Data Protection

The Data Protection Act 1998 ("the DPA") is a piece of UK legislation designed to strike a balance between the interests of the individual in maintaining privacy over their personal details and the possibly competing interests of those with legitimate reasons for using other people's personal information. The DPA places obligations on people and organisations that process personal data and in addition gives individuals certain positive rights in relation to data pertaining to them. Amongst other things, individuals may request access to such data and the data controller (the term used in the DPA to describe the person who determines the purpose for which data is processed) is obliged to respond to this request within 40 calendar days.

The relationship between data protection and digital curation is mutually beneficial. In one respect, robust digital curation practices together with good records management play an important part in ensuring that the provisions of the DPA can be met. From the other perspective, knowledge of the DPA is important for someone engaged in curation activity where they are curating data that is covered by the Act (perhaps they are a researcher who uses personal data in their research). In such cases, an awareness of the constraints imposed by the legislation and how it impacts the way the data can be used is crucial.

The Data Protection Principles

Under the DPA, anyone processing personal information must comply with eight principles of good information handling. The eight principles state that the data must be:

1. Fairly and lawfully processed, in particular in accordance with certain conditions in the Act
2. Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Accurate and, where necessary, kept up to date
5. Not kept longer than necessary for the purpose or purposes they are processed for
6. Processed in accordance with the individual's rights under the DPA
7. Kept secure by the taking of appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, destruction or damage
8. Not transferred to countries outside the European Economic Area, unless there is adequate protection

Benefits and value

Knowledge and institutional implementation of the provisions of the DPA and the eight principles it prescribes has immediate benefits:

- Enables compliance with obligations imposed by the legislation and avoids penalties for non-compliance
- Encourages good practice and ethical approach to use of personal data
- Improves efficiency by reducing time/resources required to meet legislative obligations
- Encourages good records management practices which will have beneficial knock-on effects throughout the organisation. These include:
  - Cutting costs by avoiding expensive data mining and retrieval procedures
  - Improving ability to respond to subject access requests, resulting in faster response time and more accurate response content

HE/FE Perspective

Data protection is often initially considered as an administrative issue, and HE/FE institutions will have an institutional framework in place to ensure the security of all personal data held for administrative reasons. It should be remembered that the DPA also applies to personal data used for research, albeit with some exemptions.

"HE and FE institutions should ensure that [...] employees and students are aware that, while some exemptions are granted for the use of personal data for research purposes, the majority of the Data Protection Principles must still be conformed to — there is no blanket exemption."

— JISC Data Protection Code of Practice for the HE and FE Sectors (January 2001)

e-Science Perspective

"The design and use of advanced Internet and Grid technologies in the social, natural and computer sciences are likely to reconfigure not only how researchers get and provide data resources and other information but also what they and the public can access and know; not only how they collaborate, but with whom they collaborate; not only what computer-based services they use, but from whom they obtain services. This reconfiguring affects the provision of data resources in ways that raise legal, institutional and social issues such as confidentiality, privacy and data protection, ownership of intellectual property rights, anonymity and accountability, and issues of trust, confidence, and risk in distributed collaboration."

— Oxford e-Social Science (OeSS) Project: Ethical, Legal and Institutional Dynamics of Grid-Enabled e-Sciences (2006)

Curation in Practice

- Anonymised data doesn't come under the DPA. Consider whether any personal details in data being curated or preserved add to its usefulness or could be removed.
- Repository administrators should check with contributors whether their deposits contain personal data. This could be covered in a deposit agreement.
- Researchers are exempted from the second and fifth data protection principles. This means that, subject to certain conditions, the further processing of personal data for research purposes is not to be regarded as incompatible with the purposes for which they were originally obtained and personal data which are processed only for research purposes may be kept indefinitely.
- The exemptions from the second and fifth principles apply to 'research purposes'. They do not apply, for example, to learning objects or teaching materials.
- The obligation in the fourth principle to keep personal data up to date is qualified by the words "where necessary". This is of benefit where it is useful to keep the data as it was at a certain point for historical/evidential/archival reasons.
- Except in limited circumstances a data controller must make a notification to the Information Commissioner which shall include the categories of data they hold and the purposes for which they process them. It is worth noting that a special purpose description (outwith the standard categories) has been approved for archives. Under this description, all archives held by an organisation can be notified, including those containing sensitive personal data.

Additional Resources

- The website of the Information Commissioner's Office (ICO) [http://www.informationcomissioner.gov.uk/], which is responsible for enforcement of the DPA and provides guidance on its application
- An ICO Data Protection factsheet [http://www.ico.gov.uk/]
- JISC Data Protection Code of Practice for HE/FE institutions [http://www.jisc.ac.uk/publications/publications/pub_dpacop_0101.aspx]
- The National Archives, Society of Archivists, and Records Management Society Code of Practice for Archivists and Records Managers [http://www.archives.org.uk/publications/dataprotection.html]
- Public Record Office, Data Protection Act 1998: A Guide for Records Managers and Archivists [http://www.nationalarchives.gov.uk/documents/dpguide.pdf]
- Kalra, D et al. Security and confidentiality approach for the Clinical E-Science Framework (CLEF) [http://www.clinical-escience.org/industrial/sep2003/AHM2003-DKalra-CLEF-Security-Confidentiality-Paper.pdf], 2003
- A JISCmail-based mailing list for those interested in data protection and related topics [data-protection@JISCMAIL.AC.UK]