what is GDPR?

The General Data Protection Regulation (GDPR) is a new data protection law which comes into full effect in 2018. It sets out the main principles of data protection and the responsibilities organisations have when handling personal data. It protects individuals' personal information and improves their control over how it is collected, stored, shared and used.

The core principles of data protection remain broadly the same, so if you know about the DPA requirements, you'll find GDPR familiar. But GDPR provides a far more comprehensive framework for data collection, processing and storage. The penalties for getting it wrong are also much more severe.

article 5 of the GDPR requires that 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 considered to 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 are inaccurate, having regard to the purposes for which they are processed, are 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 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; and

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."

article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

In brief, GDPR gives individuals more control over the data held on them. It introduces tougher fines for privacy breach and non-compliance, and there are some key changes, such as the age of minors.

- An individual's consent over how their data is processed is given a higher standard. Consent must be quite clear and freely given, and can be withdrawn. Consent must be a positive opt-in, so pre-ticked boxes alone will no longer be sufficient. Individuals have the right to know in detail how their personal data is processed, used and shared. (Consent is not the only reason for processing data - there are other reasons such as 'legitimate interests'.)

- Individuals have greater rights, including the right to have their data corrected or erased, to restrict the processing of their data and to reclaim their personal data and send it on elsewhere. Reasonable requests are free of charge and must be met within a month.

- The ICO must be notified about any breaches where there may be a risk to the rights and freedoms of individuals. All breaches must be recorded even where notifying the ICO isn't necessary.

- The fines for organisations which don't get it right can be much larger than previously (up to 4% of annual worldwide turnover and €20 million).

- Some organisations will have to appoint data protection officers to oversee their data processing activities.

- Data controllers will have to have written contracts with any data processors they appoint. It will remain a legal requirement for data controllers to pay the ICO a data protection fee, but you will no longer have to register your data processing activities with the ICO.

For the latest information, see the Information Commissioner's Office (ICO) website, which has lots of resources from basic tools to detailed guides. It's worth checking back regularly as GDPR information is still being updated. If you sign up for the ICO newsletter, you will get regular updates on the guidance available.

ICO checklist and your next 12 steps

ICO compliance self-assessment