KEEN
DICEY
GROVER
CHARTERED
ACCOUNTANTS
TEL: 01753 652098

Updated 25 May 2018

The General Data Protection Regulation

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018, placing additional obligations on businesses in regard to the safeguarding of personal data.

The GDPR requires all organisations that deal with individuals living in an EU member state to fully protect the personal information belonging to those individuals, and to have documented proof of such protection. The UK's decision to leave the EU has not affected the introduction of the legislation in the UK.

The regulations require a consistent and transparent approach to data processing, and the financial penalties for failing to comply are severe – with fines of up to €20m or up to 4% of total annual worldwide turnover.

Requirements for businesses

While the principles of the GDPR are broadly similar to the existing Data Protection Act (DPA), there are some key changes placing additional obligations on businesses.

The GDPR places a new emphasis on accountability and transparency when it comes to dealing with personal data. While businesses may already be compliant with many of the regulations as covered under the DPA, they are also required to provide documentary evidence of their compliance with the GDPR.

Specifically, the GDPR rules state that businesses must be accountable for their data usage, and must identify a lawful basis for processing personal data.

The GDPR specifies that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up-to-date; where personal data is inaccurate, it should be either erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary
- 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.

The GDPR builds on the existing rights and principles for individuals under the DPA, as well as introducing some additional rights. Some of the key rights under the GDPR include:

- **Condition for consent** – you must obtain consent from individuals to gather information for specific purposes, and be able to prove that you have done this
- **Right to access data** – individuals may request details of information that is held about them, how, why and where it is accessed, what categories of data are being accessed and who has access to the information. The maximum amount of time allowed to deal with a subject access request has also been reduced from 40 to 30 days under the GDPR, and the right to charge a subject access fee has been removed (except in the case of unfounded, excessive or repetitive requests)
- **Right to erasure** – meaning that individuals have the right to ask that data about them is deleted. This would include ensuring that all copies of information are deleted, including data stored in an online cloud system
- **Right to rectification and objection to profiling** – individuals may request that inaccurate data is corrected, and may object to any profiling that could result in them being discriminated against.

The law places particular emphasis on the issue of consent, stating that an indication of consent must be specific, unambiguous and freely given. Positive consent cannot be assumed from inaction, such as failing to click an online 'unsubscribe' box, or from the use of pre-ticked boxes. Businesses also need to make sure that they capture the date, time, method and the actual wording used to gain consent, so it is important to ensure that your business has the means to record and document such information.

Additional obligations apply to certain organisations and those with more than 250 employees.

Complying with the regulations

Businesses should ensure that they are compliant with the GDPR, as fines for non-compliance may be severe. Some of the main areas to consider include:

- Making sure members of staff are aware of the regulations, and providing ongoing training
- Identifying the lawful basis for your data processing activity
- Reviewing and classifying the personal data your business holds, its origins and who you share it with
- Creating an audit trail
- Reviewing your procedures relating to consent, requesting and documenting fresh consents from customers where necessary to ensure that your business is seeking, collecting and managing consent in line with the GDPR
- Updating procedures to ensure they cover the enhanced rights for individuals, including the right to have data erased and the right to data portability, as well as new protection for children's data and the reduced 30 day deadline for subject access requests
- Reviewing your privacy notices
- Adopting a principle of 'data protection by design' for all future projects
- Including procedures for identifying and investigating data breaches
- Assigning responsibility for data protection to a key member of staff; appointing a Data Protection Officer (DPO) will be a legal requirement for some organisations
- Making sure that your data and processes are regularly reviewed to ensure that they remain

compliant.

Further information and guidance can be found on the Information Commissioner's Office website: www.ico.org.uk.