Data Protection for Communication Officers 25 October 2016

Max Todd
Assistant Registrar, Compliance
Information Compliance Team, Council Secretariat

UNIVERSITY OF OXFORD

DATA PROTECTION ACT

Purpose: To allow organisations to use personal data, whilst protecting privacy

1. Requires organisations to comply with eight principles of good information handling (the '***data protection principles'***)

2. Grants people ***rights*** in relation to their personal data, including, most importantly, the right to access that information

COSTS OF NON-COMPLIANCE

- **Enforcement**: Information Commissioner's Office (ICO) can fine up to £500K or require changes in policies and procedures
- **Reputational damage** : ICO names and shames. Media publicity
- **Damage to relations** with donors, prospects, alumni, etc
  - Distress from exposure of private and confidential information
  - Risk of financial loss from identity fraud
  - Rising expectations of data privacy and security

KEY DEFINITIONS

Personal data (PD)– Data that relates to an identifiable individual e.g. email address, alumni number, opinions, intentions.

Sensitive personal data (SPD)– Data about health, race/ethnicity, religious/political beliefs, sexual life, criminal record, criminal allegations. Stricter requirements apply to SPD.

Processing – Any activity with data: collecting, storing, disclosing to 3rd parties, analysing, deleting, etc

Data controller – Responsible for complying with DPA i.e. OU or college

Data processor – 3rd party that processes PD on behalf of data controller e.g. mailing house, event organiser, venue staff

PRINCIPLE 1 – FAIR AND LAWFUL PROCESSING

- Must be ***transparent*** by providing a ***Privacy Notice:***
  - Identity of data controller: Who is processing the data?
  - Purposes of processing: How will you use their data?
  - Any other information needed for processing to be fair e.g. *any disclosures of PD to 3rd parties, any transfers overseas*
- Consider how processing affects interests of data subject
- Only process PD in ways they would ***reasonably expect***

UNIVERSITY PRIVACY NOTICES

Generic privacy notices

- Students: https://www.ox.ac.uk/students/life/it/studentrecord/data?wssl=1
- Staff: http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/staffinfo/
- Alumni/donors: https://www.alumniweb.ox.ac.uk/oao/dataprotection

Separate privacy notices will be necessary if processing:

- PD for non-standard uses not covered by above notices
- PD of other groups of data subjects e.g. research subjects

PRINCIPLE 1 – SATISFY A PROCESSING CONDITION

- Must meet a processing condition in Schedule 2 of Act
- If processing sensitive personal data, must additionally meet a processing condition in Schedule 3
- Purpose is to ensure there is a legitimate basis for processing personal data
- Only one condition relevant to marketing:
  - **Processing has the CONSENT of the individual– Explicit consent if SPD**

WHAT IS VALID CONSENT?

'..*any freely given, specific and informed indication of wishes by which the data subject signifies agreement to personal data being processed.....'*

- Individual must have a genuine choice: provision of service cannot be conditional on consent for processing if unnecessary for service
- Individual must know what they are consenting to
- Must be indicated by some positive action e.g. ticking a box
- Not opting out (e.g. not replying to an email) does not constitute consent

CHANGING CONSENT

- Consent can be withdrawn or varied
- Record and respect preferences expressed by data subject
- Otherwise processing will be unfair and in breach of first data principle

Privacy and Electronic Communications Regulations (PECR)

- Provides rules for unsolicited direct marketing by **electronic means** (email, text, fax) or **telephone**
- Need prior ***consent*** for unsolicited marketing by e-mail, text or fax i.e. positive indication of agreement
- Every marketing email or text must provide opt-out opportunity
- Telephone calls must not be made to a person registered with Telephone Preference Service (TPS) or who has otherwise objected. DPA still applies

PRINCIPLE 2 – PURPOSE LIMITATION

- Personal data shall be not be used in a way that is *incompatible* with original purposes

- Limits use of PD to purposes in *privacy notice/DP statement* unless the new or different purpose is what the individual would *reasonably expect*

- If new or different purpose falls outside reasonable expectations you must get *consent*

PRINCIPLES 3-5: DATA STANDARDS

3rd principle – PD must be adequate, relevant and not excessive in relation to purposes for which it is processed

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. Guidance on retention of student and staff data on DP webpages

PRINCIPLE 6 – RIGHTS OF INDIVIDUALS

- Right of *'subject access'* – right to receive a copy of information held about you
- Subject access seen as central to DPA. Few exemptions from disclosure. Must comply within 40 calendar days
- Assume everything you record about a person is disclosable – take care when recording information
- Right to *object to direct marketing* – No exceptions– Must comply with request: within 28 days for electronic marketing or two months for postal

PRINCIPLE 7 – SECURITY

- Must protect PD by taking '*appropriate technical and organisational measures*'
- What is '*appropriate*' depends on nature of data and potential for harm to individual from data breach
- Data processor must be subject to a contract with standard DP clauses
- Encrypt PD on memory sticks or laptops

UNIVERSITY OF OXFORD

PRINCIPLE 8 – OVERSEAS TRANSFERS

- *No transfers* outside EEA if inadequate data protection
- Relevant if using American cloud service providers e.g. DropBox, MailChimp, SurveyMonkey, Eventbrite
- 'Safe harbor scheme' replaced by 'EU-US Privacy Shield'
- If not covered by Privacy Shield, only two options:
  - Use of EU's 'model clauses'
  - Transfer has consent of individuals concerned
- See new guidance on DP webpages: www.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/

APPLICATION OF DATA PROTECTION PRINCIPLES

EXAMPLES

EXAMPLE 1 – SHARING OF PD

Mr Smith has accepted an invitation for a university event and rings you to ask whether his good friend, Mr Jones, will be attending. You know that Mr Jones has also accepted the invitation.

- Is it OK to tell Mr Smith that Mr Jones will be coming?
- Is it OK to give him Mr Jones' contact details?

EXAMPLE 2 – USE OF STAFF PD

You want to set up a departmental newsletter.

- Do you need consent to use staff email addresses for this purpose?

You want to organise a staff event using Eventbrite.

- What issues do you need to consider?

EXAMPLE 3 – SENSITIVE PERSONAL DATA

Replying to an event invitation, Mr Smith indicates that he uses a wheelchair and may need help accessing the venue

- Can you record that information?
- Can you share it with venue staff who are non-university?
- Can you retain it?

EXAMPLE 4 – USE AND RETENTION OF PD

Mr Smith tells you that he wishes to bring his husband to the dinner you are organising

- Can you record that information?
- Can you retain that information after the dinner?

EXAMPLE 5 – MARKETING

An electronic event invitation is sent to Mr Jones as a cold mailing, using an email address in the public domain. Mr Jones does not respond but as it is hoped he will attend future events, further invitations are planned.

- Was the initial approach permissible under DPA/PECR?
- Is it OK to send further invitations?

FURTHER INFORMATION

QUERIES

Data.protection@admin.ox.ac.uk

GUIDANCE:

https://www1.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/

UNIVERSITY OF OXFORD