Data Security Legislation

DATA SECURITY AND THE GDPR

General Data Protection Regulation

General Data Protection Regulation 2018

The General Data Protection Regulation (GDPR) replaced the Data Protection Act in May 2018. It is designed to overhaul how businesses process and handle data.

The new regulation applies to not just the UK's data protection laws, but all of Europe's. It is designed to give greater protection and rights to individuals and their data.

The GDPR also applies to all companies worldwide that process personal data of European Union (EU) citizens.

The GDPR Act

In the UK, the Data Protection Act (1998) set out how our personal information could be used by companies, government and other organisations.

The Data Protection Act was derived from Europe's framework for data protection laws, the "Data Protection Directive."

The new UK legislation is called the "Data Protection Bill", which in turn, is derived from the new GDPR.

What is covered by the Act?

Personal and sensitive data is covered by GDPR.

GDPR now includes data that can be considered pseudonymised. This is making data less identifiable; for example, a name is replaced with a unique number.

The purpose is to render the data record less identifying and, therefore, reduce concerns with data sharing and data retention.

Rights of the Individual

The GDPR provides eight main rights that individuals have. These are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights relating to automated decision-making profiling

Research Task

- How does GDPR 8 main principles apply to you?

Comparison

Data Protection Act: Rights	General Data Protection Regulation: Rights
A right of subject access	The right to be informed
A right of correction	The right of access
A right of prevent distress	The right to rectification
A right to prevent automatic decisions	The right to erasure
A right of complaint to the Information Commissioner	The right to restrict processing
A right to compensation	The right to data portability
	The right to object
	Rights relating to automated decision-making profiling

Giving consent to process Personal Data

The threshold for consent to use on individual's data is much higher than the previous Data Protection Act.

Any request for consent must be very clear, easy to read and in a plain language that the data subject can understand.

In practice, if consent is required to collect and use your personal data, it is likely that an express opt-in will be the least that is required.

Consent

Can be withdrawn at any time (and it must be easy to do so)

Is not always appropriate (e.g. if data would be processed anyway)

Won't be valid if there is too much of an imbalance of power (e.g. if an employer asks an employee for consent, the employee may feel obliged to give it even if they didn't want to)

Needs to remain valid (meaning it may need to be asked for again after a given period of time)

Responsibilities of companies

A Controller and A Processor

- The GDPR also applies to companies that process and control personal data. It divides individuals and organisations into two categories: a controller and a processor. This can be seen in the Table

Controller	Processor
Determines for what purpose the personal data is being used.	Needs to follow a specific set of legal obligations placed on them by the GDPR.
Responsible for making sure the Processor is complying with the GDPR.	Maintain records of personal data, and the processing activities carried out on that data.
	Has the legal liability and it is them that is responsible if there is a data breach?

Article 5

Article 5 of the GDPR states the main principles of the act. It states that personal data shall be:

- processed lawfully, fairly and transparently
- only collected and used for lawful purposes
- adequate, relevant and not excessive for that purpose
- accurate and up to date
- stored no longer than necessary
- kept secure, and its integrity and confidentiality are protected

Accountability Principles

There is also a new accountability principle, which means companies and organisations need to be able to demonstrate compliance with these principles.

Data Protection Act: Principles	General Data Protection Regulation: Principles
Fairly and lawfully processed	Processed lawfully, fairly and transparently
Processed for limited purposes	Only collected and used for lawful purposes
Processed in line with your rights	Adequate, relevant and not excessive for that purpose
Adequate, relevant and not excessive	Accurate and up to date
Accurate	Stored no longer than necessary
Not kept for longer than necessary	Kept secure and its integrity and confidentially are protected
Secure	
Not transferred to other countries without adequate permission	

Data Stored Outside the EU

Our data is stored across many countries. Cloud-based storage means that our personal data can now be stored on a server in a country outside of the EU.

Countries outside of the EU may have very different laws to our own when it comes to keeping data secure.

The GDPR states that data can only be transferred to a country, or international organisation, when an adequate level of protection is guaranteed.

Breach of data security

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Research Task

- Who do we report GDPR security breaches too?

What level of security is required?

The GDPR does not define the security measures that you should have in place.

It does require a level of security that is 'appropriate' to the risks presented by the processing.

You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

Levels of security 2

- This reflects both the GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security.
- It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.
- So, before deciding what measures are appropriate, you need to assess your information risk.

Level of Security 3

- Before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:
- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

GDPR video

Other Legislation Relating to Data Security

- The European Convention on Human Rights. Article 8
- Freedom of Information Act (Scotland)
- Computer Misuse Act
- (A non exhaustive list)