Introduction to data protection

Max Todd, Assistant Registrar
Compliance, Council Secretariat

Tuesday 18 November 2014

AIMS

Overview of DPA: *8 Data Protection principles*

Security: *What level of security is required and what happens if there is a security breach?*

Marketing: *Rules on electronic marketing*

Changes to EU DP law: *What lies round the corner?*

DATA PROTECTION ACT

- ***Purpose***: To allow organisations to use personal data (PD) for legitimate purposes, whilst protecting the rights of individuals, particularly their right to privacy
- Provides a ***framework*** rather than detailed rules
- Organisations must handle PD in accordance with 8 '***data protection principles***'

Scope of DPA

Personal data: Data that relates to a living individual, who can be identified from that data, on its own or in combination with other data, e.g. email address, student number, job title

Processing: Anything you do with PD - collecting, holding, using, disclosing etc

Sensitive personal data: Data relating to health, race / ethnicity, religious / political beliefs, trade union membership, sexual life, criminal record

Data controller: Organisation that determines purposes for which PD is processed and that is responsible for complying with DPA, i.e. the University

Principle 1 – Fair and Lawful Processing

People need to be aware you are holding PD on them and what you are using it for

When collecting PD, provide a ***Privacy notice***, indicating***:***

- Who is processing the data?
- What will be done with the data?
- Any other information needed for processing to be fair, e.g. disclosures to 3rd parties

Principle 1– Satisfy a processing condition

- Processing has ***consent*** of data subject
- Processing is necessary to fulfil a ***contract*** with data subject, *e.g. student or staff contract*
- Processing is necessary to meet other legal obligation, *e.g. salary data to HMRC, ethnic data to HESA*
- Processing is necessary to meet your legitimate interests (or those of a 3rd party), balanced against rights and interests of individual

Principle 2 – Purpose Limitation

- Personal data shall be processed only for specified purposes and not used in a way ***incompatible*** with those purposes
- Data can be used for a new or different purpose, if it is one that people would ***reasonably expect***
- Otherwise, you will need ***consent***

University privacy notices

Students: '..*perform its educational, pastoral, statutory and administrative purposes'*

Staff: '..*comply with its contractual, statutory, and management obligations and responsibilities'*

Alumni: *'..use data for a full range of communications and marketing activities with you (by mail, email, telephone, fax or text message)'*

Principles 3-5: Data standards

3rd principle – PD must be adequate, relevant and not excessive in relation to purposes of processing

4th principle – PD must be accurate and, where necessary, kept up to date

5th principle – PD must not be kept for longer than is necessary for purposes of processing

Principle 6: Rights of individuals

- Right of ***subject access*** i.e. right to access one's PD
  - Applies to data held in any form
  - Cannot exclude data just because it is difficult to locate
  - Limited exemptions from disclosure, e.g. 3rd party rights
  - Everything is potentially disclosable
  - Centrally processed – refer requests to data protection team
- Right to object to ***direct marketing***
  - No exemptions, no discretion
  - Must comply within reasonable period, e.g. 28 days for electronic marketing

Principle 7 – Security

- Must take ***appropriate*** technical and organisational measures
- '***Appropriate***' means proportionate to:
  - potential harm to the individual, e.g. distress or financial loss from identity theft
  - state of technological development
  - resources of the data controller
- ***Assess the risk case by case***: at all levels and at all times, from protecting the network to sending an email or storing hard copy records

Security breaches - enforcement by Information Commissioner's Office (ICO)

- Security is biggest area of risk - 90% of enforcement action
- ICO will act if breach has ***potential*** to cause significant harm
- Enforcement options
  - Undertaking
  - Enforcement notice
  - Monetary penalty notice – fine of up to £0.5m
- Reputational damage - ICO names and shames

How do security breaches happen?

- **External attack**
- **Individual carelessness**
  - Sending confidential data to the wrong email address, fax number or postal address
  - Loss or theft of unencrypted mobile devices, e.g. laptops, tablets, smartphones
  - Loss or theft of hard-copy records

Protecting personal data

- Encryption of mobile devices: laptops, tablets, smart phones, memory sticks
- ICO requires encryption where loss of data could cause distress or financial loss
- Consider alternatives to email – Sharepoint, Weblearn, OxFile

Sharing PD with service providers

When sharing data with 3rd party service-providers ('data processors' under DPA), e.g. mailing house etc:

- Must have written contract defining what processor can and cannot do with PD so that they handle data only in accordance with your instructions
- Processor must take same security measures you would need to take if you were processing the data yourself
- Any breach by processor will be your responsibility. Legal responsibility is with data controller, not data processor.

Principle 8 – Overseas transfers

- Personal data shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for personal data
  - EU's 'White list' e.g. Canada, Argentina, Switzerland
  - Safe harbor scheme for US companies
  - Self-assessment of adequacy
  - Exemptions
    - Consent
    - Necessary for contract performance
    - Legal proceedings

Marketing (1)

- DPA applies if directed at particular individuals (but not organisations)
- Definition of marketing is not limited to commercial marketing, i.e. sale of goods or services
- Includes promotional material, including that produced by non-profit bodies

Marketing (2)

- Privacy and Electronic Communications Regulations (PECR) 2003 - rules for marketing by **electronic means** (email, sms, fax) or **telephone**
- Need prior ***consent*** for unsolicited marketing by email, fax, text or automated call, i.e. positive indication of agreement
- Consent not necessary for telephone marketing, but must not call anyone who has objected, including by registering with Telephone Preference Service (TPS)

FURTHER INFORMATION

DATA PROTECTION QUERIES

data.protection@admin.ox.ac.uk
max.todd@admin.ox.ac.uk, x80299

Website

www.admin.ox.ac.uk/dataprotection

UNIVERSITY OF OXFORD