General Data Protection Regulations

The General Data Protection Regulations (GDPR) come into force from 25 May 2018.

Here is brief guide on the changes.

The GDPR applies to personal data:

What is Personal Data?

It means data which relates to a living individual who can be identified –

a) from the data, or
b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It also includes IP addresses

If you hold and process personal information about your clients, employees or suppliers, you are legally obliged to protect that information.

The Principles:

GDPR has a set of principles by which you must adhere to if you hold or process personal information:
Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals
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 incompatible with the initial purposes
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
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 is 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
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

The key principle is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals

To rely upon this principle, you also need to show that you have a lawful basis (condition) before you can process the personal data:

The Conditions are:

6(1)(a) Consent of the data subject
6(1)(a) Processing is necessary for the performance of a contract with the data subject or to take steps to enter a contract
6(1)(a) Processing is necessary for compliance with a legal obligation
6(1)(a) Processing is necessary to protect the vital interests of a data subject or another person
6(1)(a) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6(1)(a) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

For example; where you rely upon the principle of lawful processing - you would need to seek the consent of the individual (the data subject) – consent must be positive.

Individual Rights:

With the regulations come extensive rights for individuals.

These are:

The Right to be Informed

Individuals will have a right to be informed and you have an obligation to provide fair processing of information – usually by having a privacy notice and ensuring it is GDPR compliant.

The Rights to Access

Individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data

The Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The Right to Erase

Also, known as the right to be forgotten. The individual has the right to request the deletion of or removal of personal data where there is no compelling reason for its continued processing.

The Right to Restrict Processing

Individuals have the right to restrict or block processing of personal data.

The Right to Portability

This allow individuals to reuse their personal data across different services.

The Right to Object

The right to object to direct marketing/research

Rights Related to Automated Decision Making and Profiling

This provides safeguarding for individuals against the risk of decision taking without human intervention.

The regulations promote accountability and governance. Companies are expected to put into place measures to demonstrate that they comply with the principles and state explicitly that this is their responsibility.

For example:

- Data protection policies
- Staff training
- Audits
- Reviews
- Who will deal with data protection issues
- If your company has more than 250 employees, you are required to maintain records of activities relating to high risks processing.

Breach

The Regulations will introduce a duty on all organisations to report certain types of breaches not only to the regulator but in some cases to the individual.

The Regulations also impose restrictions of transferring personal data outside of the European Union.

The GDPR establishes a tiered approach to penalties for breach which enables the DPAs to impose fines for some infringements of up to the higher of 4% of annual worldwide turnover