Podbriefing Summary Note

Data Protection Law

Overview

The Podbriefing video on data protection provides a summary of the key elements of data protection law that staff need to be aware of.

It supplements the University's Data Protection Act Policy, a link to which can be found at the end of the Podbriefing and at the end of this summary. We have also included links to useful further information, such as the University's Data Protection Act Policy, and information on relevant case law.

Content and Aims

Focus

This briefing is provided by Geraldine Swanton, a practising lawyer who specialises in data protection within the education sector. The focus of the video is on key legislation, outlining the basic principles and concepts underlying data protection.

Five Data Protection Scenarios

Alongside the briefing, five scenarios feature staff members seeking advice on various different data protection problems. These illustrate key issues experienced in practice, focusing on individual rights of access to data and the sharing, accuracy and security of data.

Consequences

Failure to comply with the data protection regime can have very serious consequences for both the individual and the organisation involved. For example, fines as high as £500,000 can be issued for an organisation that has breached the data protection regime.

Finally, while the problems in the scenarios are portrayed actors, the circumstances involved are based on real incidents.

Key Points

There are two main concepts to consider first: personal data and processing.

Personal Data

Personal data:

- Identifies an individual
- Includes opinions in regards to that individual
- Includes information which informs or influences decisions affecting an individual
- Conveys biographical information about the person (for example; it must go beyond merely recording their presence at a meeting)

An individual has a right to a copy of their personal data on written request.

Subject Access Requests (or SARs) are requests for a copy of an individual's personal data. This would not necessarily be an entire document, only the information relating to the individual.

Q: Can I stop people from seeing opinions I've expressed about them?

A: It is a criminal offence to conceal or destroy data with the intention of preventing access.

Remember that personal opinions amount to data on an individual, therefore be careful what opinions you express when drafting and sending documents or emails.

Processing

This includes anything that can be done with information, from creation to destruction. It covers a wide range of activities such as sending emails or storing data.

Processing must be fair and lawful.

Use and processing of personal data can be justified in the following ways:

- You have the individual's consent
- Pursuing a legitimate interest of the University (as long as the use does not amount to an unjustified breach of the individual's privacy
- Compliance with a legal obligation

- Necessary for the performance of a contract to protect the vital interests of the individual

Q: Can we share a student's data with their parents?

A: Consent is not always necessary; however disclosing information without consent can be a breach of an individual's privacy.

In this case you should obtain the student's consent first, or tell the parents to obtain the information directly from their son or daughter. The parents have no right of access to their child's personal data.

Amount of data and handling

Data must be adequate, relevant and not excessive.

Try not to collect irrelevant personal data.

Data is not to be used for unauthorised wider purposes.

Data should not be kept for longer than is necessary.

Q: What happens if I give out inaccurate information?

A: The mistake should be rectified immediately and procedures should be put in place to periodically check the accuracy of the information.

Personal data needs to remain accurate and up to date in order to avoid errors that could cause damage or distress to individuals.

Data overseas

Transfer of personal data outside of the European Economic Area (EEA) is only possible if there will be an adequate level of protection in the receiving country.

Protection is deemed adequate if:

- The individual's consent to the transfer has been obtained,
- Destination is included in an approved list of countries issued by the European Commission or,
- The Transfer is made subject to standard clauses issued by the Information Commissioner

Research data

Personal data should only be used for specified and lawful purposes.

Individuals need to be aware of how their data will be used.

Transparency and fairness are important principles of the data protection regime.

Staff need to always be aware of why they have generated the data.

Sensitive personal data

Sensitive personal data includes data on:

- Physical or mental health
- Sexual life
- Political opinions
- Trade Union membership
- Racial origin
- Religious beliefs
- Commission or alleged commission of criminal offences

Informed written consent is required to use sensitive personal data.

All personal data, but especially sensitive personal data needs to be stored and used in a secure and confidential way.

Q: What happens if sensitive personal data is stolen?

A: The information commissioner can impose fines of up to £500,000 for any reckless or deliberate serious breach of the Data Protection Act that causes substantial damage or distress to an individual.

Many of the fines imposed have been for breaches in relation to sensitive personal data.

Encryption is of data is a good way to ensure adequate protection.

Relevant Cases

Glasgow City Council - £150,000 fine

Glasgow City Council were fined £150,000 in June 2013 for losing two unencrypted laptops, containing the personal data of 20,143 people.

Greater Manchester Police - £150,000 fine

Greater Manchester Police were fined £150,000 in October 2012 after the theft from an officer's home of a memory stick containing details of over 1000 people linked to serious crime investigations. It had no password protection.

London Borough of Barnet - £70,000 fine

London Borough of Barnet were fined £70,000 in May 2012 for losing sensitive information relating to 15 vulnerable young people during a burglary at an employee's home.

(Source: http://www.ico.uk/enforcement/fines)

For up to date examples of the penalties issued for breaches of the Data Protection Act, and information on how these are calculated, see the website for the Information Commissioner's Office.

(http://ico.org.uk/enforcement/fines)

Further Information

Data Protection Act Policy

Policy on the Release of Personal Information

http://www.nottingham.ac.uk/academicservices/policies/data-protection/data.aspx

Handling Requests for Personal Data – Staff Guide

http://www.nottingham.ac.uk/academicservices/policies/data-protection/data.aspx

Electronic Mail Usage Policy

http://www.nottingham.ac.uk/hr/guidesandsupport/universitycodesofpracticeandrules/electronicmailusage.aspx

Code of Practice for Users of the University Computing Facilities

http://www.nottingham.ac.uk/hr/guidesandsupport/universitycodesofpracticeandrules/electronicmailusage.aspx

Information Security Policy 2012/13

(Available for staff on Workspace via http://www.nottingham.ac.uk/is/computer/security.aspx)