Data Protection

DATA PROTECTION ACT 2018 AND UK GDPR

What is the Data Protection Regime?

It is the general Data Protection regime that applies to most UK businesses and organisations. It covers the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

What is Data Protection?

Data protection is the fair and proper use of information about people.

And involves implementing the General Data Protection Regulation (GDPR) principles that ensure people can trust that your use of their data is in a fair and responsible manner.

Who must adhere to the Data Protection Act 2018?

Anyone who collects personal information about individuals for any purpose must comply.

And anyone who comes into contact with personal data that is not their own.

What is Personal Data?

Personal data is any information which is related to an identified or identifiable natural person.

Identifiers include; a name, an identification number, location data, an online identifier, telephone number, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data etc.

Data Protection Glossary.

What is processing?

Almost anything you do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

Who is a ‘controller’?

A controller is the person that decides how and why to collect and use the data. This will usually be an organisation but can be an individual. If you are an employee/volunteer acting on behalf of your employer, the employer would be the controller.

Data Protection Glossary.

Who is a ‘Processor’?

A processor is a separate person or organisation who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller’s obligations.

UK GDPR's 7 Key Principles.

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Lawfulness, fairness and transparency.

“ (a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

You must ensure that you do not do anything with the data in breach of any other laws.

You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

You must be clear, open and honest with people from the start about how you will use their personal data.

1. Purpose limitation

"(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

You must be clear about what your purposes for processing the data are from the start.

You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

1. Data minimisation

"(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Adequate, sufficient to properly fulfil your stated purpose, and no more.

Relevant, the data has a rational link to that purpose and only limited to what is necessary, you do not hold more than what you need for that purpose.

Accuracy

“(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.

If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.

Storage Limitation

“ (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

Storage Limitation

You need to think about, and be able to justify, how long you keep personal data. This will depend on your purposes for holding the data.

You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.

Integrity and confidentiality

You must ensure that you have appropriate security measures in place to protect the personal data you hold.

This is the ‘integrity and confidentiality’ principle of the GDPR – also known as the security principle.

Accountability

"(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

The UK GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Accountability and Governance.

Accountability is one of the data protection principles - it makes you responsible for complying with the UK GDPR and states that you must be able to demonstrate your compliance.

You must practise the appropriate technical and organisational measures, put in place to meet the requirements of accountability.

Accountability and Governance.

The Organisation has set out procedures on how data is processed and handled, in line with the UK GDPR and the Data Protection Act 2018, it is our responsibility to adhere to them.

This will ensure we protect information that pertains to vulnerable people, who have entrusted us with their information.

By using good practises, we also protect the organisation’s reputation and allow it to continue its work.