What businesses need to know about the General Data Protection Regulation

Our current data protection laws first came into effect 20 years ago, and there has been a huge change in technologies and data usage since then. There is also a strong drive to have common data protection laws across the EU due to the increased globalisation of business.

Therefore, the law needed to be updated. The General Data Protection Regulation (GDPR), an EU regulation, was implemented on 25 May 2018.

This fact sheet is designed to give you an overview of GDPR and the key changes that it has brought about for businesses.

What is GDPR?

GDPR set out to update and modernise data protection law in Europe and, indirectly, across the globe.

Although, the UK has voted to leave the EU, the UK is bound by GDPR until the date of departure and potentially throughout any implementation period (if one is agreed). It is envisaged that post-Brexit, many businesses will still be bound by GDPR as they are likely to still be needing to process data that has originated in an EU country. It is also important to note that the UK's Data Protection Act 2018 encompasses many of the key principles of GDPR and will remain in force regardless of the UK's status in Europe.

Leading up to the implementation of GDPR the Information Commissioner's Office (ICO) issued guidance which reassured businesses that if they were complying properly with UK data protection legislation, then they had a good starting point for GDPR, as the privacy principles essentially remained the same. However GDPR did introduce new concepts and powers, which we look at below.

What were the key changes introduced by GDPR?

- **Increased enforcement powers – prior to the introduction of GDPR,** the maximum fine for a data breach in the UK was £500,000. GDPR l significantly increased the maximum fines and the ICO now has authority to impose fines on data controllers and data processors on a two-tier basis, as follows:
    - up to 2% of annual worldwide turnover of the preceding financial year or €10 million (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default.
    - up to 4% of annual worldwide turnover of the preceding financial year or €20 million (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects' rights and international data transfers.
- **Data processors –** prior to the introduction of GDPR, data protection laws in the UK did not apply to data processors, but GDPR introduced direct rules which cover them. Whilst the law is still mainly focused on data controllers, there are new accountability obligations for data processors. These include keeping records of data processed, designating a data protection officer where required and notifying the data controller where there has been a breach. Article 28(3) of GDPR also sets out extensive provisions which must be included in a contract with a data processor.
- **Privacy impact assessments** – under GDPR businesses are required to carry out data protection impact assessments when implementing any processes that use new technology that is likely to result in a high risk to data subjects.
- **Privacy by design -** businesses must take data protection requirements into account from the inception of any new technology, product or service that involves the processing of personal data, with an ongoing requirement to keep those measures up-to-date.
- **Appointment of Data Protection Officer (DPO) -** certain businesses are required to appoint a DPO.
- **Subject access requests** a business is now required to respond to a data subject access request within one month from the date of receipt of the request. You will need to provide more information than formerly required (such as your data retention period and the right to have inaccurate information corrected) and you will not be able to charge for this.
- **Consent -** GDPR requires a very high standard of consent. It says that consent must be given by a clear affirmative action, establishing a freely given, specific, informed, unambiguous indication of the individual's agreement to their personal data being processed. This means that consent can no longer be inferred from silence, pre-ticked boxes or inactivity.
- **Privacy notice -** under GDPR, additional wording must be included in your privacy notice to include the legal basis for processing the data and your data retention periods. Such information must be concise and comprehensible.
- **Right to be forgotten -** individuals now have the right to request that businesses delete their personal data in certain circumstances.
- **Extra-territoriality -** GDPR applies whether or not you are located in an EU country. It applies if you offer goods and services to EU residents (whether or not you require payment), or if you monitor behaviour of EU residents.
- **Notification -** the notification process has been removed. There is instead an obligation on the data controller and the data processor to maintain certain detailed documentation.

- **Data breaches must be notified -** GDPR introduced a requirement to report data security breaches without undue delay and where feasible within 72 hours.

- **Article 27** - Article 27 of the GDPR requires that an organisation located outside the EU which is offering goods or services to individuals in the EU, or monitoring their behaviour and processing their personal data for those purposes will need to appoint a representative in the EU. The function of the representative is to hold records of data processing activity, to act on the organisation's behalf in relation to data protection matters in the EU and to act as the first port of call for EU supervisory authorities or as a portal for the receipt of data subject access requests.

What businesses need to know about the General Data Protection Regulation

Advice and support

We can help ensure your business is GDPR compliant.

We can advise on whether your existing consents to process personal data can be relied upon under GDPR. We can review your privacy notices to see if they comply with the GDPR requirements and can review your contracts with data processors to ensure that they include all of the provisions as required by GDPR.

Article 27 Representative

With offices in Dublin and Geneva, our affiliate company Willans Data Protection Services can act as your Article 27 Representative within the EU.

GDPR training

We can provide you with bespoke training solutions to suit your business needs. This can be delivered face-to-face or via webinar or an online platform such as Skype.

Disclaimer: This is a guide only and does not constitute legal advice. Specific advice should be sought for each case; we cannot be held responsible for any action (or decision not to take action) made in reliance upon the content of this publication.

Contact

Please contact one of the lead lawyers in our data privacy team:

Matthew Clayton matthew.clayton@willans.co.uk

Kym Fletcher kym.fletcher@willans.co.uk

Willans LLP | solicitors
28 Imperial Square, Cheltenham
Gloucestershire GL50 1RH, UK

+44 (0)1242 514000
www.willans.co.uk
Twitter @WillansLLP
LinkedIn WillansLLP