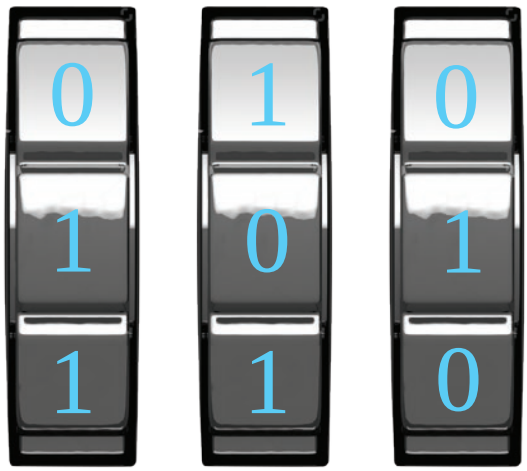
EVERSHEDS SUTHERLAND

Safe and sound

The General Data Protection Regulation ("GDPR")



The General Data Protection Regulation (2016/679) was initially published by the European Commission in January 2012 with the aim of harmonizing data protection legislation within the European Union. After four years of negotiation, it was finally adopted on 27 April 2016. Following a two year implementation period, the GDPR will come into force across the European Union on 25 May 2018 and it will replace national legislation which implements the existing Data Protection Directive 95/46/EC ("**Directive**").

Effect of the GDPR

The GDPR is set to be one of the most wide ranging pieces of legislation passed by the EU in recent times, however, it is important to note that the GDPR builds on familiar rules and principles, currently found within both the Directive and the Irish Data Protection Acts 1988 and 2003 (as amended) ("**Acts**").

The GDPR, therefore, aims to affect a change in organisations cultures and attitudes towards data protection generally. It is important for organisations not to fear the GDPR and to understand that many of the principles laid down by the current regime continue to apply under the GDPR. The increased onus of compliance introduced by the GDPR will no doubt impose a greater administrative burden on organisations and this coupled with greater sanctions highlights the need for organisations to ensure compliance.

Key Changes

1. Extra-Territorial Scope

Unlike the current regime, the GDPR extends the territorial reach of EU data protection law. It captures not only the processing of personal data by EU based data controllers and data processors which have EU establishments, but, it will also apply to all data controllers and data processors established outside of the EU but which offer goods or services to EU data subjects (even if for free) or which monitor the behaviour of EU data subjects, irrespective of whether the processing takes places in the EU or not. This highlights the fact that the GDPR will have a much broader impact than the current regime.

2. Accountability

The GDPR introduces the concept of accountability, which requires organisations to not only comply with the obligations of the GDPR but also to "demonstrate" such compliance. Organisations are required to keep detailed records of their processing activities and implement appropriate technological and organisational measures to ensure, and demonstrate, that the processing is carried out in accordance with the GDPR.

3. Data Processors

The GDPR introduces a new direct and specific statutory obligation on data processors in relation to accountability, co-operation with the supervisory authority, data security, data breach notifications and data protection officers. This will have a significant impact on organisations that are traditionally data processors. Organisations can expect more detailed contract terms regarding data protection generally including, in particular the appointment of sub-processors. Similar to data controllers, non-compliant data processors may also be subject to enforcement action under the GDPR.

4. Consent

The GDPR introduces a more prescriptive basis for consent. Under the GDPR, data subjects must freely give "specific, informed and unambiguous consent" to the processing of their data. The difference between consent and explicit consent is less clear, both now must be given by a statement or some form of clear affirmative action. The GDPR also requires that data subjects give additional consent for each additional processing operation. Furthermore, data subjects can withdraw their consent at any stage and it must be easy for them to do so.

5. Individuals' Rights

The GDPR creates some new rights for individuals and strengthens some of the existing rights, including the right to restrict processing, the right to data portability, and rights in relation to automated decision making and profiling. While data subject rights is not a novel concept under the GDPR, data subject will now have more control over the processing of their personal data. Data subject access requests can be made under the GDPR free of charge and will have to be responded to within a shorter timeframe, placing an even greater burden on organisations. In addition, a data subject access request can only be refused if it is manifestly unfounded or excessive.

6. Privacy Notices

The GDPR builds on the current fair processing requirements by increasing the amount of information that you must provide to data subjects when collecting their personal data, to ensure that such processing activities are fair and transparent. Organisations must provide the information in an easily accessible form, using clear and plain language.

7. Breach Notification

The GDPR introduces a mandatory data breach notification mechanism whereby data breaches must be notified by the data controller to the relevant data protection supervisory authority without undue delay and in any event within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects. If this risk is high, then data subjects must also be notified of the breach without undue delay. Practically, this will require companies to put in place a data breach policy. In addition, the GDPR now also places a positive obligation on data processors to notify data breaches to the data controller without undue delay.

8. International Data Transfers

The GDPR continues to impose restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

9. One Stop Shop

The GDPR introduces the concept of the "one stop shop" compliance framework. This framework is relevant to organisations who operate across many jurisdictions as such organisations will be predominantly regulated by the supervisory authority where they have their "main establishment".

10. Sanctions

The GDPR provides new and increased caps on the level of fines that supervisory authorities (i.e. the Data Protection Commissioner in Ireland) are permitted to impose against both data controllers and now also data processors. It also provides supervisory authorities with extensive powers to enforce compliance, including the power to impose significant fines. Organisations can face fines of up to €20m or 4% of their total worldwide annual turnover in the previous year. Supervisory authorities will have a discretion as to whether to impose a fine, and the level of that fine.

How we can help

Eversheds Sutherland are currently working with a large number of organisations to create a GDPR compliance roadmap which in turn enables organisations to be clear in relation to the steps that need to be taken in order to ensure GDPR compliance.

The key to success is to begin the process as early as possible in order to allow for a smooth transition.

We can help to educate you and your workforce in relation to who's data you hold, what data you hold, why you hold the data, how long you should retain the data for and where you are holding/storing the data.

For more information

For more information or advice in relation to compliance with the current data protection regime and/or the changes being introduced by the GDPR, please contact any member of the Eversheds Sutherland GDPR Implementation Team:

Marie McGinley
Partner, Head of IP, Technology and DP

T: *+353 1 6441 457*
mariemcginley@eversheds-sutherland.ie

Ciara McGrath
Solicitor

T: *+353 1 6644 336*
ciaramcgrath@eversheds-sutherland.ie

eversheds-sutherland.ie