmelsen i direktivets art. 28 nr. 1, annet ledd om at tilsynsmyndighetene skal kunne utøve de funksjoner som tillegges dem «i full uavhengighet». Brevet av 17.9.1996 presiserer at Personregisterlovutvalget selv vil ta stilling til hvordan dette kravet skal forstås. Dette er jeg innforstått med. Men den nevnte passus i direktivet kan tjene som et passende inntak til den problemstilling om et uavhengig datatilsyn i Norge som jeg skal forholde meg til. På denne bakgrunn skal jeg likevel komme med noen videre bemerkninger.

Funksjonell og administrativ uavhengighet

Den danske versjon av direktivet (jeg har ikke sjekket andre versjoner) nevner uttrykkelig at uavhengigheten skal gjelde de «funksjoner» som tilsynet skal utøve. En rimelig tolkning synes å være at tilsynsmyndigheten skal være uavhengig under utførelsen av selve tilsynsarbeidet (behandling av søknader om konsesjon, kontroll m.v.). Forsåvidt fremstår utvalgets antagelse (i brevet av 17.9.) om at direktivet bare tar sikte på «funksjonell uavhengighet», som plausibel (men rent språklig kan det jo innvendes at også administrasjon m.v., se nedenfor, har med «funksjoner» å gjøre). Siden det antagelig vil være tale om (en eller annen form for) forvaltningsorganer (se likevel under 5 nedenfor), vil det særlig måtte bli tale om uavhengighet i forhold til Kongen (regjeringen) og departementet.

Omvendt vil et mulig krav om uavhengighet i spørsmål som gjelder administrasjon og budsjett m.v., antagelig stå mindre sterkt. Men i praksis vil det slett ikke alltid være mulig å skille skarpt mellom uavhengighet i spørsmål av «faglig» og økonomisk/administrativ karakter. Utenfor Personregisterlovutvalgets mandatområde kan eksempler hentes bl.a. fra debatten om domstolenes administrative avhengighet av Justisdepartementet.

Avhengighet i økonomisk/administrative spørsmål kan i seg selv ha betydning for graden av rettslig og faktisk uavhengighet i «faglige» spørsmål. Men selv om de involverte personer selv mener at forholdet mellom det organ (vedkommende fagdepartement) som har det overordnede økonomisk/administrative ansvar, og det «uavhengige» forvaltningsorgan, ikke reiser noe problem, kan det være viktig å sørge for at organiseringen gir omverdenen *tillit* til at uavhengigheten i «faglige» spørsmål er vel ivaretatt.

Et særtilfelle i grensen mellom «funksjonell» og «administrativ» uavhengighet gjelder kompetansen til å utpeke medlemmer av det «uavhengige» organ. Det kan tenkes hevdet at uavhengighet av ett organ (eller av et sett av organer) bare kan tenkes hvis myndigheten til å utpeke de personer som skal bemanne det «uavhengige» organ, er lagt til *andre* organer enn dem som de utpekte skal være uavhengige av. F.eks. skulle et organ der medlemmene er oppnevnt av Kongen, ikke kunne være «uavhengig» av Kongen (eller departementet).

Vekten av en slik antagelse vil imidlertid variere. Hvis det er tale om en posisjon som er begrenset i tid (f.eks. til x år), og det ikke er adgang til å oppnevne samme person mer enn én gang, vil uavhengigheten normalt være større enn hvis det er adgang til gjenoppnevning. Det samme gjelder åpenbart hvis posisjonen er besatt uten noen bestemt tidsbegrensning (bortsett fra aldersgrensen) og ikke kan bringes til opphør av den oppnevneende myndighet alene.

Muligheten til å gjøre bruk av tidsbegrensede, forholdsvis langvarige mandater uten adgang til gjenoppnevning kan etter mitt syn fortjene større oppmerksomhet i debatten om hvordan mer eller mindre «uavhengige» organer kan bygges inn i forvaltningsapparatet i Norge.

«Uavhengighet»

Det er viktig å presisere at begrepet «uavhengighet» er relativt. Dette gjelder allerede i den relasjon som nettopp er nevnt: I Norge er ingen forvaltningsorganer helt uavhengige i økonomisk/administrativ henseende. Den uavhengighet som et organ måtte ha, gjelder høyst i det jeg stikkordmessig har kalt «faglige» spørsmål.

Videre er begrepet relativt fordi det naturligvis ikke er meningen at et organ skal være «uavhengig» også av loven (grunnloven, EF-retten osv.). Dette betyr at valget av *rettslig form* vil ha stor betydning for hvilken grad av uavhengighet som f.eks. Datatilsynet vil kunne nyte godt av. Hvis f.eks. lovs form benyttes, vil organet ikke være beskyttet mot senere lovendring. Derimot vil det være beskyttet mot kgl.res. eller departementsvedtak (f.eks. i form av «instruks») som etter sitt innhold står i strid med loven.

Jeg nevner endelig at begrepet «uavhengighet» er relativt i den forstand at uavhengigheten – innenfor grensene av vedkommende lov og «faglige» område – kan være et resultat av sperrer mot ulike former for «styring». Slike former kan f.eks. være *instruks* om saksbehandling, lovtolkning eller skjønnsutøvelse, adgang for andre til å *omgjøre* det «uavhengige» organets vedtak på grunnlag av klage eller av eget tiltak, og *vilkår* for bevilgninger. Den sistnevnte form gir et nytt eksempel på at grensedragningen mellom faglige og økonomisk/administrative spørsmål kan være uklar.

Uavhengigheten blir større jo flere og viktigere former for styring som loven osv. står i veien for. Her skal jeg nøye meg med å nevne at det vanskelig kan bli tale om å karakterisere et organ som rettslig «uavhengig» av et organ som har kompetanse til å omgjøre det førstnevnte organets vedtak og/eller som kan gi det instruks om vedtakenes innhold.

Så lenge de sistnevnte grenser er respektert, vil jeg i det følgende snakke om «uavhengighet» av Kongen og/eller departementet uten å presisere nærmere hvor omfattende uavhengighet det er snakk om.

Den videre fremstilling

De konstitusjonelle spørsmål som Personregisterlovutvalget ønsker å få belyst, må behandles med utgangspunkt i den relasjon klagenemnda (og evt. Datatilsynet) skal

settes inn i. Med dette som utgangspunkt, skal jeg organisere den videre fremstilling i fire punkter.

Først (under 2) skal jeg se på den konstitusjonelle adgang til å legge myndighet til å avgjøre klager over vedtak som er truffet av Datatilsynet, til en nemnd som skal være uavhengig av Kongen/departementet. Under 3 er problemstillingen den samme, men slik at diskusjonen tar særlig sikte på klager over Datatilsynets vedtak i saker der Kongen/departementet er part.

En noe annen problemstilling kommer opp når den uavhengige nemnd ikke lenger skal avgjøre klager (bare) over vedtak som er truffet av Datatilsynet, men (også) klager over vedtak truffet av Kongen eller departementet (se under 4).

Endelig skal jeg si litt om den konstitusjonelle adgang til å organisere Datatilsynet og klagenemnda direkte under Stortinget, på omtrent samme måte som Stortingets ombudsmann for forvaltningen i dag er organisert (se under 5).

2 UAVHENGIG NEMND TIL Å AVGJØRE KLAGER OVER VEDTAK AV DATATILSYNET

Emnet

På denne bakgrunn går jeg over til de mer spesifikke spørsmål som er stilt meg. Såvidt jeg skjønner er utgangspunktet at Datatilsynet også i fremtiden skal ha en forholdsvis høy grad av uavhengighet av Kongen og departementet. Det er også mulig at graden av uavhengighet vil bli økt ved at klager over vedtak som tilsynet treffer, ikke lenger skal gå til et departement, men til en egen klagenemnd e.l. I brevet av 17.9. 1996 tales det om

«et uavhengig organ som skal behandle klager over tilsynsorganets myndighetsutøvelse, herunder enkeltvedtak i forvaltningslovens forstand. Klageorganet skal i den forbindelse selv treffe enkeltvedtak og utøve annen tradisjonell myndighetsutøvelse.»

I norsk forvaltning finner vi mange organer som har en viss grad av uavhengighet av Kongen og/eller fagdepartementet (se nærmere i f.eks. *Eckhoff* og *Smith*: Forvaltningsrett (6. utg., 1997) s. 182 flg.). Dette gjelder åpenbart for en rekke organer med rådgivende funksjoner (f.eks. utredningsutvalg). Men det er også mange eksempler på organer som utøver forvaltningsmyndighet av samme type som den mulige klagenemnd i saker om personregistrering.

Som allerede nevnt er imidlertid det rettslige grunnlag som pretensjonen om uavhengighet skal hvile på, av stor betydning. Rettslig sett har ikke Kongen (regjeringen) selv evne til å gjøre forvaltningsorganer uavhengig av Kongen – så lenge ikke grunnlov, lov m.v. står i veien, vil Kongen alltid kunne omgjøre sine egne vedtak. Departementenes kompetanse er begrenset på samme måte, osv. Men departementene er bundet av bestemmelser som Kongen har truffet: Rettslig sett er det intet i veien for at Kongen kan gjøre bestemte forvaltningsorganer mer eller mindre uavhengig av det enkelte departement. På samme måte er lavere organer i forvaltningen bundet av bestemmelser truffet av Kongen eller et departement. Og *hele* forvaltningen er bundet av loven (så lenge ikke bestemmelser med høyere rang – f.eks. i grunnloven – står i veien).

Hvis et forvaltningsorgan skal sikres rettslig uavhengighet av forvaltningsorganer som er plassert høyere i forvaltningshierarkiet, må uavhengigheten altså forankres i bestemmelser i formell lov (eller grunnlov). Det er også til slike bestemmelser at vi må gå for å få beskjed om hvor omfattende uavhengighet det er tale om.

Den konstitusjonelle adgang

Lovs form er altså nødvendig for å sikre f.eks. Datatilsynet en viss uavhengighet av Kongen eller departementet. Utgangspunktet er også at loven *kan* sikre organer i forvaltningen en høy grad av uavhengighet i denne relasjon. Jeg kan ikke se at noen av de såkalte prerogativer i grunnloven kap. B representerer noen begrensning i dette utgangspunkt på personregisterlovens område. Og det har lenge vært enighet om at bestemmelsen i grl. § 3 om at «Den utøvende makt er hos Kongen», ikke har karakteren av prerogativ i den forstand at den skulle stå i veien for at Stortinget ved lov legger myndighet til andre enn Kongen. – Jeg lar det foreløpig stå hen om lovgivernes frihet i relasjon til grl. § 3 har noen grenser og hvor disse grensene i så fall går.

Det konstitusjonelle utgangspunkt er videre at statsråden overfor Stortinget (og eventuelt Riksretten) har det endelige ansvar for virksomheten i departementet og det underliggende forvaltningsapparat. Det har enkelte ganger vært anført at dette utgangspunkt står i veien for å legge myndighet til organer som Kongen eller departementet ikke kan instruere eller hvis vedtak de ikke kan omgjøre. Et slikt syn har imidlertid lite for seg. Statsrådenes ansvar kan ikke gå lenger enn deres myndighet rekker. Hvis Stortinget ved lov legger myndighet til et organ på en slik måte at deler av den myndighet for statsråden (eller regjeringen) som normalt vil følge av forvaltningsapparatets hierarkiske oppbygging (jfr. grl. § 3) er avskåret, kan statsråden heller ikke stilles til ansvar for forhold som ligger utenfor hans eller hennes myndighet.

Dette betyr likevel ikke at statsråden kan si seg fri for ansvar for alt som skjer (eller ikke skjer) på vedkommende område: For det første vil uavhengigheten i praksis aldri være absolutt (se under 1 ovenfor). For det andre gir bl.a. det hierarkiske utgangspunkt som følger av grl. § 3, grunnlag for å si at en statsråd har selvstendig ansvar for å følge med på «sitt» område. Tilsynet kan bl.a. gi grunnlag for – hvis nødvendig – å foreslå at Stortinget endrer loven, bevilger mer penger til formålet e.l. – Disse spørsmål er diskutert nærmere i min artikkel «Statsrådenes politiske og konstitusjonelle ansvar for statlige virksomheter med styre», Nordisk Administrativt Tidsskrift 1994 s. 91-110.

Problemstillingen har vært litt oppe i diskusjonen om Sametingets fremtidige rolle. I forbindelse med Opplæringslovutvalgets forslag om å gi Sametinget beslutningsmyndighet i bl.a. visse læreplansspørsmål, er den oppsummert på følgende måte:

«Utvalget understreker at [forslaget] ikke vil skape konstitusjonelle problemer så lenge kompetansen til å fastsette visse læreplaner og læreplantillegg legges til Sametinget ved lov. Det konstitusjonelle og parlamentariske ansvar som hviler på den fagstatsråd som til enhver tid er ansvarlig for opplæringssektoren, vil være tilsvarende begrenset. I hovedtrekk vil ansvaret være begrenset til de oppgaver som loven legger til departementet, og desuten til det mer generelle ansvar for å følge utviklingen i vedkommende sektor med sikte på etter behov å foreslå f.eks. lovendring eller budsjettmessige tiltak» (NOU 1995:18 Ny lovgivning om opplæring s. 263 sp. 1 – for ordens skyld gjør jeg oppmerksom på at jeg selv var leder for det utvalg som avga utredningen).

Opplæringslovutvalget viser videre til at Justisdepartementets lovavdeling, i brev av 26.1.1995 til Kommunal- og arbeidsdepartementet, uttaler seg «entydig i samme retning». Jeg legger derfor til grunn at det standpunkt jeg her gir uttrykk for, iallfall i sine hovedtrekk er juridisk holdbart.

Jeg nevner endelig at også forslaget om å opprette en uavhengig nemnd til å avgjøre klager over visse vedtak av Utlendingsdirektoratet (se Ot.prp. nr. 38, 1995-96), bygger på en forutsetning om at det er konstitusjonell adgang til å fastsette slike bestemmelser i lovs form. Det var andre grunner til at stortingsflertallet våren 1996 gikk imot forslaget.

Forskjellig fra det *rettslige* spørsmål om lovens adgang til å legge myndighet til forvaltningsorganer som i større eller mindre utstrekning skal operere på siden av det ordinære forvaltningshierarki, er spørsmålet om det *ønskelige* i en slik ordning. Stortingsvedtaket i 1977 om at statsforvaltningen «som hovedregel» skal organiseres på en slik måte at Kongen (og departementet) har «instruksjons- og kontrollmyndighet» over andre organer (Tid.S. 1976-77 s. 4077), hører nærmest hjemme i denne delen av problemstillingen.

Det er imidlertid verdt å nevne at vedtaket selv synes å bygge på en forutsetning om at det ikke er noe *konstitusjonelt* i veien for å legge beslutningsmyndighet til forvaltningsorganer som i en viss utstrekning skal være unndratt Kongens og departementets instruksjonsmyndighet m.v. Ellers ville det jo ikke ha noen hensikt å angi når det kunne komme på tale å *fravike* det hierarkiske utgangspunkt («særlige hensyn»).

Om vedtaket av 1977 skal jeg ellers nøye meg med å nevne at Stortinget ikke selv er bundet av det, hverken i plenum eller som lovgiver. Og overfor regjeringen begrenser vedtaket seg – som nevnt – stort sett til å angi at forslag om å gjøre unntak fra utgangspunktet om at forvaltningsapparatet skal organiseres i et hierarki under den politisk ansvarlige ledelse, må «begrunnes i særlige hensyn». Hvilke hensyn som Personregisterlovutvalget – eventuelt fulgt av departementet og regjeringen – vil (eller bør) anse gode nok til å begrunne et slikt unntak, er det ikke min oppgave å gå inn på.

Konklusjon: På Personregisterlovutvalgets område er det ikke noe konstitusjonelt til hinder for å legge beslutningsmyndighet til organer som i «faglig» henseende (jfr. under 1 ovenfor) skal opptre uavhengig av Kongen og/eller departementet.

Fortsettelse: Særlig om myndighet til å oppnevne medlemmer av klageorganet

Hverken Sametinget som organ eller den slags myndighet på opplæringsområdet som det er foreslått å legge dit (se ovenfor), er av samme karakter som det påtenkte klageorgan på personregisterlovens område. Men på iallfall to punkter er de to eksemplene av samme karakter: I begge tilfelle er det tale om kompetanse til å utøve offentlig myndighet. Og i begge tilfelle er det – eller kan det bli – tale om å la andre enn Kongen (eller departementet) oppnevne medlemmene.

Som kjent blir Sametingets medlemmer utpekt ved direkte valg, på samme måte som medlemmene av kommunestyre og fylkesting. Personregisterlovutvalget har vært inne på tanken om å foreslå at Stortinget skal oppnevne alle eller noen av klageorganets medlemmer. De to eksemplene har altså felles at (noen av) medlemmene av et organ som teknisk sett er en del av forvaltningen, utpekes (eller kan bli utpekt) av andre enn Kongen eller vedkommende fagdepartement.

Også når det gjelder oppnevningsmyndigheten, må det skilles mellom det som konstitusjonelt er mulig og det som – av politiske eller andre grunner – er ønskelig. Det er det førstnevnte punkt som er mitt emne her.

Stortinget er noen ganger tillagt myndighet til å oppnevne medlemmer av kollegiale organer i forvaltningen. Et forholdsvis ferskt eksempel på at Stortinget ved lov har gitt Stortinget i plenum myndighet til å oppnevne medlemmer av et organ som ikke er tillagt avgjørelsesmyndighet, gir loven av 3.2.1995 nr. 7 om kontroll

med etterretnings-, overvåkings- og sikkerhetstjenesten (men det kan hevdes at dette utvalget ikke er en del av «forvaltningen»). Noen eksempler på myndighet for Stortinget til å oppnevne medlemmer av organer med avgjørelsesmyndighet i forvaltningen, er nevnt i Ingvaldsen-komiteéns innstilling (NOU 1972:38) – forøvrig er det fortsatt slik at Stortinget oppnevner bl.a. hovedstyrets formann i Statens Fiskarbank (se lov av 28.4.1972 nr. 22). Men jeg har ikke i farten kunnet finne eksempler på at denne modellen er fulgt for organer med kompetanse av samme type som det påtenkte organ til å behandle klager over vedtak av Datatilsynet.

I den senere tid har det også vært foreslått å tildele Stortinget en rolle i utvelgelsen av personer til å bekle stillinger eller verv som forutsetningsvis skal utøves uavhengig av Kongen eller departementet (f.eks. sentralbanksjef eller dommer i Høyesterett). Men i slike tilfeller behøver ikke løsningen å ligge i at Stortinget alene oppnevner de aktuelle personene; en annen, nærliggende modell er at Kongen beholder myndighet til å utpeke personer som Stortinget har godkjent. Dessuten har forslagene så langt ikke ført frem.

Da Datatilsynet ble oppnevnt, foreslo et flertall i stortingskomiteén å gi Stortinget myndighet til å oppnevne medlemmene av styret (jfr. Innst.O. nr. 47, 1977-78). Når forslaget falt, var det ikke fordi en slik løsning ble ansett for å være konstitusjonelt umulig.

Dette er også mitt standpunkt. Så lenge det ikke står i strid med prerogativene etter grunnloven kap. B (se ovenfor), kan jeg ikke se noe konstitusjonelt til hinder for at Stortinget i lovs form gir Stortinget i plenum kompetanse til å oppnevne medlemmer av det påtenkte klageorganet. Dette gjelder uten hensyn til om myndigheten gjelder alle eller bare noen av medlemmene.

Utgangspunktet om hierarkiske organisering av statsforvaltningen (jfr. bl.a. grl. § 3) kan ikke antas å stå i veien for en slik løsning. Iallfall i prinsippet vil løsningen heller ikke avvike mer fra utgangspunktet om at statsrådene har ansvar for forvaltningens virksomhet enn det som følger allerede av lovbestemmelser om at deler av organets myndighet skal utøves uavhengig av Kongen og/eller departementet. Slike bestemmelser vil gjelde uten hensyn til om organets medlemmer er utpekt av Kongen/departementet eller av f.eks. Stortinget. Og omvendt vil ikke oppnevning av Stortinget i seg selv være nok til å unndra de som sitter i de aktuelle stillinger eller verv, fra instruksjonsmyndighet som det ellers måtte være grunnlag for (sml. her bemerkningen i NOU 1972:38 på s. 41 sp. 1).

Når svaret byr på tvil, kan vårt syn på hvor omfattende uavhengighet det er tale om, riktignok bli påvirket av bl.a. hvor oppnevningsmyndigheten ligger (se nærmere f.eks. i *Eckhoff og Smith: Forvaltningsrett* s. 187 flg.). Men noen diskusjon om hva som måtte være gjeldende rett på dette punkt etter at personregisterloven er endret, er det ingen grunn til å ta opp her. Det som er viktig, er at organets stilling blir gjort klart mulig i loven selv.

Både Ingvaldsen-komiteén og utenriks- og konstitusjonskomiteén i Stortinget synes å bygge på at det ikke vil være noe konstitusjonelt til hinder for å la Stortinget oppnevne medlemmer av kollegiale forvaltningsorganer med vedtaksmyndighet; ellers gir det jo ikke mening å uttale seg om når slik oppnevning «bør» eller ikke bør skje. De mer eller mindre restriktive utsagn om Stortingets adgang til å oppnevne medlemmer av forvaltningsorganer med vedtaksmyndighet som finnes i NOU 172:38 s. 41 (jfr. s. 38-40) og i Innst.S. nr. 277 (1976-77) s. 14-15, tar etter alt å dømme sikte på det *ønskelige* i slike ordninger. Det er ikke min oppgave å gå inn i noen diskusjon av dette spørsmål.

Konklusjon: Det er ikke noe konstitusjonelt til hinder for at Stortinget ved lov gir Stortinget i plenum myndighet til å oppnevne medlemmer av det påtenkte klageorgan.

3 SÆRLIG OM UAVHENGIG NEMND TIL Å AVGJØRE KLAGER OVER DATATILSYNETS VEDTAK I SAKER DER KONGEN OG/ ELLER DEPARTEMENTET ER PART

Emnet

Den foregående diskusjon av adgangen til å opprette en uavhengig nemnd til å avgjøre klager over Datatilsynets vedtak, har ikke tatt hensyn til hvem som er part i de sakene som blir forelagt klagenemnda. Det tilleggsspørsmål som brevet av 6.12.1996 tar opp, er om adgangen til å legge avgjørelsesmyndighet i klagesaker til en slik nemnd, blir snevrere i saker der Kongen eller et departement opptrer som part.

Slik partsstatus vil kunne foreligge når Datatilsynet behandler saker om registre som eies av Kongen/departementet. Slike saker må holdes adskilt fra saker der Kongen og/eller departementet selv treffer vedtak etter personregisterlovgivningen (se nærmere under 4 nedenfor). Grensen mellom posisjonene som registreier og som vedtaksmyndighet vil neppe være vanskelig å trekke.

Spørsmålet er som utgangspunkt generelt. Men ifølge brevet springer det særlig ut av en bestemt side av departementets rolle etter personregisterloven (slik den lyder i dag): Etter § 41 gjelder ikke konsesjonsplikten etter § 9 jfr. § 10 for personregistre i organ for stat eller kommune som er opprettet ved egen lov.

Ordlyden («som») kan tyde på at det er *organet* som må være opprettet ved «egen lov». På sin side legger brevet av 6.12.1996 tilsynelatende til grunn at unntaket for konsesjonsplikt tar sikte på *registre* som er opprettet ved lov. For det spørsmål som brevet tar opp, er det imidlertid uten betydning hvilket svar man vil gi på dette tolkningsspørsmålet.

Det kan oppstå tvil om betingelsene etter § 41 for å opprette personregister uten konsesjon, er oppfylt. Ifølge brevet er det i så fall Justisdepartementet som avgjør saken, mens Administrasjonsdepartementet (nå: Planleggingsdepartementet) avgjør om det foreligger konsesjonsplikt i saker der Justisdepartementet er part.

Spørsmålet er altså om en klagenemnd som skal være uavhengig *både* av Kongen og departementet, kan gis kompetanse til å avgjøre tvilsomme rettsspørsmål i saker der Kongen eller et departement er part.

Spørsmålet kan behandles uten hensyn til om det er Kongen *eller* departementet som er part. I den sammenheng jeg her tar sikte på, er det ingen konstitusjonell grunn til å skille mellom «Kongen i statsråd» og «departementet». Etter grunnloven er departementene «statsrådets kontorer», departementssjefen er samtidig medlem av regjeringen, og en statsråd er ansvarlig overfor Stortinget (og Riksretten) både som departementssjef og som medlem av Kongens råd. Til dette kommer at myndighet som etter lov ligger til «vedkommende departement» eller til «departementet», også kan utøves av Kongen i statsråd, og at Kongen som hovedregel har kompetanse til å delegere sin myndighet til departementet (begrensningene i dette utgangspunkt går jeg ikke inn på). Det videre diskusjon kan derfor skje uavhengig av om det er Kongen eller departementet som opptrer som part.

Den konstitusjonelle adgang

Det klare utgangspunkt er at rettsregler gjelder inntil de blir endret. Dette gjelder også i saker der personregisterloven kommer til anvendelse på registre som eies av Kongen eller et departement.

På den annen side har også Kongen og departementet vid adgang til å fastsette og endre rettsreglene ved å bruke forskriftsmyndighet som de har fått tildelt i mange lover. Innenfor rammen av gjeldende lov (og av EF-direktivet) vil dette kunne

gjelde også på personregisterlovens område. I den grad slik kompetanse måtte bli gitt, og kompetansen omfatter også den type av spørsmål som brevet av 6.12.1996 tar sikte på, vil den kunne benyttes til å gi forskrift om hvorvidt offentlige eide registre skal være undergitt konsesjonsplikt.

Hvis det ikke er aktuelt å legge slik forskriftskompetanse til Kongen/departementet, er utgangspunktet – som nevnt – at loven gjelder inntil den blir endret. Da må det organet som loven gir myndighet til å treffe vedtak, selv ta standpunkt til lovens nærmere innhold. Denne myndigheten må utøves på vedtaksorganets eget ansvar. Plikt for organet til å legge den lovtolkning til grunn som en part i en sak går inn for, vil representere en tilsvarende beskjæring av organets uavhengighet av parten.

Også kompetanse for Kongen/departementet til å gi bindende instruks om lovens innhold i det enkelte tilfelle, vil åpenbart representere et inngrep i uavhengigheten til det organ som instruksjonen er rettet til. Ut fra hensynet til mest mulig klare ansvarsforhold, er det formen «instruks» som eventuelt bør velges hvis Kongen/departementet likevel skal gis kompetanse til å «styre» Datatilsynet eller klagenemnda i enkeltsaker, slik at det ikke er aktuelt å gi forskrift (se ovenfor). Men den praktiske forskjell mellom de to former må ikke overdrives: Autoritative standpunkter til lovens tolkning i enkeltsaker blir uforsvarlige hvis de ikke etter sitt innhold kan legges til grunn også i andre saker av tilsvarende karakter.

Uavhengighet innenfor grensene av de lovbestemmelser som gjelder til enhver tid, må altså være utgangspunktet – her som overalt ellers. Jeg har tidligere kommet frem til at en slik løsning i sin alminnelighet ikke kan by på konstitusjonelle problemer. Det har lenge vært akseptert at loven kan opprette organer som er uavhengige (også) i den forstand at den instruksjonsmyndighet for Kongen/departementet som ellers ville ha foreligget, er avskåret.

Jeg kan ikke se noen grunn til å anta at løsningen må bli en annen der Kongen/departementet er part i de saker som verserer. Den type avgjørelser som vi tar sikte på her, faller klart utenfor de områder som etter grunnloven er undergitt kongelig prerogativ. Dette betyr at lovgivningen som utgangspunkt står fritt.

Jeg kan ikke se at partsstatus for Kongen/departementet gir noe grunnlag for å fravike dette utgangspunktet – i seg selv gir jo ikke slik status noen myndighet til å treffe rettslig bindende avgjørelser. Jeg kan heller ikke se at dette gir noe grunnlag for å fravike utgangspunktet om at loven står fritt til selv å bestemme hvem som skal oppnevne medlemmer av den påtenkte klagenemnda.

Konklusjoner: De samme som under 3 ovenfor.

4 UAVHENGIG NEMND TIL Å AVGJØRE KLAGER OVER VEDTAK AV KONGEN OG/ELLER DEPARTEMENTET

Emnet

Så langt har jeg tatt sikte på adgangen til å opprette et organ til å avgjøre klager over vedtak som er truffet av Datatilsynet. Hvis man tar sikte på å etablere et uavhengig forvaltningsorgan til å avgjøre klager over rettslig bindende vedtak som er truffet av Kongen og/eller departementet, kommer enkelte spørsmål i tillegg.

På samme måte som i relasjon til klagenemndas kompetanse i saker der Kongen/departementet er part, legger jeg også her til grunn at den konstitusjonelle adgang til å legge avgjørelsen av klager til et uavhengig organ er den samme enten det påklagede vedtak er truffet av Kongen eller av departementet. Forutsetningen er selvsagt at nemnda skal være uavhengig av *både* Kongen og departementet.

Til realiteten nevner jeg først at det ikke er noen konstitusjonelt avgjørende grunn til å anta at klager over f.eks. Datatilsynets avgjørelser alltid må kunne rettes

til Kongen/departementet (eller at Kongen/departementet må sikres adgang til å gripe inn på eget initiativ). Som jeg tidligere har vært inne på, vil adgang for Kongen/departementet til å omgjøre vedtak som lavere plasserte organer i forvaltningen har truffet, være et viktig skår i disse organenes uavhengighet. Jeg har også nevnt at adgangen til å skape slik uavhengighet ved lov, som utgangspunkt er utvilsom.

Statens teleforvaltning og Statens teleforvaltningsråd gir forholdsvis nye eksempler på at en viss uavhengighet av departementet er tilsiktet. Men eksemplene kan også brukes til å illustrere at viljen til konsekvent å gjennomføre en slik linje ikke har vært uten grenser. For det første er det Kongen selv som har bestemt at klage over enkeltvedtak truffet av Statens teleforvaltning skal avgjøres av Statens teleforvaltningsråd (se f.eks. kgl.res. av 7.12.1994 nr. 1182 om forskrift om leide samband i offentlige telenett § 18). Dette betyr at Kongen også kan oppheve bestemmelsen eller eventuelt selv overta behandlingen av enkelte klagesaker. For det andre har Kongen bestemt at klagesaker «av prinsipiell betydning eller telepolitisk karakter» likevel skal avgjøres av departementet. Betydelig potensiell usikkerhet ligger her allerede i at de nevnte begreper er lite presise. Men det viktigste er å få frem at bestemmelser av denne typen innebærer at de avgjørelsene på området som presumptivt er mest sentrale, fortsatt skal være forbeholdt Kongen/departementet. Den uavhengighet som teleforvaltningsorganene utenfor departementet kan sies å nyte godt av, er tilsvarende begrenset.

Jeg nevner for ordens skyld at også den nye telekommunikasjonsloven av 23.6.1995 nr. 39 legger kompetansen til å «bestemme funksjonsfordelingen» mellom de nevnte organene til Kongen (som endog har delegert sin myndighet til departementet), se § 1-5. Av det som tidligere er sagt om betydningen av rettslig form på dette området, følger at loven på dette punkt ikke avspeiler noen sterk vilje til å sikre de aktuelle kontrollorganene en høy grad av uavhengighet i forhold til Kongen og departementet.

Det er altså ikke grunn til å anta at det rettslig er noe i veien for å legge avgjørelsen av klager over Datatilsynets vedtak direkte til det påtenkte klageorgan uten at klagen først er behandlet av Kongen/departementet. I den grad uavhengighet av Kongen/departementet er tilsiktet, er det også denne vei man *bør* gå.

Den konstitusjonelle adgang

Ifølge brevet av 17.9.1996 er det likevel en mulighet for at avgjørelsen av klager over vedtak av Datatilsynet vil bli lagt til Kongen/departementet med *etterfølgende* adgang til overprøving i det påtenkte klageorgan. En slik løsning vil gripe inn i utgangspunktet om politisk, parlamentarisk og konstitusjonelt ansvar for regjeringen og for den enkelte statsråd på en helt annen måte enn hvis det påtenkte klageorganet bare skal overprøve vedtak av Datatilsynet.

Det konstitusjonelt forsvarlige i en slik løsning byr på adskillig tvil. Mitt syn er at et slikt inngrep i utgangspunktet om regjeringens og statsrådenes ansvar overfor Stortinget er betenkelig. Det konstitusjonelle utgangspunkt om maktfordeling vil være bedre tjent med at kontrollen med de skjønnsmessige sider av vedtak som Kongen eller departementet har truffet, på vanlig måte blir forbeholdt Stortinget. Når partene i den enkelte sak bestrider at vedtak som er truffet av Kongen/departementet er rettmessige, er domstolene rette adressat.

Denne argumentasjonen kan ikke sies å være logisk bindende. Også i denne relasjon er det mulig å si at statsrådenes ansvar ikke kan gå lenger enn deres myndighet: Hvis loven har lagt klagemyndighet til et organ som skal være uavhengig av Kongen/departementet, kan statsrådene ikke gjøres ansvarlig for hva dette organet

foretar seg. Men mitt syn er likevel at en ordning der organer i forvaltningen skal ha myndighet til å overprøve vedtak av Kongen/regjeringen, er betenkelig sett på bakgrunn av elementer av grunnlovens maktfordelingssystem som fortsatt er i behold (og som det er grunn til å beholde): Jeg tenker på prinsippet om handlefrihet for regjeringen på regjeringens eget ansvar – overfor Stortinget og overfor domstolene.

Trygderetten er det kanskje mest utpregede eksempel på et forvaltningsorgan med domstollignende oppgaver og organisering. Dette organet overprøver vedtak av trygdemyndighetene. Men etter § 2, 2. ledd i trygderettsloven av 16.12.1966 nr. 9 kan Trygderetten ikke prøve vedtak som treffes av Kongen eller et departement. Lovkomitéen hadde ikke foreslått noen slik bestemmelse, men den kom inn i loven etter forslag i proposisjonen. Begrunnelsen lyder:

«Justisdepartementet har uttalt at det av konstitusjonelle grunner neppe vil være adgang til å gi et selvstendig forvaltningsorgan rett til å overprøve avgjørelser som er tatt av Kongen eller et departement» (jfr. Ot.pr. nr. 5 (1966-67) s. 13-14).

I det utrykte brev fra Justisdepartementet som proposisjonen viser til, er den nevnte uttalelsen ikke nærmere utdypet eller begrunnet. *Ole-Erik Øie*: Trygderetten og dens rettsanvendelse (1994) s. 62 antar at departementet har «hatt i tankene bestemmelsen i grunnlovens § 3 om at den utøvende makt er hos Kongen og i § 12 tredje ledd om at Kongen fordeler forretningene blant statsrådets medlemmer. Kanskje hadde man også lydighetsbudet i grunnlovens § 21 i tankene». Jeg finner imidlertid ikke grunn til å gå inn i spekulasjoner om hvilket resonnement som ligger bak.

Jeg gjør for ordens skyld oppmerksom på at både Øie, Eckhoff og Frihagen antar at Trygderetten har kompetanse til prejudisielt å prøve *forskrifter* gitt av Kongen eller departementet (se Øie, op.cit. s. 62 flg. med videre henv.). Men dette spørsmålet er ikke identisk med det jeg her diskuterer, og jeg skal ikke gå nærmere inn på det.

Også Forvaltningskomitéen (1958) er såvidt inne på spørsmålet. Utgangspunktet tas i en diskusjon om hvorvidt den ordning med en stortingsoppnevnt ombudsmann for forvaltningen som komitéen foreslo, ville kreve grunnlovsendring i den grad ombudsmannen «skal kunne utøve kontroll i saker som er behandlet av departementet og statsrådene». Komitéens svar er at det ikke skulle være nødvendig med grunnlovsendring «når ombudsmannen ikke har avgjørelsesmyndighet» (s. 427).

Uttalelsen er meget kort, den er ikke nærmere begrunnet, og den gjelder ikke direkte den situasjon som jeg her tar sikte på. Men i den grad den likevel kan tillegges vekt, må den telle til støtte for det syn at myndighet til å overprøve avgjørelser av Kongen eller departementene, av konstitusjonelle grunner ikke kan legges til uavhengige forvaltningsorganer med vedtaksmyndighet.

Som en kommentar til proposisjonens begrunnelse for bestemmelsen i trygderettsloven § 2, 2. ledd (se ovenfor) har *Eckhoff* i motsatt retning gitt uttrykk for at han finner det «vanskelig å forstå hvilke forfatningsregler som skulle være til hinder for» at et uavhengig forvaltningsorgan gis myndighet til å overprøve avgjørelser av Kongen og departementene (Forvaltningsrett, 5. utg. s. 611; i *Eckhoff* og *Smith*: Forvaltningsrett, 6. utg. er denne uttalelsen tatt ut, se s. 622). Også *Frihagen* gir uttrykk for at det etter hans «skjønner ikke [ville] representere noe brudd med våre forfatningsregler om en hadde fulgt lovutvalgets forslag» om å gi Trygderetten adgang til å prøve også vedtak av Kongen og departementet (Forvaltningsrett, Bind III (4. utg., 1992) s. 100-101).

Heller ikke disse to forfatterens synspunkter er nærmere begrunnet. Men mitt inntrykk er nok at de knytter seg forholdsvis nært til Trygderettens karakter som «de facto domstol». Det var nærmest bare i navnet at man avsto fra også formelt å karakterisere den som en «domstol». Men resultatet ble altså at Trygderetten rettslig sett må karakteriseres som et forvaltningsorgan (i *Eckhoff* og *Smith*: Forvaltningssrett s. 619 flg. o.a.st. nevnes den som et viktig eksempel på et «domstollignende forvaltningsorgan»). Det er dette som gir eksemplet interesse i vår sammenheng.

Jeg nevner også at Justisdepartementets syn, som proposisjonen til trygderettslov bygger på, godt kan være holdbart selv om det ikke kan pekes på bestemte «forfatningsregler» som står i veien. Mine betenkeligheter med den løsning som er antydnet, bygger mer på trekk ved det konstitusjonelle system som sådan enn på bestemte «regler».

Som nevnt må spørsmålet anses for å være tvilsomt. Mitt samlede syn er likevel at de argumenter med tilknytning til maktfordelingssystemet som jeg har skissert, har mye for seg. Det er grunn til å fastholde det utgangspunkt som ligger i at det politiske, parlamentariske og konstitusjonelle ansvar for Kongens/departementenes egen virksomhet hviler på den enkelte statsråd og på regjeringsskollegiet. Kontroll med regjeringens utøvelse av skjønnsmessig myndighet hører først og fremst hjemme i Stortinget. Det samme gjelder kontrollen med at vedtak som er truffet av Kongen/departementene, ligger innenfor de rettslige grenser for disse organenes myndighet.

Rettslig kontroll etter initiativ fra partene i den enkelte sak (og fra andre med rettslig interesse, eller prejudisiell kontroll i straffeprosessens former) hører derimot først og fremst hjemme i domstolene. Dette gjelder også når de omstridte vedtak er truffet av Kongen/departementet. Og rent praktisk sett kan det ikke være mye å tjene på å skyte en klagenemnd e.l. inn mellom forvaltningsvedtaket og domstolene, som jo i alle tilfelle vil kunne få saken i siste instans.

Konklusjon: Jeg finner spørsmålet noe tvilsomt, men antar at et uavhengig forvaltningsorgan ikke kan tillegges myndighet til å avgjøre klager over vedtak som er truffet av Kongen/departementet.

Fortsettelse: Særlig om myndighet til å oppnevne medlemmer av klageorganet

Det foregående diskusjon om adgangen til å legge overprøving av vedtak som er truffet av Kongen/departementet til et uavhengig forvaltningsorgan, gjelder uten hensyn til hvem som skal utpeke medlemmene av det påtenkte klageorganet. Det samme gjelder min negative konklusjon.

På denne bakgrunn blir en diskusjon om hvorvidt medlemmene av det påtenkte klageorganet kan oppnevnes av Stortinget, rent subsidiær. Jeg skal derfor nøye meg med å nevne at de synspunkter som bærer konklusjonen i foregående avsnitt, også trekker i retning av at medlemmene av forvaltningsorganer som eventuelt skal overprøve avgjørelser av Kongen/departementene, iallfall ikke kan oppnevnes av Stortinget. En slik ordning vil bidra ytterligere til å forkludre utgangspunktet om at det er statsrådene som står ansvarlig for vedtak av Kongen og departementene.

5 UAVHENGIGHET GJENNOM ORGANISERING UNDER STORTINGET

Emnet

Endelig er jeg bedt om å drøfte den konstitusjonelle adgang til å organisere Datatilsynet direkte under Stortinget. Organisatorisk måtte det vel bli tale om en modell

som omtrent tilsvarende den måte som f.eks. Stortingets ombudsmann for forvaltningen er organisert på.

Oversendelsen av 4.1. d.å. viser at utvalget særlig har tenkt på organiseringen av Datatilsynet. Den viser videre at tilsynet etter forutsetningen «fortsett skal treffe rettslig bindende vedtak, for eksempel ved konsesjonsbehandling eller ved å gi bindende pålegg om sletting».

Denne forutsetning må vel innebære at organiseringen av Datatilsynet i forhold til Stortinget reiser omtrent samme rettsspørsmål som den organisatoriske plassering av den påtenkte klagenemnd. I brevet av 17.9.1996 er det forutsatt at klagenemnda skal treffe rettslig bindende vedtak av samme type som Datatilsynet. Hvis det organ som skal overprøve tilsynets vedtak skal være en del av den utøvende makt, ville det ikke gi god sammenheng å legge «underinstansen» (Datatilsynet) inn under Stortinget.

Diskusjonen under 2-4 ovenfor gjelder adgangen til å gi (særlig) den påtenkte klagenemnda som forvaltningsorgan en høy grad av «funksjonell» uavhengighet i forhold til andre deler av den utøvende makt (særlig Kongen og departementet). Det spørsmål jeg her skal se på, gjelder ikke forholdet mellom forvaltningsorganer, men adgangen til å legge myndighet til å treffe bindende vedtak til organer som «skal høre direkte under Stortinget».

Skillet mellom «forvaltningsorganer» og organer «under Stortinget» er ikke alltid skarpt. Adgang for Stortinget til å oppnevne medlemmene av f.eks. klagenemnda vil representere et skritt i retning av å legge organet «under Stortinget». Dette gjelder uten hensyn til om det i andre relasjoner måtte være rimelig å betegne organet som et «forvaltningsorgan». Men det er ikke grunn for meg til å gå nærmere inn i disse spørsmål. For mitt formål er det tilstrekkelig å forutsette at det er tale om organer med beslutningsmyndighet som ligger «direkte under Stortinget» i den forstand at de administrativt (derunder i budsjettspørsmål) hører inn under nasjonalforsamlingen.

Graden av «funksjonell» (eller faglig) uavhengighet er det ikke nødvendig å gå inn på. Jeg skal likevel nevne at Stortinget som lovgiver har en viss adgang til å delegerer sin beslutningsmyndighet til Stortinget i plenum (slik det er gjort f.eks. i visse saker om konsesjon til vassdragsregulering). Også i saker som gjelder personregistre kan iallfall deler av beslutningsmyndigheten i teorien tenkes organisert på en slik måte. Men en slik løsning vil vanskelig kunne oppfylle rimelige krav til «funksjonell» (eller faglig) «uavhengighet» av politiske myndigheter. Jeg skal derfor se bort fra denne mulighet.

Siden det er tale om organer med beslutningsmyndighet i forhold til borgerne, legger jeg endelig til grunn at bestemmelser om organisering «under Stortinget» vil måtte gis ved lov.

Den konstitusjonelle adgang

Forutsetningen om at de aktuelle organer skal kunne treffe rettslig bindende vedtak, innebærer at eksempler hentet fra eksisterende organer «under» Stortinget gir liten veiledning.

Riksrevisjonen kan vi se bort fra allerede av den grunn at ordningen er hjemlet i grunnloven selv (§ 75 bokstav k).

Derimot var Stortingets ombudsmann for forvaltningen inntil nylig bare hjemlet i særlov (den nåværende bestemmelsen i grunnloven § 75 bokstav l ble vedtatt i 1995). Men Ombudsmannen skiller seg fra de organene som er aktuelle på personregisterlovens område ved at hans arbeid bare skal kunne ut i uttalelser, først og fremst om Ombudsmannens syn på den enkelte sak (se særlig § 10). Han kan rikti-

gnok treffe bindende avgjørelser av prosessledende karakter, f.eks. om krav om opplysninger (lovens §§ 7 og 8). Men det er liten grunn til å sette denne form for beslutningsmyndighet i samme stilling som slike former for myndighet til å treffe realitetsavgjørelser som etter forutsetningen skal ligge til Datatilsynet (og klagenemnda). Dette skyldes også at den nevnte type av rettslig bindende beslutninger som er lagt til Ombudsmannen, bare er rettet mot offentlige organer og tjenestemenn, ikke mot private.

Kontrollutvalget for etterretnings-, overvåknings- og sikkerhetstjenesten, som er underlagt Stortinget, er organisert ved lov (av 3.1.1995 nr. 7) uten spesifikk støtte i grunnloven. Men også dette organet savner myndighet til å treffe rettslig bindende avgjørelser om realiteten i de saker som det tar opp.

Så langt jeg har kjennskap til, har spørsmålet om den konstitusjonelle adgang til å legge tilsynsorganer m.v. med beslutningsmyndighet direkte inn under Stortinget, likevel aldri vært underkastet noen inngående vurdering. Dette er i seg selv en kilde til en viss usikkerhet.

En grunn til at spørsmålet ikke har vært inngående drøftet, kan tenkes å være at det alltid har vært ansett som klart at svaret måtte bli negativt. Konvensjonelle oppfatninger av denne typen kan imidlertid ikke ukritisk legges til grunn som konstitusjonelt «riktige».

Et negativt syn på den konstitusjonelle adgang er lagt til grunn i en utredning som Arve Føyen i 1982 utarbeidet etter oppdrag av Justisdepartementet (Complex nr. 1/83). Han antar at et organ «underlagt Stortinget må være et rent ombudsmannsorgan ... uten myndighet til» å treffe bindende vedtak av den typen som er tillagt Datatilsynet. Han har riktignok «ikke funnet konkrete holdepunkter for at det må være slik, men det er vel nærliggende å støtte seg til det alminnelige maktfordelingsprinsippet». Hans syn får en viss støtte i den etterfølgende lovproposisjon (Ot.prp. nr. 34, 1986-87, s. 10).

Innenfor de materielle grenser som grunnloven stiller opp (f.eks. mot å legge dømmende myndighet til Stortinget, jfr. § 96), vil Stortinget som utgangspunkt selv kunne utøve beslutningsmyndighet. Dette kan skje både i lov og ved plenarvedtak. Denne myndigheten kan også benyttes til å legge myndighet til domstolene og til den utøvende makt. Den er en mulighet som ofte har vært benyttet. Men dette betyr ikke uten videre at Stortinget også har kompetanse til å overføre beslutningsmyndighet til organer som er direkte underlagt Stortinget selv.

Når vi skal besvare det sistnevnte spørsmålet, må vi *for det første* huske at antallet organer i Stortinget som kan utøve beslutningsmyndighet, er langt lavere enn tallet på Stortingets «organer» i og for seg. Dette henger sammen med at grunnloven i første rekke legger kompetansen til å treffe rettslig bindende vedtak på vegne av den «lovgivende» makt til Stortinget, Odelstinget og Lagtinget. Alle vet at Stortingets komitéer i praksis spiller en meget stor rolle. Men komitéene har ikke myndighet til å treffe bindende vedtak om materielle spørsmål i forvaltningen. Det samme gjelder Sivilombudsmannen og Kontrollutvalget for etterretnings-, overvåknings- og sikkerhetstjenesten.

Uten at betydningen av dette uttrykket må drives for langt, kan vi altså si at de organer som administrativt er «direkte underlagt Stortinget», i første rekke skal tjene som *hjelporganer* for Stortinget (bl.a. i utøvelsen av nasjonalforsamlingens egen kontroll med forvaltningen). Noe unntak fra denne hovedregelen kjenner jeg ikke til.

For det andre må det nok regnes som et grunnleggende prinsipp i vår forfatning at utøvelse av offentlig myndighet som ikke er lagt til domstolene eller til Stortinget, skal utøves av organer som er underkastet det parlamentariske og konstitusjonelle ansvar for regjeringen og for den berørte statsråd. Omfanget av dette ansvaret

behøver ikke å være så stort – som jeg har vært inne på bl.a. under 2 ovenfor, vil statsrådets ansvar for «uavhengige» organer kunne være begrenset til en form for ansvar for å «følge med». Men slike grenser for ansvaret vil måtte bygge på de grenser for regjeringens instruksjonsmyndighet m.v. som er skapt av Stortinget som lovgiver. De representerer ikke i seg selv noe brudd med det grunnleggende prinsipp.

For det tredje har vi det moment om «maktfordeling» som bl.a. Føyen har nevnt. Dette momentet knytter an til grunnlovens skille mellom en «lovgivende» og en «utøvende» makt (se bl.a. grl. §§ 3 og 49). Dette skillet er selvsagt ikke uberørt av overgangen fra personlig kongemakt til parlamentarisme. Heller ikke i praksis er det helt skarpt; dette skyldes bl.a. at Stortinget som lovgiver noen ganger legger «forvaltningsmyndighet» til Stortinget i plenum (f.eks. i visse konsesjonssaker), og at det ikke er mulig å trekke noe materielt skille mellom «lovgivning» i formell lov og i forskrift. Men likevel er det etter mitt skjønn rimelig å si at det maktfordelingsprinsipp som har fått uttrykk i grunnloven, står i veien for å bygge opp et «forvaltningsapparat» direkte under Stortinget. Et datatilsyn eller en klagenemnd med beslutningsmyndighet som administrativt er lagt under Stortinget, vil nettopp representere en slik utvikling.

I forlengelsen av denne argumentasjonen nevner jeg at organisatorisk plassering «under» Stortinget sikkert vil få som konsekvens at reglene i bl.a. forvaltningsloven av 10.2.1967 ikke kommer til anvendelse. Hensynet til rettsikkerhet m.v. gjør det vanskelig å godta en slik konsekvens. Men siden det her ikke egentlig er tale om «konstitusjonelle» spørsmål, går jeg ikke videre i argumentasjonen.

Det er ikke helt klart for meg hva Føyen siktet til da han – i den ovenfor nevnte utredningen – ga uttrykk for at han manglet «konkrete holdepunkter» for sitt negative syn på den konstitusjonelle adgang til å legge beslutningsmyndighet til organer «underlagt» Stortinget. På samme måte som under 3 ovenfor vil jeg presisere at et svar kan være konstitusjonelt «riktig» selv om det ikke følger av bestemte «regler» i f.eks. grunnloven. Også i relasjon til det spørsmål som jeg her er opptatt av, vil svaret kunne tre frem av argumentasjon omkring vårt konstitusjonelle styringssystem mer generelt. I hvert fall et stykke på vei er det en slik argumentasjon som er ført frem i de foregående avsnitt.

Konklusjon: Jeg antar at Stortinget konstitusjonelt er avskåret fra å legge vedtaksmyndighet overfor borgerne til organer som administrativt ligger «direkte under Stortinget».

Vedlegg 6

Allmennmoralske normer for behandling av personopplysninger

Av Dag Elgesem

1 INNLEDENDE SAMMENDRAG

Det følgende er en beskrivelse og diskusjon av allmennmoralske normer for behandling av personopplysninger. Her står individets samtykke til overføring av personlige opplysninger sentralt. Normer for behandling av personopplysninger knytter seg til ulike 'kanaler' for flyt av personlig informasjon. Ulike sider ved personlig kontroll og samtykke til flyt av personlig informasjon i slike kanaler diskuteres. Samtykkemodellens sentrale rolle i våre etiske vurderinger, og dens begrensninger, illustreres avslutningsvis med et eksempel (oppsøkende genetisk informasjon) på et personvernproblem hvor individuelt samtykke ikke er tilgjengelig.

2 KANALER OG RESTRIKSJONER

Ulike sosiale arenaer er kjennetegnet ved ulikheter i flyt av personlig informasjon. For eksempel er det store forskjeller i så henseende i våre hjem, på en offentlig gate, i en politisk organisasjon, eller i et sykehus. Vi kan se slike arenaer som *kanaler* for flyt av personlig informasjon. Slike kanaler er kjennetegnet ved forskjellige typer restriksjoner. Det dreier seg for det første om restriksjoner på hvilket publikum som har tilgang til kanalen og den informasjonen som flyter der. For det andre dreier det seg om restriksjoner på hvilken type informasjon som får lov å flyte i kanalen, f.eks. om det er en kanal for overføring av sensitiv, personlig informasjon eller ikke. Ulike kanaler er kjennetegnet ved ulike sett av slike restriksjoner. For eksempel er det i våre hjem restriksjoner på hvilket publikum som har tilgang til kanalen, men ingen klare restriksjoner på hvilken type informasjon som får lov til å flyte der. Det er opp til de som bor der å bestemme. En gate eller et torg, derimot, er kjennetegnet ved at det ikke er noen restriksjoner på hvilket publikum som har tilgang til denne kanalen, men at det *er* klare restriksjoner på hvilken type informasjon som får lov å flyte i denne kanalen. For eksempel er det klare grenser for hva det er passende å ta opp med en tilfeldig sidemann på T-banen. Et tredje eksempel på en kanal for flyt av personlig informasjon er livet i en politisk organisasjon. Her er det noen milde begrensninger på hvem som har tilgang til kanalen. Men det er relativt lik tilgang for alle som først er tilknyttet. Det er også normer for hvilken type informasjon som får flyte der, men disse er mye mer liberale enn på en åpen gate for eksempel. Et fjerde eksempel på en kanal for flyt av personlig informasjon i denne vide forstanden, er et sykehus med sine rutiner for informasjonsbehandling, pasientarkiver, o.s.v. Her er det også klare begrensninger på hvilket publikum som har tilgang til kanalen, og på hvilken type informasjon som får flyte der. Disse begrensningene er imidlertid mye strengere enn tilfellet er for en politisk organisasjon.

Restriksjonene som kjennetenger ulike kanaler kan være enten *normative* eller *fysiske*. Taushetsregler for helsepersonell er eksempel på normative restriksjoner på hvilket publikum som har tilgang til den personlige informasjon som overføres og genereres i en helseinstitusjon. Veggene i et hus er fysiske restriksjoner på andres tilgang til denne kanalen. Restriksjoner på hvilken type informasjon som får lov å flyte i en kanal er primært normative. Ved et legebesøk er det normer som – i for

stor grad, mener noen – sikrer at det blir fokusert på overføring og generering av informasjon om sykdom. Men i tillegg til disse normative begrensningene er desuten tiden som er avsatt til hver pasient, en fysisk begrensning på mulighetene til å kommunisere om annet enn sykdommen.

Vi beveger oss inn og ut av kanaler for flyt av personlig informasjon. Når vi velger å gå inn i ulike kanaler, må vi ta hensyn til de restriksjonene som gjelder der. Ulike kanaler gir ulik type av kontroll. På en åpen gate har man for eksempel ikke kontroll over publikum, d.v.s. *hvem* som får del i den personlige informasjonen som genereres i denne kanalen (hvor man er, hva man har på seg, hvem man går sammen med, o.s.v). Til gjengjeld slipper man unna uten at det genereres særlig *sensitiv* informasjon. Det er som nevnt også normer *mot* å bli for personlig og påtrengende i slike arenaer. I et privat hjem er det andre normer. Her er det ikke normer mot å være personlig. Slike private sfærer gir derimot rom for utvikling av personlige relasjoner. I utviklingen av slike relasjoner spiller personlig informasjon en viktig rolle. Våre personlige relasjoner, og graden av nærhet og intimitet i dem, er i stor grad en funksjon av hvor mye og hvor sensitiv informasjon vi lar flyte i dem. I arenaer for utvikling av personlige relasjoner er det derfor svært viktig at vi selv har personlig kontroll over akkurat hvem som får hvilken informasjon om oss, fordi vår kontroll av kvaliteten av våre relasjoner avhenger av dette. Kontrollen kan ikke utøves i kraft av fastlagte normer for hvor personlige vi bør være.

Det er også innenfor offentlige arenaer ofte rom for privat kommunikasjon, der det er begrensninger på flyt av informasjon til den offentlige delen av kanalen. Det finnes 'nøstete' sfærer, d.v.s kanaler inne i kanaler. På et nivå vil en kanal for flyt av informasjon ha normer for dannelsen av mer private og begrensede kanaler innenfor sine egne rammer. En benk i en park er et eksempel på en arena som tillates brukt som et privat rom, beskyttet av felles normer mot inntreden. Normene som beskytter denne private kanalen befinner seg imidlertid på det offentlige nivået.

3 TO FORMER FOR SAMTYKKE

Vi har beskrevet kanaler i termer av restriksjoner på publikum og på type av informasjon. I tillegg trenger vi en annen dimensjon for å beskrive kontroll i kanaler. Det ble påpekt ovenfor at det i et privat hjem er sterk kontroll over hvilket publikum som har tilgang, men få restriksjoner på hvilken type informasjon som får genereres der. Dette er strengt tatt ikke riktig. Det er restriksjoner også her. Jeg leser for eksempel ikke min kones brev. Poenget er imidlertid at dette er restriksjoner som det er opp til de involverte å bestemme. Dette er forskjellig fra de normene som gjelder for kontakt med fremmede på en gate. Vi kan skille mellom *faste* restriksjoner av typen offentlige normer, og *flytende* restriksjoner som det er opp til aktørene å fastlegge.

Dette skillet mellom kanaler med restriksjoner som er faste og kanaler med restriksjoner som det er opp til de som kommuniserer i kanalen å fastlegge, gir opphav til en forskjell i typer kontroll over personopplysninger. I arenaer med flytende restriksjoner har vi en stor grad av kontroll over informasjonsstrømmen. I et privat hjem, f.eks. kan vi bestemme hvem som skal ha hvilken informasjon om oss. Hvem personene er spiller en rolle for oss, og vi har stor grad av kontroll over hvem som får tilgang til oss i denne kanalen. Som nevnt over gjør dette at private sfærer er arenaer for utvikling av personlige relasjoner. Kall denne formen for kontroll muligheten til å samtykke *i* kanalen. Et sykehus, derimot, er ikke primært en arena for personlige relasjoner. Her har vi ikke den samme detaljerte kontroll over hvilke konkrete personer som får tilgang til den informasjonen om oss. Ved kontakt med sykehuset må vi bare godta de prosedyrer for informasjonsbehandling sykehuset har. Vi har ikke som pasienter kontroll over akkurat hvem som har informasjon om

oss selv, hvordan den registreres, hvilke konkrete personer som har tilgang til den. Vi må akseptere at den brukes til de formål den er samlet inn for. Kall dette for et samtykke *til* kanalen.

Personvern er primært en beskyttelse av et samtykket *til* en kanal. Privatlivets fred, 'privacy', er primært en beskyttelse av muligheten til å samtykke *i* kanalen. Personvernet skal sikre at de betingelsene som personen forutsatte når han eller hun ga sin samtykket til kanalen, ikke forandres. For det første må samtykket være informert. Det betyr at det må være mulig å vite hvilken informasjon som blir overført, generert og registrert, utfra kjennskap til virksomheten til den institusjonen som man oppgir informasjon til. For det andre skal personvernet sikre at forutsetningene for samtykket ikke undergraves gjennom informasjonsbehandlingen. Det betyr for eksempel at informasjonen ikke må lekke ut i andre kanaler enn der hvor den er oppgitt.

Et slikt samtykke til en kanal er i en viss forstand tøyelig. Vi må godta at informasjonen brukes til de formål som den er samlet inn for, men har ikke detaljert kontroll over hvilke konkrete personer som har tilgang til informasjonen, og akkurat hvordan den brukes. Når vi oppgir informasjon om oss selv, for eksempel i forbindelse med medisinsk behandling, må vi stole på at informasjonsbehandlingen er begrenset av restriksjoner som springer ut av formålet med innsamlingen. Grensene for hva som er forenlig med formålet er tøyelige. For eksempel er det rimelig å si, slik loven gjør, at det er forenlig med samtykket til overføring av informasjon i forbindelse med behandling i sykehus, at denne informasjonen brukes til administrasjon og planlegging, og til forskning. Men dette setter ikke en klar grense for bruken.

Det er verd å merke seg at det ikke er opp til den registrerte å fastlegge grensene for bruken av informasjon i slike sammenhenger. Det fremstilles noen ganger som et allment personvernprinsipp at «informasjon som er samlet for ett formål, ikke skal brukes til et annet formål». Dette kan forstås slik at informasjonen ikke skal brukes til andre formål enn de personen hadde i det han oppga informasjonen. Dette kan imidlertid ikke være helt riktig. For eksempel er det rimelig å kontrollere opplysninger som er gitt i forbindelse med søknader om økonomisk støtte fra det offentlige, mot andre informasjonskilder. Ta nå personer som bevisst forsøker å få en stønad som de ikke har rett på. Slik kontroll av opplysningene er ikke en del av formålet som de har idet de oppgir informasjon om seg selv. Likevel kan de ikke med rimelighet motsette seg slik kontroll. Poenget er å illustrere at det ikke er opp til den registrerte å avgjøre hva som er formålet som informasjonen er samlet inn for. Formålet informasjonen brukes til må imidlertid, som påpekt ovenfor, være opplagt ut fra kjennskap til virksomhetens art.

I den etiske vurderingen av behandling av personopplysninger spiller således samtykke en sentral rolle. Et minimum for den individuelle kontroll er at den registrerte skal vite om hvilken informasjon andre har om en selv. Som regel ønsker vi noe mer, nemlig å få gi vår tilslutning til innsamlingen i forkant av denne. Mulighet til samtykke i forkant av overføringen, er en definisjon på en eiendomsrett. Dette må ikke forveksles med at vi alltid kan velge ikke å gi fra oss informasjon. Livet i et moderne samfunn er ikke mulig uten stadig å oppgi informasjon om oss selv. *Frivilligheten* av samtykket til oppgivelsen er derfor ofte begrenset. Men også i slike situasjoner er muligheten til å gi sin tilslutning til oppgivelsen viktig. Dels fordi det gir oss mulighet til å ta det med i betraktning i våre andre planer. Dels er det å anerkjenne folks rett til kontroll over informasjon om selv, en viktig måte å uttrykke respekt for dem som autonome personer.

En normativ betraktning i denne sammenhengen er at i situasjoner hvor friheten til å velge å ikke oppgi informasjon om seg selv er begrenset, der blir det desto mer påkrevet at risikoen for personvernkrænkelser er svært lav. Dette er ofte tilfellet i et

moderne informasjonssamfunn. Dessuten er det da rimelig at den som eier registeret bærer kostnadene ved å redusere risikoen for personvernkremler, ikke den registrerte selv.

4 ET EKSEMPEL PÅ SAMTYKKEMODELLENS BEGRENSNINGER: OPPSØKENDE GENETISK INFORMASJON

I den allmenmoraliske vurderingen av behandling av personopplysninger spiller altså appell til samtykke en sentral rolle. Men ikke alle personvernproblemer kan håndteres bare ved å kreve en eller annen form for samtykke. Den pågående diskusjonen om oppsøkende genetisk informasjon viser dette.

Det best dokumenterte eksemplet på problemet dreier seg om genetisk testing for arvelig forhøyet kolesterol (hyperkolesterolemi). Personer med arvelig forhøyet kolesterol har en svært stor risiko for tidlig hjerteinfarkt. Lidelsen arves dominant, d.v.s. at barn av personer med hyperkolesterolemi har 50% sjans for også å ha lidelsen. Man har imidlertid utviklet en virksom medisin som reduserer risikoen vesentlig, samt en test som med sikkerhet fastslår om man er bærer av det defekte genet. Lipidklinikken ved Rikshospitalet ønsket å utvikle et tilbud om slik testing for familier hvor denne lidelsen forekommer. Man ville ta utgangspunkt i pasienter som de hadde til behandling ved klinikken. Så ville man ved hjelp av slektsdatabaser gå bakover i slektstreeet for å finne opphavet til defekten. Fra disse tidlige bærerne skulle man så lete seg frem til nålevende bærere av det defekte genet. Disse skulle kontaktes med tilbud om test og eventuell senere behandling.

Prosjektet er foreløpig lagt i bero av personverngrunner. Det er to problemer. For det første ville det genereres personlig, sensitiv informasjon om personer uten at de vet om det. Personene som letes opp har ikke gitt sitt samtykke til den kanalen der informasjonen fremskaffes. Det andre problemet er knyttet til tilbakeføringen av informasjonen til personene i risikogruppen. Forarbeidene til lov om medisinsk bruk av bioteknologi tillater oppsøkende genetisk informasjon via slektninger, men ikke direkte av en lege som ikke har den oppsøkte personen som pasient. Problemet er, i de termer vi har operert med her, at man regner med at personer i samme slekt allerede er hektet på kanaler for flyt av personlig informasjon seg imellom. Det er imidlertid ansett som problematisk å knytte en person opp til en kanal for overføring av personlig informasjon, d.v.s. tvinge ham inn i en lege-pasient relasjon, uten hans samtykke. Problemer oppstår derfor i de – riktignok få – tilfeller der den pasienten som legen har til behandling ikke er villig til eller ikke i stand til å informere sine slektninger. I disse tilfellene står personvern hensynene i veien for at personer blir informert om sin risiko for alvorlig sykdom.

Poenget i forhold til diskusjonen av allmenmoraliske normer for behandling av personopplysninger, er at et krav om samtykke ikke hjelper oss til å avgjøre hva som er riktig å gjøre. Problemet er at det er umulig å be om folks samtykke til å bli informert om at de har en risiko for å være bærere av det defekt gen, uten samtidig å informere dem om at de har det. Dette blir en form for *paternalistisk dilemma*, der noen andre må avgjøre hva som er verst for deg: å bli forstyrret med informasjon om økt sjans for risiko, eller å ikke vite å få informasjon om at du bør la deg teste. Dette er et personvernproblem der appell til individuelt samtykke ikke hjelper oss, rett og slett fordi slikt samtykke ikke er tilgjengelig. Samtykkemodellen kommer til kort, og våre intuisjoner blir mer usikre.

Vi må da finne noe annet å gå på for å avgjøre hva som er riktig. Dette gir svakere holdepunkter for en avgjørelse enn når vi kan anvende samtykkemodellen. Blant annet viser en undersøkelse at 77% av de spurte ville ønsket å bli oppsøkt av en lege med informasjon, dersom de var i en slekt med arvelig forhøyet kolesterol. De fleste

av oss viker litt tilbake for å avgjøre moralske spørsmål ved hjelp av flertall-savgjørelser og surveyundersøkelser. Et slikt resultat må imidlertid bli tungtveiende dersom vi ikke har noe annet å gå på. Det må tilføyes at det i dette tilfellet også er andre vurderinger som er relevante. For eksempel er det sterke prioriteringsgrunner som taler mot slik virksomhet. Poenget med eksemplet er imidlertid her bare å vise betydningen, og begrensningen, av samtykkemodellen i våre moralske vurderinger. Når det dukker opp personvernspørsmål som ikke kan løses ved å kreve samtykke til overføringen av personlig informasjon, blir grunnlaget for den etiske vurderingen mye mer usikkert.