General Data Protection Regulation

A simple guide

Following three years of deliberation, in April 2016 the European Parliament and European Council finally adopted the approved General Data Protection Regulation (GDPR).

The GDPR will replace the current Data Protection Directive (which was incorporated into English law as the Data Protection Act 1998) and will deal with the protection of individuals regarding the processing of their personal data, as well as the free movement of that data. As it does not require the implementation of national legislation, it is expected to come into force in all EU member states during the first half of 2018.

How long the UK will continue to be in the EU is currently uncertain as a result of the Brexit vote but, based on the expected timescales for exit, it is likely that the UK will still be a member of the EU when the GDPR comes into force in 2018.

This guidance note provides information on some of the key talking points that your organisation will need to know regarding the new legislation.

Territorial Scope

One of the most significant changes introduced by the GDPR relates to the territorial scope of the legislation, and in particular concerns data controllers (who make decisions about how to use personal data) and data processors (who carry out those decisions) based outside of the EU.

Under the current Directive, only data controllers based within EU member states have to be concerned by the legislation. In contrast, the GDPR will apply to both data controllers and data processors operating outside of EU member states, provided that any data processing activities which they carry out either relate to the offering of goods or services to EU residents or the monitoring of the behaviour of data subjects within the EU.

The GDPR states that in determining whether a non EU organisation is offering goods to data subjects inside the EU, for the purposes of the legislation, the following should be taken into consideration:

- whether the business is offering goods or services in a language or currency of a member state
- whether the business is allowing EU citizens to place orders in the language of that member state
- whether the business is referring to EU customers in its publications.

This increased territorial scope is likely to affect non-EU online companies if they process the data of EU customers during the course of a sale or in situations where online providers use cookies or tracking devices on equipment used by EU citizens.

Consent

The current regime under the Directive allows data controllers to process data provided they have the express or implied consent of the data subject. It may also be allowed if any processing is deemed to be required for the 'legitimate interests' of the controller and if the processing of the data will not harm the data subject.

In contrast, the GDPR requires that data subjects must expressly consent to the processing of their data and that any consent must be 'freely given, informed, specific and unambiguous'. In relation to sensitive data any consent must be 'explicit' and this consent can be withdrawn at any time. It should be noted that the data controller must also be able to show that consent was granted by the data subject. As a general principle this means that any consent given requires a clear statement of intent or affirmative action from the data subject, it should not be merely implied by the conduct of the individual.

Additionally it is worth noting that parental consent will be required for the processing of any personal data relating to children under the age of 16. EU member states will be able to lower this age limit to 13 at their own discretion.

Cripps LLP
Number 22
Mount Ephraim
Tunbridge Wells
Kent TN4 8AS

T +44 (0)1892 515 121
F +44 (0)1892 544 878
E contact@cripps.co.uk
DX 3954 Tunbridge Wells

Data Processors

The current Directive only regulates data controllers and not data processors.

However, the GDPR places direct obligations on data processors such as implementing appropriate security standards, appointing a data protection officer and notifying the data controller of data breaches without undue delay.

Notification of data breaches

The GDPR places obligations on data controllers to notify the majority of data breaches to the national data protection authority (which in the UK is the Information Commission's Office (ICO)). In particular, the new legislation requires the data controller to notify any breaches without 'undue delay' and in all cases within 24 hours of becoming aware of any breaches. As a direct result of this requirement, controllers will have to have continuous monitoring and reporting systems in place at all times in order to avoid breaching the GDPR.

Although this obligation may appear onerous, many sectors already have legal obligations to report such breaches and the ICO already expects data controllers to report any 'serious breaches' that arise.

In the case of data loss or security breaches which are deemed sufficient to adversely affect the data subject's privacy or personal data, any such breaches must be reported to the data subject without undue delay, unless the controller can show that the data is unintelligible to third parties.

Removal of notification obligations

The GDPR removes the obligation for data controllers to notify or gain the approval from the ICO (or other relevant data protection authority) in certain circumstances. This appears to have been introduced in order to cut out much of the unnecessary administrative and financial work placed on data controllers in having to liaise with the national data protection authority.

However, the legislation will now require data controllers to put into effect certain procedures and mechanisms when working with new potentially high risk technologies. Additionally, there is a requirement for controllers to carry out a data protection impact assessment to determine the likelihood of risk when dealing with large scale processing.

The right to be forgotten

Individuals under the GDPR will be able request for the deletion of their personal data in certain specified circumstances. This will apply when the data is no longer required for the purpose for which it was originally collected or in circumstances where it has been unlawfully processed.

There is also an obligation for the controller to take all reasonable steps to inform third parties, to whom the data may have been disclosed, that the data subject has requested the deletion of information (the so called 'right to be forgotten').

Exceptions to the right to be forgotten will remain in place such as if there is an overriding justification to maintain the processing of data, such as a legal obligation to retain certain records.

Data Protection Officer

The GDPR requires any data controllers and data processors to appoint a dedicated data protection officer (DPO) as part of its accountability programme, if the organisation:

- is a public body or authority;
- if the core activities of the controller or processor consist of processing which requires regular and systematic monitoring of data on a large scale; or
- if the core activities involve large scale processing of sensitive data.

The DPO must be able to act independently of the organisation and is required to report directly to management. They should be selected on the basis of their professional capability and should have sufficient expert knowledge depending on the type of processing activities for which the DPO will be responsible.

Sanctions

The new legislation provides national data protection authorities the right to impose fines of up to 4% of an organisation's worldwide turnover for certain breaches of the GDPR such as failing to comply with the requirements for consent.

Additionally other specified offences can potentially result in a fine of up to 2% of worldwide turnover. The relevant data protection authority (DPA) will take into account various factors in determining a fine such as the nature, gravity and duration of any offence.

International Data Transfers

The current system has effectively been carried across from the Directive, albeit with some improvements.

This means that any personal data should not be transferred outside of the EEA unless there are appropriate safeguards in place. These might include using an approved mechanism for any proposed data transfer such as DPA approved contracts or making sure that the destination jurisdiction is deemed safe by the European Commission.

It should be noted that the GDPR removes self-assessment as a valid mechanism for transfer. Additionally, data exporters relying on consent to move data outside the EU will now have to be certain that any data subjects have been informed of the potential risks of the transfer.

The GDPR however does provide that a transfer can take place provided it is in the legitimate interests of the data controller, it is not repetitive and it only affects a small number of data subjects. Additionally, the controller must assess the transfer and deem that it has legitimate 'compelling' interests that are not outweighed by the interests of the rights of the data subject.

Binding Corporate Rules (BCRs)

For the first time, the GDPR provides recognition to the role of BCRs. BCRs are a set of legally binding corporate rules approved by a data protection authority that allow groups of companies to make intra-organisational transfers of personal data (including to offices based outside of the EEA).

The GDPR requires national data protection authorities to recognise BCRs approved by any other authority provided that they are:

- legally binding and enforced by each member of the group;
- legally binding on employees of the corporate group; and
- give enforceable rights to data subjects.

It is likely that the use of BCRs will increase as a result of the GDPR.

One-stop-shop

The GDPR also introduces the concept of a 'one-stop-shop'. Businesses which are established in multiple EU states will be able to nominate a single national data protection authority to act as the lead regulator for all of that organisation's data protection compliance issues in the EU.

This should limit the administrative burden for organisations based in multiple countries, which otherwise would have had to interact with a different DPA in each member state they operate in.

What can my organisation do to prepare for the new legislation?

Although the legislation has been agreed, it is not expected to come into force until mid-2018. However, many UK organisations will be required to significantly alter their existing data protection practices in order to ensure compliance with the new provisions.

We would encourage any organisations to begin preparing for the upcoming changes now, as depending on the size or complexity of your business, it could have significant budget, governance and communication implications. Notably the ICO states that due to the complexity of the new regime, compliance will be difficult if it is left to the last moment.

In response to the new legislation the ICO has published a 12-step checklist providing guidance on preparing for the GDPR which highlights aspects of the GDPR that are expected to have the most significant impact. The guidance can be accessed by visiting the following link: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

Contact Us

For more information about the GDPR or other data protection concerns, please contact your usual Cripps adviser or:

Irfan Baluch
Partner
T +44 (0)1732 224 006
irfan.baluch@cripps.co.uk