Journalists and Data Protection
European Directive 95/46/EC

1. The Directive in context
2. The Directive, the Data Protection Act and the scope for 'journalistic' exemptions
3. Journalism and data protection
4. How to complain to the Data Protection Registrar

1. The Directive in context

The 'Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', to give it its full title, is one of many designed to create [Preamble, Recital 1]: 'an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its people, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognised in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.'

Pointing out [Recital 2] that 'data-processing systems are designed to serve man' (sic), and that [Recital 3] 'the establishment and functioning of an internal market, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services, and capital is ensured require only that personal data should be able to flow freely from one member state to another, but also that the fundamental rights of individuals should be safeguarded.'

The Directive goes on to note that the development of an internal market, 'will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in economic and social activity' [Recital 5], and that, 'the increase in scientific and technical co-operation and the co-ordinated introduction of telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data' [Recital 6].

Acknowledging that differences exist in the laws of Member States governing data protection, some of which might hinder legitimate cross-border exchanges of information [Recitals 7-10], the Preamble asserts that the purpose of the Directive is to harmonise laws while ensuring that 'a high level of protection' is afforded to individuals living within the European Community.

The relevant domestic legislation which will require amendment if Britain is to conform with the Directive is the Data Protection Act 1984 (DPA 84).

The Directive covers the processing of data, 'only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question' [Recital 15]. It excludes data held for purely personal and domestic activities like family correspondence and address lists [Recital 12].

The Directive asserts that data, 'capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent', but Recital 33 also acknowledges exceptions to this rule, 'for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities of certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms'.

The Directive requires that, 'any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the

lawfulness of the processing', and 'must also have the right to know the logic involved in the automatic processing of data concerning him'.

The same Recital 41 also insists, 'this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software'; and 'such considerations must not, however, result in the data subject being refused all information'.

Domestic laws concerning public safety, defence, state security and criminality fall outside the scope of Community law, and the Directive allows [Recital 17] that its provisions can only apply 'in a restricted manner' to, 'the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression'.

Such exemptions [Recital 37] should only be granted, however, 'in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental freedoms', and should not put the security of processing at risk.'

Significantly Recital 37 also requires that, 'the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to judicial authorities.'

In Britain at present the supervisory authority is the Data Protection Registrar.

Member States have three years from October 1995 [Recital 69] in which to harmonise domestic legislation on data protection, and a further 12 years in which 'to ensure the conformity of existing manual files', but the Directive stresses that data held in manual files which are processed during this extension period must be processed in accordance with the new regulations.

In March 1996 the Liquor, Gambling & Data Protection Unit of the Home Office issued a Consultation Paper and requested views on the ways in which the Directive should be implemented in the United Kingdom. Responses had to be submitted by 19 July 1996.

The Consultation Paper makes it clear that 'the Government intends to go no further in implementing the Directive than is absolutely necessary to satisfy the UK's obligations in European law'.

2. The Directive, the Data Protection Act and the scope for 'journalistic' exemptions
The Directive contains seven Chapters with a total of 34 Articles.

Chapter I: General Provisions outlines the Directive's scope and objects, defines terms, and the domestic laws to which it applies. The British Government has indicated that it intends to limit the scope of the new law to living individuals.

Article 3 specifically excludes individuals who process data 'in the course of purely personal or household activity', which covers such innocent activities as keeping address books or filing straightforward information about friends and relatives on a domestic word processor.

Chapter II: General Rules on the Lawfulness of the Processing of Personal Data stipulates the terms and condition under which personal data can be collected and processed.

Article 6 insists that data should be processed fairly and accurately, for explicit and legitimate purposes, and that the data should be accurate, up-to-date, and kept for no longer than is necessary.

Member States are required to determine the basis upon which such data may be 'stored for historical, statistical or scientific use' and to ensure that adequate, but undefined, safeguards are in place to protect the individuals from breaches of this Article.

Article 7 asserts that the person about whom data is processed must have 'unambiguously given his consent'; and that processing of the data must relate to a contract into which the subject has entered with the processor, or to other legitimate purposes including ' the performance of a task carried out in the public interest or in the exercise of official authority'.

However, and most significantly, the fundamental rights and freedoms of the individual concerned over-ride even the legitimate interests of the people holding, processing or receiving such data.

Article 8 prohibits [para 1] 'the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life' unless 'the data subject has given his explicit consent' or certain other carefully defined circumstances apply.

There are similar strictures about the processing of medical records [para 3] and information about criminal convictions [para 5]; and 'a complete register of criminal convictions may be kept only under the control of official authority'.

Article 9 provides for exemptions to the Directive in the interests of freedom of expression, making it clear that such exemptions shall apply to, 'the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right of privacy with the rules governing freedom of expression'.

Article 11 requires the holders of personal details 'which have not been obtained from the data subject' to ensure that the person concerned is informed of who is holding what information about her or him and for what purposes, and to advise the data subjects of their right of access to that information and the right to rectify any inaccuracies.

Article 12 specifies that data subjects must have the right to check, correct, erase or block data held about them 'at reasonable intervals and without excessive delay or expense'; and Article 14 provides individuals with the right to object to the processing of personal information about them, and to the release of that information to third parties for the purposes of direct marketing.

Article 13 allows Member States 'to restrict the scope of the obligations and rights provided for' by certain key articles, 'when such a restriction constitutes a necessary measure to safeguard...

(among other things)...the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions' [para 1(d)], and 'the protection of the data subject or of the rights and freedoms of others' [para 1(g)].

Except in certain circumstances the holders of data are expected to notify official national supervisory bodies before processing data, to register security measures to protect the data held and to appoint in-house data protection officials [Art. 18], and to register any relevant changes to the notifiable information [Art. 19].

The British Government has indicated that, within the scope of exemptions offered by the Directive, it intends to lift what it regards as 'unnecessarily burdensome' registration requirements under the DPA 84.

Chapter III: Judicial Remedies, Liability and Sanctions insists that individuals should have the right to seek a legal remedy [Article 22], including compensation [Article 23], for any breaches of the rights guaranteed by domestic legislation in respect of the processing of personal data.

Under the DPA 84 individuals may complain to the Data Protection Registrar about suspected breaches of the regulations, and the Registrar has powers to investigate and issue notices if breaches are proven. Failure to comply with the requirements of the DPA 84 or such notices is already a criminal offence. Appeals can be made to the Data Protection Tribunal, and further appeals on points of law about a Tribunal ruling may be made to the courts.

Individuals may also seek legal redress where access to data has been refused, to ensure that inaccurate date is corrected or erased, and to obtain compensation for damage or distress caused by inaccuracy, loss, or unauthorised destruction or disclosure of personal data.

Chapter IV: Transfer of Personal Data to Third Countries explains that it is the obligation of each Member State to check whether adequate safeguards exist in third countries to which personal data may be passed to protect the rights of the individuals to whom such data refers [Article 25].

The holders of data are expected to check with the relevant authorities before divulging information to third countries. The British Government does not favour this 'prior authorisation by the supervisory authority' and would prefer that such decisions to be taken ad hoc by in-house data supervisors.

Chapter V: Codes of Conduct requires Member States and the European Commission to encourage [Article 27] the drawing up of Codes of Conduct about the holding and processing of personal information. They may be submitted for observation to an EC Working Party on the Protection of Individuals with regard to the Processing of Personal Data [Chapter VI, Article 29], which will operate in an advisory capacity, independent of the European Parliament and the European Commission.

Trade associations and other bodies representing those who deal with data processing are expected to submit to the national authority any relevant codes they have devised.
Chapter VI: Supervisory Authority and Working Party on the Protection of Individuals with regard to the Processing of Personal Data requires each Member State to ensure that at least one public authority is responsible for monitoring the application of the measures outlined in the Directive [Article 28].

In the United Kingdom this function is currently carried out by the Data Protection Registrar and the Data Protection Tribunal, although the administrative arrangements are currently under review in consequence of the Deregulation and Contracting Out Act 1994.

Chapter VI: Community Implementing Measures spells out the procedures and timetable for implementation of the Directive by Member States.

Much of the Directive is already covered by the provisions of the DPA 84, although the Directive extends regulations to include some 'manually processed' as well most 'automatically processed data', and there are other significant differences.

The Directive, for instance, includes the collection and destruction of data within the term 'processing'; it defines tighter conditions under which data may be processed; allows certain exemption for journalists; and it also confers upon the individual the right to object to the lawful processing of data and the use of data for direct marketing schemes.

Generally speaking the Directive tightens up the existing regulations that apply in Britain and is more forthright in asserting the rights of the individual. Its provisions must accord with the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which has yet to be fully incorporated into British law but to which the British Government is a signatory.

3. Journalism and data protection

Protection of sources

One of the abiding principles of journalism is the protection of sources. There have been repeated examples of powerful individuals and companies and the British courts seeking to persuade journalists to divulge the sources of 'sensitive' information. When journalists comply, as in the case of Peter Preston, then Editor of *The Guardian* and Sarah Tisdall, there is an outcry which extends beyond the industry. Politicians rely upon the principle when briefing lobby journalists, and the public certainly appreciate the importance of this confidentiality code.

The principle is acknowledged in Clause 7 of the 60-year-old Code of Conduct promoted by the National Union of Journalists, and in Clause 17 of the industry's own more recent Code of Practice currently supervised by the Press Complaints Commission. The principle was upheld by the European Court of Human Rights early in 1996, when Bill Goodwin won backing for his refusal to reveal the source of information obtained for an (unpublished) story he was researching as a reporter with The Engineer.

The Directive is not primarily concerned with this issue, but it would certainly be invoked if members of the public were to be granted unrestricted access to files and databases maintained by journalists in the course of their duties. For that reason alone it is important that there should be some exemptions from the regulations governing the collection and processing of data for journalistic purposes.

Accuracy

However, there are other issues at stake. There is always the possibility that information gathered about individuals from third parties may be inaccurate, or biased. Reliance upon third party sources is no defence if the material published is damaging or wrong.

The Directive is designed to achieve Europe-wide compliance with arrangements to ensure that individuals are protected from the dissemination of inaccurate information about them, for whatever purpose.

As a matter of natural justice, individuals who are under scrutiny should have the right to check the accuracy of material being compiled for use about them.

PressWise is emphatically not suggesting that everyone should be afforded the right to 'prior restraint', although regrettably those with sufficient financial resources have often used 'gagging writs' to prevent legitimate journalistic activity simply because they are displeased at the prospect of their affairs being scrutinised in public.

Exemptions for journalists

In its efforts to establish a balance between the individual's right to privacy [ECHR Article 8] and freedom of expression [ECHR Article 10], which in both instances includes freedom from interference by a public authority, the Directive [Article 9] has acknowledged that journalists should be exempted in part from data protection regulations, and Member States are obliged to make such exemptions.

One potential problem that arises from this provision is the matter of definition. Currently everyone is covered by the DPA 84 regardless of their profession; there is no exemption for journalists. The Directive does not allow for a blanket exemption, and the term 'journalistic purposes' is unclear. Journalistic activity cover a very wide range of tasks, from research, writing and broadcasting to public relations work, editing, sub-editing and other functions within the book and electronic publishing field.

Furthermore, an increasing number of journalists are now freelances, not tied by contract to a specific employer, so it is impossible to define 'journalistic purposes' in terms of engagement to a specific print or broadcast company.

The problem of definition and registration
If the exemption were to apply to all journalists in pursuit of their chosen trade, this might require formal registration of those to whom the exemption would apply, and the activities covered by it. That would be a retrograde step, since one of the principles of freedom of expression is that any person should be able to write and speak without constraint, so long as they operate within the laws of the land.

There has been fierce resistance in Britain, and elsewhere, to the notion of licensing journalists, whether by requiring them to be members of a specific trade union or professional body or to carry an identity card issued by a police authority. Currently anyone may become a journalist, and accommodations have been reached between editors, trades unions and police authorities about the acceptability of appropriate forms of identification.

It may be inimical to offer a definition of 'journalistic' activity, but any such attempt would need to cover all those who earn all or a substantial part of their living from collecting and/or processing information and images for publication or transmission whether by print, audio or visual broadcast, or other forms of electronic communication. This catch-all definition would include those engaged in artistic or literary expression who are eligible for exemption, and possibly many others who are not. The problem remains about how to limit or specify the circumstances under which exemption can be claimed.

However the issue of definition is resolved, the matter of exemption gives rise to further problems about what data processing items might be covered. It could be argued that journalists' contact books, and computerised or manual notebooks fall well within the Directive's definition of data as set out in Article 2 (a), (b), & (c), as do research materials and files held at home or in an office in particular by specialist and investigative journalists.

It may seem to be quite proper for these items to be exempted from the provisions detailed in Articles 5-21, 25 & 26 and 28-30, as the Directive allows, but these Articles also refer, for example, to the right of individuals to check that information held about them is correct and up-to-date.

It is entirely inappropriate for journalists to disseminate inaccurate information. Exemption might be regarded by the individuals about whom such information is held, processed or published, as a denial of the very individual rights and freedoms which the Directive is designed to protect.

The business of newspaper publishers and broadcasting companies includes but does not exclusively involve 'journalistic activity'. Nonetheless they lay claim to ownership (copyright) of the material collected and disseminated by their agents (journalists), and seek authority to exploit such material for commercial purposes. Much of that material concerns data collected, albeit legitimately, about individuals whose right to privacy is afforded greater protection under ECHR, Article 10, than any existing domestic laws in Britain.

All newspaper keep 'cuttings libraries', often filed by name or topic for ease of retrieval, and most newspapers, for instance, now own or contribute to electronic databanks containing published material which are networked throughout the world including via the Internet. It is a means of exploiting the commercial potential of the journalistic products of their staff, freelancers and contributing new agencies.

Some newspaper and publishing companies are international corporations operating beyond the scope of European Community law, which raises further questions about the extent to which exemption should be awarded to them.

The complex regulations that apply to intellectual property and copyright in an age of trans-global electronic communications may be germane to some of the issues covered by the Directive.

Ensuring correction of published errors
One major issue which the Directive could help to resolve is the matter of correcting inaccurate material published by a newspaper, magazine or broadcast programme, and in particular the correction of manually or electronically held databanks of material previously published in a newspaper.

A not infrequent complaint of aggrieved individuals is that even after a correction has been published following the dissemination of inaccurate information about them, no system exists to ensure that cutting files or databanks are similarly corrected. Inevitably the inaccurate information resurfaces when journalists rely upon the uncorrected cuttings libraries or databanks. This can cause distress and has even been known to result in newspapers having to pay substantial damages for 'innocently' repeated libels or malicious falsehoods.

In implementing the Directive the British Government should take steps to ensure that, whatever exemptions are granted for 'journalistic purposes', the owners of cuttings libraries and databanks should be required to 'tag' all material which has been demonstrated to be inaccurate, or the veracity of which has been challenged. Responsibility for tagging such material should rest with the in-house supervisor of data protection.

If data collected for journalistic purposes is to be exempted in its pre-publication form, exemptions that might prevent persons mentioned in the material from having access to cuttings files of databanks for the purposes of correcting inaccurate information should be qualified.

In other words exemptions should only apply to data held for the purpose of publication prior to publication. Once that has entered the public domain, the individuals concerned should have the right to correct inaccuracies. In certain circumstances there may be a case for allowing that person the right to ensure that related but unpublished information is checked for accuracy.

Non-journalistic data held by publishers
However the matter of exemption is resolved, a clear distinction must be made between information garnered by journalists for journalistic purposes and that which is gathered by newspaper/magazine or broadcasting/production companies for marketing or promotional purposes. There should be no exemption for data processing in the non-journalistic aspects of the company's business.

Within the companies there should be a clear differentiation made between the storage and supervision of and access to these separate types of data collection and processing. It would be appropriate for separate and distinct in-house data protection supervisors to be made responsible for these different categories of data.

Material gathered for one purpose should not be used for the other, and respondees to advertisements, box numbers, competitions (other than winners) or promotional vouchers should be assured that any information they supply will be subject to the full provisions of the Directive and the amended DPA 84 as they affect more conventional forms of data processing.

Redress and regulation
The issue of redress falls within Article 23, from which there are no opportunities for exemption. It requires Member States to ensure that anyone suffering damage as a result of 'unlawful processing', and the holding or processing of inaccurate material, may obtain compensation. The in-house supervisor of data processing may avoid liability if it can be shown that s/he 'is not responsible for the event giving rise to the damage'.

Some clarification of this is required since it may lead to demands that the person responsible for editorial decisions should be held liable in the event of the publication of inaccurate information previously held in a form covered by the Directive or the DPA 84.

While aggrieved parties may favour such a sanction against an Editor, it is unlikely that the Editor will have been responsible in the first instance for checking the veracity of information held in databanks compiled by researchers, librarians or other journalists and which might anyway have been covered by exemptions.

Print and broadcast publishers are reluctant to pay compensation to aggrieved parties unless obliged to do so by the courts, in defamation cases for instance. However, if it is right that compensation should be available to a person who suffers damage as a result of the processing of inaccurate information in other commercial operations, it is entirely appropriate that a person about whom inaccurate information has been published to much wider audiences should also be compensated. Quite apart from any harm done to reputation and relationships, especially for those who cannot afford to sue for libel, the process of obtaining corrections and apologies can be both time-consuming and expensive.

One further vexed question remains about enforcement issues dealt with in Articles 22-24, 27 & 28 and covered in the main by the exemptions offered in Article 9. The Directive makes it clear that these exemptions should not absolve journalistic, artistic or literary activity from 'measures to ensure security of processing' [Recital 37] or 'certain ex-post powers' (see paras 2.08 7 2.09 above).

This has given rise to fears that the Data Protection Registrar may become a Privacy Commissioner 'by the back door', and begs the question about which is the appropriate national authority to whom companies or individuals who hold and process journalistic should in the end be accountable.

At present the Data Protection Registrar is the most obvious public supervisory authority in the field. However, if there are to be special exemptions for journalistic activity in order to balance the sometimes conflicting demands of freedom of expression and the right to privacy, s/he may not be the most appropriate authority to whom complainants should appeal or journalists report.

Since the Press Complaints Commission currently has no statutory powers, and is entirely funded by the newspaper & magazine publishing, it cannot be regarded as an independent public supervisory authority. Nonetheless it does have a responsibility for ensuring that printed publications comply with a Code of Practice which covers accuracy and privacy.

The Broadcasting Standards Commission, which is poised to take over the roles of the Broadcasting Complaints Commission and the Broadcasting Standards Council in 1997, does have statutory powers and can legitimately claim public status and an independence from the industry it regulates.

The convergence of new communications technologies and increased cross-media ownership are strong arguments for a single, independent regulatory authority covering the print and broadcast media, established on a statutory footing. This would be an ideal vehicle for the monitoring of data processing within both industries.

Of course, were the European Convention for the Protection of Human Rights and Fundamental Freedoms to be fully incorporated into British law, individuals would have access to legal redress were either of their rights to privacy or to freedom of expression put at risk by the actions of journalists, the companies that employ them, or public authorities. And both parties to the dispute would have equal access to the law to establish the balance between these rights which the Directive and its exemptions are designed to protect.

How to complain to the Data Protection Registrar
If the Press Complaints Commission won't help, perhaps the data protection registrar can - a case study.

Obtaining redress when newspapers or other forms of the media get things wrong is not easy. Libel actions are frequently ruled out for reasons of expense, the Press Complaints Commission is a weak reed with the odds loaded against the complainant, and even the statutory regulators of radio and television provide little remedy except in extreme cases.

Just as worrying is the fact that inaccurate or defamatory information can remain on computer files for years, ready to be unearthed and repeated by the next reporter assigned to an associated story. In such cases, however, something can be done. A PressWise client, Robert Henderson, has established a useful precedent by using the Data Protection Act to ensure that articles relating to him on media computer files are "tagged" to record the fact that he has challenged their contents. Those who seek to use the files in future have therefore been given fair warning that there may be trouble in store.

We record below Mr Henderson's guide to the required procedure for complaining to the Data Protection Registrar, based on his personal experience.

The origin of the complaint
In 1995 Mr Henderson contributed an article, which he had entitled "Racism and national identity", to *Wisden Cricket Monthly*. It was published in the July edition under the headline "Is it in the blood?"

In it he commented on racism in other Test-playing countries and what he considered to be the deleterious effect on the England cricket eleven of selecting large numbers of immigrants - white, black and Asian - for the team. Such immigrants, he claimed, could not in the nature of things be driven by patriotism.

There was an immediate outcry in the national press, attacking Mr Henderson and his ideas. [Indeed, PressWise would like to make it clear that by publishing the results of his efforts to obtain redress, we do not endorse the views expressed in that article]

A libel case was brought against the publisher and substantial damages were awarded to some of the sportsmen implicated in the article.

Meanwhile Mr Henderson had sought and was refused, a right of reply to published comments about his article. A complaint to the Press Complaints Commission proved equally fruitless.

However, he is a persistent man. He complained to his MP, Frank Dobson, that he had been denied natural justice. Dissatisfied with Mr Dobson's (lack of) response, Mr Henderson wrote first to Tony Blair, then in opposition, and subsequently to his wife Cherie Blair. Just before the last election the Blairs complained to the police about his letters. The next thing Mr Henderson knew *Mirror* reporters were at his door, and a sensational article and photograph appeared accusing him of harassing the Blairs, describing him as a racist and potential stalker and containing a claim from a police source that we has guilty of a crime for which he had not and still has not been charged.

The inaccuracies of the article convinced Mr Henderson that the *Mirror* had not seen the letters complained about, and once again he sought redress from the PCC. They were equally unsympathetic and refused to consider his complaint after a lengthy correspondence.

Undeterred Mr Henderson turned to the Data Protection Act to obtain information held in police records about Blairs' complaint, to ascertain that the cropped photograph of him used by the *Mirror* had been cropped to obscure the fact that it had been taken while he was inside his home, and to try and correct the errors in the offending story.

Because all national newspapers now hold their entire contents on free-text databases, he set about establishing the principle that they fell within the scope of the 1984 Data Protection Act. That principle was finally acknowledged by the Data Protection Registrar in July 1999, and the two newspapers chosen by Mr Henderson as his targets for articles they published about him in 1997 - the *Mirror* and the *Daily Record* - have been forced to put messages on their databases showing that he has challenged the data.

This is Mr Henderson's guide to using the Data Protection Act:

1. Some important facts about the DPA:

a) Definitions

A person or organisation holding qualifying data is known as the DATA USER.

A person seeking knowledge of the data held by a DATA USER is known as the DATA SUBJECT. Only individuals can be DATA SUBJECTS.

b) What qualifies as data covered by the DPA?

In principle, any data held by a person or organisation in a form in which it can be automatically processed falls within the DPA. In practice, this normally means data held on computer, most commonly in a database or spreadsheet.

Exceptions to the general provisions of the DPA exist. The most important are for data that is held for word-processing purposes only and various exemptions where legal or security considerations arise. However, none of these have relevance where you are challenging a newspaper story held on a free-text database.

c) Accuracy

Statements of opinion cannot be challenged on the grounds of accuracy. Statements of fact can.

Even with factual inaccuracies, the position is modified in the case of THIRD PARTY STATEMENTS. Provided the DATA USER makes it clear within the data they hold that a statement about a DATA SUBJECT is (1) a third party statement and (2) places any objections to the statement on the computer in a manner which allows the objections to be seen every time the data is accessed, the DATA USER has met their obligations under the DPA. It does not, however, affect their liability to libel suits.

2. How to obtain data

You must make what is known as a SUBJECT ACCESS REQUEST. To assist you in this I have drafted the following standard letter:

"Under section 21 of the 1984 Data Protection Act, I formally request details of any data qualifying under the act held by the [insert name of individual, group, company or institution from whom data is sought] which contain information relating to me. If you do not hold any qualifying data, the act requires that you advise me of this in writing.

You may have a form which you send to those making a Subject Access Request. The Office of the Data Protection Registrar assures me that such forms have no legal status. Therefore, I insist that you act upon this letter. If there is additional relevant (See DPA Guidelines) information you require, please put your questions in a letter.

My request covers all computer hard and soft disks, the Internet, the Web and any other electronic method of recording computer generated files such as tape and CD, together with any non computer recorded and/or generated data - for example, data held on a Document Image Processing System - which can be the subject of the automatic processing of data.

The data need not be directly held by you or the corporate body of which you are a part. It is enough for you or the corporate body to control the content of the record and/or the use of the data. Thus any qualifying data held by a third party, such as a computer bureau, comes within the scope of the act. You must provide me with print outs of data held by a third party if the data falls within the act.

The act allows you forty days in which to comply with my request. You are legally obliged to reply to this letter and legally obliged to give the information sought in paragraph 1.

Deleting data after receipt of this letter will not absolve you from your obligation to provide me with details of the deleted files. Indeed, such action would constitute an offence if it is done for the purpose of denying me information about data held by you at the time of my request."

If you have not received a reply within 50 days (give them slightly longer than the legal requirement to show that you are reasonable) make a complaint to the DATA PROTECTION REGISTRAR. This merely requires a copy of the SUBJECT ACCESS letter you have sent and a short note to the DPR stating that the DATA USER is substantially past the statutory period of 40 days.

3. Challenging Data

The DPA is based on eight DATA PROTECTION PRINCIPLES. These are:

THE FIRST PRINCIPLE

'The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.'

THE SECOND PRINCIPLE

'Personal data shall be held only for one or more specified and lawful purposes.'

THE THIRD PRINCIPLE

‘Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.'

THE FOURTH PRINCIPLE

'Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes '

THE FIFTH PRINCIPLE

'Personal data shall be accurate and, where necessary, kept up to date.'

THE SIXTH PRINCIPLE

'Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

THE SEVENTH PRINCIPLE

'An individual shall be entitled
(a) at reasonable intervals and without undue delay or expense -
    (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
    (ii) to access any such data held by a data user; and
(b) where appropriate, to have such data corrected or erased.'

THE EIGHTH PRINCIPLE

'Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.'

The most useful PRINCIPLES for your purposes are 1, 5 and 7.

PRINCIPLE 1 can often be relevant because the media frequently receive information illegally, for example from the police. Any civil servant and many other public servants such as the police will have signed the Official Secrets Act. If they give information to a newspaper without official authorisation, they have committed a criminal offence. So, interestingly, has the recipient of the information, regardless of whether he or she has signed the Official Secrets Act. Any public servant, whether they have signed the Official Secrets Act or not will be in breach of laws protecting confidentiality, and most probably in breach of the disciplinary code of the organisation for which they work, if they provide information to third parties without proper authorisation.

PRINCIPLES 5 and 7 are your main weapons, particularly 5. They allow you to:
1. challenge the accuracy of stories held on the newspapers' databases,
2. request their amendment or removal, and
3. request the placing of your objections on the computer in a way which allows then to be seen whenever the data is accessed.

When you are making a challenge to data, always cite the PRINCIPLE(S) which have been breached.

I suggest that you allow FOUR WEEKS for the DATA USER to reply to your requests for amendments, deletions and notes to be made and/or placed on the offending data.

If the DATA USER fails to reply within FOUR WEEKS, make a complaint to the DPR. If you receive a reply from the DATA USER which is unsatisfactory, make a complaint immediately to the DPR. My extensive experience in dealing with newspapers leads me to the conclusion that they will invariably try to brazen things out. Sending more than one letter on any subject is a waste of time. Therefore, you will expedite matters best by placing your complaints in the hands of the DPR as soon as you reasonably may.

Send all your letters to the DATA USERS and to the DPR by recorded delivery. This will cut off one of the principle excuses for delay, namely that post has not been received.

Your letters to the DATA PROTECTION REGISTRAR should be addressed as follows:

Mrs Elizabeth France
The Data Protection Registrar
The Office of the Data Protection Registrar
Wycliffe House
Water Lane
Wilmslow

Cheshire SK9 5AF

The Office of the DPR can also be contacted by:
Tel: 01625/545700
Fax: 01625/524510
E-mail: data@wycliffe.demon.co.uk

The DPR publishes extensive "Guidelines". These are essentially the DPA in non-lawyer form. A copy may be obtained free of charge on request from the Office of the DPR. The latest set of Guidelines was issued in Sept 1997.

Latest information
The 1998 Data Protection Act (DPA)

From 24/10/01 those who hold data about you will have to supply in most circumstances not merely data held electronically but also most manual data. the old "word processing" exemption is no more and manual data filed in only the most casual way, for example in a file marked with your name, will qualify.

The Data Protection Registrar is now called the Information Commissioner. The post is currently held by Elizabeth France. She now has responsibility not only for the DPA, but also the Freedom of Information Act. She can be contacted at:

The office of the Information Commissioner
Wycliffe House
Water lane
Wilmslow
Cheshire SK9 5AF

Tel: 01625-545700

E-mail - data@wycliffe.demon.co.uk

NB E-mails may not be answered for two or three weeks.

Example letter for subject access request
Under section 7 of the 1998 Data Protection Act, I formally request details of any data qualifying under the Act held by [insert name of person or institution to whom the subject access request is directed] which contain information relating to me. If wish to claim that you do not hold any qualifying data, the Act requires that you advise me of this in writing.

You may have a form which you send to those making a Subject Access Request. The Office of the Information Commissioner assures me that such forms have no legal status. Therefore, I insist that you act upon this letter. If there is additional relevant (See DPA 1998 Guidelines) information you require, please put your questions in a letter ASAP.

My request covers all computer hard and soft disks, the Internet, the Web and any other electronic method of recording computer generated files such as tape and CD, together with any non computer recorded and/or generated data - for example, data held on a Document Image Processing System - which can be the subject of the automatic processing of data.

The 1998 Act has greatly broadened the range of data which qualifies. The so-called "word-processing" exemption no longer exists and thus virtually any text data held on a computer potentially qualifies. The other great general change is the fact that data now qualifies where the data subject can be identified by details other than their name.

The Act also provides for manual data to be supplied. The manual data which qualifies is very wide ranging. For example, if data is kept in a file marked with a person's name in an office desk, that would count as a qualifying manual filing system.

The first transitional exemption period from the provisions of the Act ended on the 24 October 2001. The exemptions provided for automated data are now completely removed and those applying to manual data only during the second transitional exemption period are greatly reduced from those available before 24/10/01. Please ensure that you understand the provisions of the second transitional period before replying to this subject access request.

The data need not be directly held by you or the corporate body of which you are a part. It is enough for you or the corporate body to control the content of the record and/or the use of the data. Thus any qualifying data held by a third party on your behalf comes within the scope of the Act. You must provide me with print outs of data held by a third party if the data falls within the act.

The act allows you forty days in which to comply with my request. You are legally obliged to reply to this letter and legally obliged to give the information sought.

Deleting data after receipt of this letter will not absolve you from your obligation to provide me with details of the deleted files. Indeed, such action would constitute an offence if it is done for the purpose of denying me information about data held by you at the time of my request.

I enclose a cheque for £10. This is the maximum which can be charged for a subject access request.

Robert Henderson
philip@anywhere.demon.co.uk