McEwanWallace
Undivided attention
Chartered Accountants
Business Advisers

68 Argyle Street
Birkenhead, Wirral
CH41 6AF
T: 0151 647 6681
F: 0151 666 2115
E: enquiries@mcwallace.co.uk
W: www.mcwallace.co.uk

The new data protection regulations: is your business prepared?

The new General Data Protection Regulation (GDPR) is set to come into effect in May 2018, strengthening the obligations on all businesses in regard to the safeguarding of individuals' personal information. Here we provide an overview of the new legislation and outline some key areas to consider.

What is the GDPR?

With the exponential growth of the digital economy, and significant changes to the ways in which information is collected and used, having in place clear and robust policies on data protection is now more important than ever.

On 25 May 2018, the new GDPR will come into effect, requiring all organisations that deal with individuals living in an EU member state to protect the personal information belonging to those individuals, and to have verified proof of such protection. Failure to comply with the new regulation will result in significant fines.

The new GDPR places an emphasis on transparency and accountability, and requires businesses of all sizes to be responsible for safeguarding the collection, storage and usage of personal data, stating that the protection of personal data is an individual's 'fundamental right'.

The GDPR applies to processing carried out by organisations operating within the EU, and also to those offering goods or services to individuals who live in the EU – including international businesses which are located outside, or process data outside, the EU. The UK's decision to leave the EU will not affect the introduction of the GDPR, and the government plans to introduce similar legislation thereafter, so it is essential to ensure that your business is prepared.

What constitutes personal data?

The GDPR expands on the existing Data Protection Act (DPA) definition of 'personal data', including not only information such as the names and addresses of customers, but also information on current and former employees and associates. In addition, it encompasses a significantly greater range of personal identifiers.

Taking account of changes in technology, this now includes 'online identifiers' such as IP addresses or website cookies which are used to collect individuals' information – and even in some cases personal data that has been pseudonymised, depending on how difficult it is to identify the individual.

'Sensitive personal data' is defined in the GDPR as 'special categories of personal data' and its parameters have been expanded to include such categories as genetic data and biometric data where this is used to identify an individual person.

The new rules apply to both controllers and processors of data, as defined under the DPA – with the 'data controller' determining the purposes and manner in which data will be processed, and the 'data processor' being responsible for processing the data on behalf of the controller.

Under the GDPR, data processors will be specifically required to maintain records of personal data and processing activities and will have increased legal liability for any breaches. Meanwhile, data controllers will be under additional obligations to ensure that their contracts with processors are compliant with the GDPR. Certain types of data breach must also be reported to the relevant authority, under the new laws.

What does it mean for my business?

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 will be required to provide documentary evidence of their compliance with the GDPR.

Specifically, the new 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 new 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.

What action should I take?

It is important to prepare for the new regulations and introduce robust processes and controls, ahead of time. Failure to act could impact on your reputation and your bottom line, and the financial penalties for non-compliance are severe, with fines costing up to €20m or up to 4% of total annual worldwide revenue, whichever is the greater.

The arrival of the GDPR brings with it the need to adopt a forward-thinking approach to data protection, building in the appropriate privacy and security protections from the outset wherever possible when developing or using products or services that involve the use of personal data.

Businesses should take steps now to assess their readiness for the GDPR, allocating a sufficient budget and resources to examining their existing data sets and security processes, to identify and mitigate potential areas of risk.

Some of the main areas for action might include:

- ☑ Making sure members of staff are aware of the new 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 a new protection for children's data and the reduced 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.**

With stringent new regulations approaching, businesses are advised to review their data privacy and security practices, identifying areas of risk and introducing robust processes and controls, ahead of time. This will not only help to ensure that you are compliant, but will also help to improve your business's efficiency and engender loyalty and engagement amongst your customers.

This information is for general guidance only. Professional advice should be sought before taking or refraining from any action.