

Data Protection Workshop

How the Law Affects You

Part 1: Legal overview

Peter Garrod

Data Management Officer

pg7@soas.ac.uk



Workshop structure

- Part one: legal overview
 - The Data Protection Act and what it requires: key concepts, individuals' rights, legal obligations etc.
 - 'Interface' between Data Protection and Freedom of Information.
- Part two: what Data Protection means for SOAS and for SOAS staff.

What is 'Data Protection'?

- **Rights and legal obligations** rooted in EU law: **1995 EC Data Protection Directive**.
- Implemented in the UK as the **Data Protection Act 1998**.
- replacing the Data Protection Act 1984.
- A regulatory body – the **Information Commissioner**.
- **Codes of practice**: CCTV, Employment Practices.

What is 'Data Protection'?

- Appeal process: individuals can request an **assessment** by the Commissioner as to whether our processing of their data is lawful.
- They can **sue** if they suffer damage or distress as a result of our actions.
- Enforcement powers of the Commissioner:
 - Information notices
 - Enforcement notices.
 - Criminal prosecution in serious cases (e.g. fraud).

Why do we need to worry about it?

- Data Protection Act applies to **all organizations** which hold and process personal data...including SOAS.
- **All SOAS staff** will process data about other people in some form in the course of their work.

For all personal data...we have to:

- **Register** our processing with the Information Commissioner (**notification**).
- Process personal data in accordance with **individuals' rights** (e.g. right of **subject access**).
- Process personal data in accordance with eight **Data Protection Principles**.
- ... but first: let's look at some **key concepts**.

What is “personal data”?

- Information about **living** individuals who can be **identified** from the data, or other information which we hold or are likely to obtain.
- So DPA does not cover:
 - Information about the **deceased**.
 - **Aggregated** data.
 - **Anonymised** data.
- Personal data **does** include:
 - **Coded** data.
 - **Indirect references**, where identity is obvious.
 - **Opinions** or **intentions** towards an individual.

What is “personal data”?

- Concept of ‘personal data’ has been in flux in recent years....
- The official view now seems to be that *any information* that can be linked to an identifiable, living individual should be considered to be personal data.
 - European Commission ‘Article 29 Working Party’ report issued in June 2007.
 - The UK Information Commissioner’s revised guidance ‘Determining What is Personal Data’ (August 2007).

What is “sensitive” personal data?

- Subcategory of personal data within the DPA.
- Personal data relating to **racial or ethnic origins, political opinions, religious beliefs, trade union membership, health, “sexual life”**, commission or alleged commission of **offences, criminal proceedings**.
- Subject to additional protections.

What formats of data are covered?

- For bodies like SOAS which are subject to both the Data Protection Act *and* the Freedom of Information Act...
- The **format** in which personal data is held is now **largely irrelevant**.
- Paper and electronic data is covered by the DPA.
- If data is in **paper format only**, how the data is held can have some implications for:
 - The extent of protection by the DPA.
 - Individuals' right of access to personal data.

What formats of data are covered?

- Data Protection Act 1998: personal data is information which is:
 - Processed automatically by equipment, or intended to be processed automatically; or
 - Paper format data held or intended to be held in a **relevant filing system**:
 - A system in which data is **structured by reference to individuals** or by criteria relating to individuals, so that **specific information** on an individual is readily accessible.
 - E.g. a filing system with files on individuals in which information can be located easily.

What formats of data are covered?

- Freedom of Information Act 2000: for bodies to which FOIA applies, **other types** of paper format personal data are now covered by the Data Protection Act but with more limited protection.
- If personal data is in paper form and is **not** in a relevant filing system...
 - It has to be **kept up to date**.
 - Individuals have a **right of access** and a **right to request the correction of inaccurate data**.
 - Other aspects of DPA do **not** apply (e.g. notification).

What formats of data are covered?

- For organisations subject to FoI, individuals have a right of access to personal data about them if:
 - The data is in **electronic form**; or
 - The data is in **paper form** in a “**relevant filing system**”; or
 - The data is in paper form, not in a “relevant filing system”, but in a system which is **structured by reference to individuals or criteria relating to individuals** (e.g. a file on an individual); or
 - The data is in paper form and the person has **described** the data in a way which allows it to be located.
- In **all** cases (regardless of format), we have the right to ask for information which we reasonably need to locate the data.

Other key concepts...

- DPA regulates the **processing** of personal data
 - **Processing: anything** that you do to data (gathering, holding, storing, analysing, disclosing, transferring etc).
- **Data controller**
 - An organisation which holds and processes personal data.
- **Data processor**
 - An organisation which processes personal data on behalf of a data controller (e.g. outsourcing).
 - Data controller is legally responsible, and must ensure that the contract reflects Data Protection obligations.
- **Data subject**
 - Anyone who is the subject of personal data.

What rights do individuals have under Data Protection?

- They can prevent us from processing their data in a way which is likely to cause them **substantial damage** or **substantial distress**.
- Exercised by serving a legal 'section 10' notice.
- There are exemptions which mean we don't always have to comply: e.g. if the processing is:
 - Required for performing a contract with them, or for entering into a contract;
 - Required by any other legal obligation;
 - In their "vital interests" (life and death emergencies only!).

Individuals' rights

- They can prevent us from using their data for **direct marketing** purposes (including marketing for **non-profit** purposes).
- In the area of direct marketing...also need to consider **EC Directive on Privacy and Electronic Communications** (implemented 2003).
- Regulates direct marketing by **email, fax, telephone** and **automated dialling**.

Individuals' rights

- Email marketing: an organisation can only send unsolicited communications with the recipient's **prior consent**, or if:
 - There is a previous business relationship with the recipient;
 - The email is for similar goods/services; and
 - The recipient is given the right to **opt out** when their data is gathered, and at all stages.
- Affects academic mailing lists – as 'marketing' can be non-commercial.

Individuals also have the right to...

- Require us to **correct** or **erase** inaccurate data.
- Prevent decisions being made *solely* by automated processes (e.g. credit scoring).
- Be informed about automated decision making processes which affect them, where the decision is made solely by automated means.
- Request access to data which we hold about them (right of “**subject access**”).
- ...and these rights apply to anyone, anywhere in the world – if we hold their data.

Subject access rights

- Individuals have the right to be given, on request:
 - A **description** of any data which relates to them;
 - A **copy** of the data;
 - Any information about the **source** of the data; and
 - Any information necessary to **understand** the data.
- ...and they have a right to be told:
 - The **purposes** for which the data is being processed;
 - The **recipients** to whom the data may be disclosed.
- Usually, it's sufficient to provide access to the data with any codes, etc explained.

Subject access requests

- Must be in **writing**.
- Data controller can charge a fee (usually £10), and ask for ID.
- Data controller has **40 calendar days** to respond.
- If it's a valid request, the data must be supplied in "permanent form" (i.e. paper), provided...
 - The information is "personal data" in the sense of the DPA (some information may fall under FoI instead).
 - Data subject has provided us with the information we reasonably need to locate the data, if requested.
 - No **exemptions** apply.

Examples of exemptions...

Access to data would:

- Prejudice **crime prevention or detection**.
- Endanger physical or mental health.
- Disclose information subject to **legal professional privilege**.
- Disclose the **personal data of other individuals**.
- Involve “disproportionate effort”.

Other limitations on the right of access...

- We don't have to **create** data for the purpose of answering a request.
- We don't have to release:
 - Data created **after** receipt of a request; or
 - Data destroyed **before** receipt of the request.
- Data can be amended or destroyed after receipt of a request, if that would have happened anyway.
- ...**but** the *intentional* concealment, alteration or destruction of data in order to prevent its release, once it has been requested, is a **criminal offence** for which SOAS and individual staff can be liable.

18 Oct 2007

Obligations under DPA: notification

- We have to **register** our processing of data with the Information Commissioner (“notification”).
- DPA requires us to:
 - Only process data in accordance with our notification.
 - Keep our notification **up to date**.

Public register of data controllers

- Provides *very general* information on:
 - Identity/details of data controller.
 - **Purposes** for which data is being processed (e.g. “staff administration”).
 - **Types of data subjects** involved (e.g. “staff”).
 - **Classes** of data processed (e.g. “employment details”).
 - Persons to whom data may be **disclosed**.
- Available on Commissioner’s website:
<http://www.esd.informationcommissioner.gov.uk/esd/search.asp>
- Structure is set by the ICO and based on standard templates.

Obligations under DPA: Data Protection Principles

- We have to process data in accordance with 8 **Data Protection Principles**.
- **First Principle**... personal data must be processed **fairly** and **lawfully**....
- **'Fairly'** means that we have a general obligation to provide individuals with information about how their data will be used, when we gather data, so far as *practicable*.
- **'Lawfully'** means that we must not process personal data in any way which is unlawful (e.g. violating the common law of confidence).

Obligations under DPA: First Data Protection Principle

- First DP Principle also requires that any processing of personal data should meet certain **specific conditions**.
- Two sets of conditions in the Act that relate to the First Principle:
 - Conditions that apply to the processing of **any personal data** (Schedule 2) – at least one must apply.
 - Conditions that apply to the processing of **sensitive personal data** (Schedule 3).
 - **Sensitive personal data**: one of the general processing conditions must apply **and** one of the sensitive data conditions must *also* apply.

Processing of *any* personal data: at least one of the following must apply...

1. The data subject has **consented** to the processing;
....or the processing is necessary:
2. for performing a **contract** with the data subject; or
3. for a **legal obligation** other than a contract; or
4. to protect the **vital interests** of the data subject; or
5. for the administration of justice, statutory functions, functions of a government department, or any other “functions of a public nature exercised in the public interest”; or
6. to pursue the **legitimate interests** of the data controller or third parties, and it does not prejudice the rights, freedoms or legitimate interests of the data subject.

Examples of conditions for the processing of *sensitive* personal data

1. The data subject has given **explicit** consent; or
2. The information has been **made public** by the data subject;
.... or the processing is necessary:
3. To protect the **vital interests** of the data subject or another person; or
4. For **employment law** purposes; or
5. For the administration of justice, legal proceedings, the defending of legal rights, the exercise of statutory functions, or the functions of a government department; or
6. For **medical purposes** or a **counselling service**; or
7. For **law enforcement**; or
8. For **equal opportunities monitoring**.

Conditions for processing – the role of consent

- **Common misconception:** you can only process personal data with the individual's consent.
- The **consent** of the individual isn't always essential:
 - There are plenty of “fair processing” conditions which allow us to lawfully process data *without* consent.
- But it's *desirable*, especially for processing sensitive personal data.

Other Data Protection Principles

- **Second Principle**...personal data shall be obtained only for a **specified** and **lawful** purpose, and must not be processed in a manner incompatible with that purpose (must be no “**further processing**”).
- Means that:
 - We must **either** collect data for a purpose covered by our notification, **or**
 - When we gather the data, we must **tell** the data subject what we are going to do with it (normally required by the First DP Principle); and
 - We must not use the data later on for an entirely different purpose, unless that’s permitted by DPA.

Other Data Protection Principles

- **Third Principle**...personal data shall be **adequate**, **relevant** and **not excessive** for the purpose for which it is processed.
- **Fourth Principle**...personal data shall be **accurate** and where necessary, **kept up to date**.
 - We must take **reasonable** steps to ensure accuracy (e.g. correcting data when we know it's inaccurate).
 - Individuals can require us to correct inaccurate data.

Other Data Protection Principles

- **Fifth Principle**...personal data shall not be kept for longer than necessary.
 - But ... **there are no specific retention periods in the Act!**
 - If other legal requirements say we should keep information for a certain period – that will prevail (e.g. 6 years for VAT data).
 - Otherwise, retention periods should be based on business needs and any standards/codes of practice.

Other Data Protection Principles

- **Sixth Principle**...personal data must be processed in accordance with the **rights** of data subjects.
- **Seventh Principle**...appropriate measures must be in place to prevent the **unauthorised or unlawful processing** of data and the **accidental loss, destruction or damage** of data.
- **Eight Principle**...data must not be transferred outside the European Economic Area unless the recipient territory provides an adequate level of data protection.

When can data be transferred outside the EEA?

- The country has been recognised by the EC as providing an adequate level of protection.
- The data is transferred to a US company which has signed up to the 'Safe Harbour' agreement.
- The data is transferred under a contract using model clauses approved by the EC.
- ...Or the transfer is exempt from the 8th Principle, e.g.
 - The data subject has given consent.
 - The transfer is necessary for performing a contract with the data subject (or with a third party at behest of the data subject).
- European Court of Justice has decided that putting data on the web does not in itself violate the 8th Principle.

'Interface' between Data Protection and Freedom of Information

- Freedom of Information has created a **general right of access** to recorded information held by public authorities.
- ...so there is a potential for overlap and conflict with Data Protection.
- To avoid this, FoI has a complex 'interface' with the Data Protection Act.

Personal data and Fol

- Fol Act s.40(1): absolute exemption for personal data relating to the person making an Fol request.
 - If you request data about yourself under Fol, you must re-submit your request as a DPA request.
- Fol Act s.40(3): personal data about **third parties** is exempt from release if disclosure would contravene the Data Protection Principles.

Personal data and Fol

- Information Commissioner: limited situations where third party personal data **can** be legitimately released under Fol:
 - **Basic information about staff:** name, job title, responsibilities, work contact details.
 - **Salaries/expenses** of very senior staff, **grades** of junior staff.
 - **Decisions** or **actions** made by individuals in an **official or work capacity**.
- Other types of personal data...generally exempt from release to third parties under Fol.

Data Protection Key Points

- Data Protection extends to **personal data** on identifiable living individuals.
- Data subjects have **rights**, including a right of access to their data.
- We have obligations to:
 - Maintain our notification with the ICO; and
 - Process data in accordance with the Data Protection Principles.
- DPA and FoI intersect.