Data Protection Act

Contents

1 Introduction

Digital technology has transformed almost every aspect of our lives in the twenty years since the last Data Protection Act was passed.

Since information systems and business models become more complex, a number of organisations may be working together in an initiative that involves processing personal data.

1.1 What it is

makes our data protection laws fit for the digital age in which an ever increasing amount of data is being processed empowers people to take control of their data supports UK businesses and organisations through the change ensures that the UK is prepared for the future after we have left the EU

1.2 Why we have it

We use it to deal with data protection when dealing with Britsh data who doesn't belong to EU

When it comes to EU we use **GDPR** which is essentially DPA but applied when dealing with information coming from EU

2 The key principles

It is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

2.1 Lawfulness, fairness and transparency

Ensures that users can understand what it is there are signing up to when they hand over personal data. This principle requires that organisations use language that is 'clear, plain and accurate' as to what a data subject is consenting to

2.2 Purpose limitation

Stipulates that personal data, which is collected for a specific, previously stated and understood purpose, must not then be used for other applications.

2.3 Data minimisation

Ensuring that the extent or amount of data collected and/or processed is adequate, relevant and limited to the intended purpose

2.4 Accuracy

Makes organisation responsible for either updating inaccurate information or getting rid of it.

2.5 Storage limitation

Restricts organisations from keeping hold of data for indefinite periods of time, or beyond that of its intended purpose

2.6 Integrity and confidentiality

Previously known as the 'security' principle, integrity and confidentiality of personal data must be upheld with the appropriate security measures. As with many of the other principles, there is an inherent responsibility to implement both physical and technological controls to ensure compliance.

2.7 Accountability

Requires organisations to take responsibility for the personal data being handled and their compliance with the other six principles. Appropriate measures and records are also required to be in place as to demonstrate compliance.

2.8 International Transfer of Data

Regulates the transfer of personal data to countries or organisations outside the UK to make sure they are sufficiently compliant with the standards laid forth by the legislation.

3 Difference between data processor and data controller

The DPA draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the data controller that must exercise control over the processing and carry data protection responsibility for it.

3.1 data controller

"data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

3.2 data processor

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.3 processing

It means obtaining, recording or holding data or carrying any set of operations on the data, including

- organisation, adaptation or alteration of the information or data
- retrieval, consultation or use of the information or data
- disclosure of the information or data by transmission dissemination or otherwise making available
- alignment, combination, blocking, erasure or destruction of the information or data

4 GDPR penalties

There will be two levels of fines based on the GDPR. The first is up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher. The second is up to €20 million or

4% of the company's global annual turnover of the previous financial year, whichever is higher. The potential fines are substantial and a good reason for companies to ensure compliance with the Regulation.

The Parliament had requested for fines to reach €100 million or 5% of the company's global annual turnover. The agreed fines are the compromise that was reached.

Fines for infringements will be considered on a case-by-case basis and will take a number of criteria into consideration, such as the intentional nature of the infringement, how many subjects were affected and any previous infringements by the controller or processor.