CS 978 – Legal, Ethical, and Professional Issues for the Information Society

Lecture 4 – Data protection: *from DPA to GDPR*

Introduction

The arrival of legislation to protect data formed around the notions of self-determination and privacy. The premise of data protection legislation is that only the individual has a right to determine who uses their data (outside of law enforcement and certain other state functions) and for which purposes.

The first data protection law was introduced in the German state of Hesse in 1970, and this was soon followed by legislation across Europe, starting with Sweden in 1973, Germany as a whole in 1977, France, Denmark, Norway, and Austria in 1978, and in the UK the first Act was introduced as the Data protection Act 1984. This Act was updated in 1998, and most recently in 2018 as a result of the EU's GDPR.

How should data protection be controlled?

There are a number of ways that can be considered in terms of controlling access to and protecting data. Not all of them deal with the issue of legal enforcement, although this is certainly a key strategy as we will see. Other solutions include:

- **Voluntary codes**: where an industry or professional body agrees on standards and protocols for controlling access to personal data. This is normally voluntary but is a major exercise in public relations for many industries who struggle with a bad image. Example in the UK would be the direct mail industry which finances the Mailing Preference Service (http://www.mpsonline.org.uk/mpsr/) and the Telephone Preference Service (www.tpsonline.org.uk), both opt-out services for consumers who wish to stop junk mail and sales telephone calls.
- **Consumer education**: making citizens aware of good practice in controlling their own data, for instance not passing it on carelessly and being aware of their rights in accessing it and preventing others misusing it. The Information Commissioner in the UK offers a *Personal Information Toolkit* (copy available on MyPlace) to educate the public about all of their information rights
- **Technological solutions**: solutions that allow data to be encrypted when transferring offer some security for both organisations and consumers. A common example of this is in the encryption of credit card details on e-commerce websites, however software

solutions can be purchased that also allow encryption of personal data such as emails. Encryption is increasingly being used as solution for both consumers and businesses.

For those countries who have legislated for data protection, a core set of principles tend to govern their actions. These principles embody rights the user has with regard to the information that is stored about them, and include:

- a right to inspect the information;
- a right to have it corrected if it is erroneous;
- a right to sue for compensation if wrongful information has caused them damage;
- in some instances, a right to object to such information being held at all.

Data protection legislation varies considerably across the world in the degree of protection which it actually affords the individual. However, across the European Union, data protection is taken extremely seriously, and all countries who operate in or do business in the EU need to take the issue equally seriously.

Data protection principles

Under the 1998 Data protection Act eight principles governed the ethos of the Act. These were that data should be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than necessary
6. Processed in line with data subject's rights
7. Secure
8. Not transferred to countries without adequate data protection

These principles have been updated as part of GDPR, as we will see below.

In September 2016 the highest fine yet imposed was given to telecom company Talk Talk, who were fined £400,000 for the hack of their website in 2015. The fine was based around principles 5 and 7 of the 1998 Act, and related to the database of another company Talk Talk had purchased (Tiscali) which had an old database system accessible via the web. Almost 150,000 account details were obtained in the hack, almost 16,000 of which included full bank account details, and a further 28,000 included full debit/credit card details. The hack saw the company lose £60m in value and 85,000 customers once the hack was made public. Fines under GDPR are likely to be significantly higher, and as well as the financial implications for organisations concerned, are likely to raise significant issues of public trust.

The rights of the Individual

The key right of a citizen is to be able to find out what data an organisation has stored about them, ensure it is done so lawfully, and to be able to have any erroneous information corrected. Rights strengthened under GDPR will be discussed further below.

Challenges with data protection law

One of the arguments against making penalties in breaching the act more severe related to the idea that companies may hold stringently to the law in fear of breaching it, even when doing so might be the right thing to do.

A tragic case occurred in 2003 in London when an elderly couple were found dead in their home after their gas had been cut off because of a £140 bill that was unpaid. British Gas did not inform social services about the plight of the couple out of fear of breaching data protection legislation, and they were inevitably criticized for their inaction. The Information Commissioner stated that: "It is ridiculous that organizations should hide behind data protection as a smokescreen for practices which no reasonable person would ever find acceptable….".

Towards the General Data Protection Regulation (GDPR)

Even though the EU data protection regime is one of the most stringent in the world, moves to make it even more so resulted in the development of the General Data Protection Regulation, or GDPR. In EU law, a *regulation*, unlike a *directive*, has automatic legal validity. While a directive is designed to be incorporated into the law of member states via specific legislation in those states, a regulation automatically applies in law. Notwithstanding the decision of the UK to leave the EU in the referendum of June 2016, the UK government has indicated that they still wish to apply GDPR within UK law.

The GDPR was passed by the European Parliament in May 2016 and comes into force in May 2018. It strengthens and amends data protection in several important areas.

Definitions of personal data

The scope of what can be called personal data has been expanded significantly to cover a range of types of information on a data subject. Personal data can now include names of people, email addresses, bank details, and contributions to social networking sites, photographs, and even computer IP addresses. The key rubric is that any piece of information that can make someone *identifiable* is potentially personal data.

Consent

The focus that consent must be informed is clear in the GDPR. The agreements people sign must be easily readable, accessible, and with the purposes for the consent being requested made clear. Long streams of legalese will no longer be acceptable, and opting in will be the only acceptable

standard for sensitive personal data. Therefore, tick boxes where you have to opt out of having your data collected will not be acceptable for organisations requesting sensitive personal data.

Right to access

Rights to know if your data is being processed and to access it if so, have been expanded. In addition, a person is able to request an *electronic* copy of their data for free from a data controller. In addition, the right to **data portability** is enshrined in GDPR, meaning the data subject can request their data in machine readable format to allow them to pass it to another data controller.

Right to be forgotten

Also referred to as data erasure, this provides the right to have their data deleted if it is no longer needed or if the processing it was stored for is no longer taking place. Data controllers can balance public interest versus the subject's rights in this regard.

Breach notification

This will become mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Privacy by design

A consideration in the UK for some time, privacy by design is the notion that when building any service or application that will store personal data, it must be done so with privacy as a primary objective. Privacy must not be an afterthought; it must be central to the design of the system.

Data protection officers/processors/controllers

The GDPR places clear guidelines on organisations with regards to processing personal data. Data controllers (usually the organization the subject has given their data to entities who define the parameters of what data is needed and how it will be processed. Data processors are entities who undertake processing of data on behalf of the data controller. For instance, a bank would be a data controller, and they use credit reference agencies (data processors) to check customer credit worthiness. Increasingly as services move to the cloud and data is stored there by third parties, the clarity between processor and controller is important to define.

Data Protection Officers (DPOs) must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data. DPOs:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

Punishment

Organisations can be fined a maximum of 4% of their annual turnover or 20 Million Euros, whichever is larger, for data breaches. The fines are tiered, and organisations with good DPA practice will not be punished as severely as those without.

Lawful basis for processing

An important aspect of data protection under GDPR is that an organisation cannot process data unless it has a lawful basis for doing so. There are six types of lawful basis:

- Consent: which must be informed, and requires a positive opt-in from the data subject to the processing. The guidance on what the processing would consist of should be clear and unambiguous in order for the consent to be genuinely informed.
- Contract: this is allowed if you need the data to fulfil a contractual obligation to the data subject, or if they have asked you to do something before entering into a contract (e.g. provide a quote)
- Legal obligation: If you need to process the data to comply with a common law or statutory obligation
- Vital interests: if you need to process the data to protect someone's life. You cannot use this lawful basis for processing health or other sensitive data if the subject is capable of giving consent, even if they refuse consent
- Public task: if you need to process the data in the exercise of official authority of public functions, or if the processing is in the public interest as set out in law
- Legitimate interests: this is the most flexible lawful basis for processing, but is not always the most appropriate. It is likely to be so if you are processing data in reasonable ways that subject's would expect, and which have minimal privacy impact.

The new data protection principles

Under the GDPR there are now six data protection principles, and seventh over-arching principle. These are:

a) Lawfulness, fairness and transparency
b) Purpose limitation
c) Data minimization
d) Accuracy
e) Storage limitation
f) Integrity and confidentiality (security)

And the overarching principle of Accountability.

The GDPR became law in May 2018 and as a result a new *Data Protection Act 2018* came into force in the UK at that time. The idea is this will also make the UK ready for business with the EU post Brexit.

Conclusions

Data protection legislation in the UK and EU is robust, and anyone involved in an activity that gathers information on the public must be aware of what it stipulates. Technology allows personal data to be used in a myriad of ways, and the expansion of big data as a concept, and the ability to data mine may entice us into believing things have changed with regards utilizing personal data. In truth, while technology has changed, law has not, and professionals need to be very careful in how they use the data of citizens/customers in delivering services to them.

Further Reading

ADAMS, Andrew A. and McCRINDLE, Rachel J. (2008) *Pandora's Box: social and professional issues of the information age*. Chichester: John Wiley and Sons. **Chapter Seven**.

Information Commissioners Office (2018). *Data protection reform.* Available from: https://ico.org.uk/for-organisations/data-protection-reform/

DMcM/09-2018