TIERNEY IP

EUROPEAN INTELLECTUAL PROPERTY CONSULTANCY

European Union

General Data Protection Regulation

Implications for businesses which process data of persons within the European Union

On 25 May 2018, significant new obligations will be imposed on all businesses which process personal data of natural persons located within the European Union. The obligations are outlined in the European Union's 'General Data Protection Regulation 2016/679 (GDPR)' and will be automatically applicable in all current 28 Member States of the European Union.

Significantly, GDPR will have extra territorial effect and will therefore also apply to businesses outside the European Union which process personal data of EU based persons. This means that if a non-EU based business actively targets consumers in the European Union and, in the process, collects or monitors the behaviour of such consumers, it will have to ensure compliance with GDPR. Furthermore, non-EU based businesses which process personal data of EU based subjects will need to appoint a representative in the European Union to act as the link between them and the relevant Supervisory Authority in the Member State of the persons being targeted. Alternatively, if you target the EU in general, you can choose the Member State where you wish to base your representative.

Businesses in the European Union which handle and process personal data of natural persons of every nationality will also have to comply with the new requirements introduced under GDPR.

Obligations under GDPR

The new obligations under GDPR can be summarised as follows:

1. A data controller will be required to maintain documentation about how it processes and holds personal data.
2. Data controllers will be required to undertake data protection impact assessments in situations where processing of personal data is risky.
3. Implement data protection by design.

Requirement to appoint a Data Protection Officer

Many businesses will also need to appoint a Data Protection Officer who will need to demonstrate sufficient expert knowledge of the data protection law and the GDPR in particular. A Data Protection Officer can be an employee or an external contractor.

Those who process data within an organisation (Data Processor) will have to maintain a written record of all processing carried out at the request of a Data Controller.

Rules regarding data breaches.

The GDPR contains very strict provisions regarding notification of a data breach.

A Data Processor must notify a Data Controller on becoming aware of a data breach without delay. The Data Controller is then required to notify the Supervisory Authority of the EU Member State where it is based of the data breach within 72 hours. In some cases, data subjects will also have to be notified of breach.

Transfer of personal data outside of the European Economic Area

The GDPR also contains provisions regarding the transfer of personal data outside of the European Economic Area. For example, if an organisation transfers personal data outside of the EEA, data subjects will have to be informed of the transfer and the risks associated with it.

Requirement of Consent

A significant feature of GDPR will be a data subject's consent to the processing of his/her personal data.

The over-riding rule of GDPR is that a data subject should be able to withdraw consent to the processing of his/her date just as easily as giving consent in the first place. For sensitive data (e.g. medical), consent must be explicit.

If personal data is processed for purposes of direct marketing, the data subject will have the right to object. Furthermore, the right must be brought to the attention of the data subject.

In Ireland, the proposed Data Protection Bill 2018 to implement GDPR currently stipulates that parental consent will be required for the processing of data for children under the age of 13.

Breaches of GDPR

For breaches of the GDPR, there is provision for the imposition of significant fines. In the most serious cases, fines of up to 4% of worldwide turnover may be imposed.

A welcome feature of the GDPR is that individual cases of data protection breaches will be handled by the Supervisory Authority of where the undertaking has its main establishment. This is known as the 'One Stop Shop' rule. The GDPR however will facilitate Supervisory Authorities of the Member States where a complaint originated to work with the Supervisory Authority of the Member State where the undertaking has its main establishment.

While the GDPR has removed the requirement for undertakings to register with their local Supervisory Authority, significant power has been given to Supervisory Authorities to undertake audits, either on the basis of their own initiative, or as a result of a complaint.

It is also important to bear in mind that if an organisation's Data Impact Assessment reveals that processing personal data would result in significant risk of breach without corrective measures being

put in place, the relevant Supervisory Authority must be notified. The Supervisory Authority may use its enforcement powers to ensure compliance with GDPR.

Rights of data subjects

Data subjects will also have significant rights under GDPR. These include:-

A right to know about data being processed about themselves.

A right of access to data.

Correction of personal data which is incorrect.

A right to object to personal data being processed for purposes of direct marketing.

A right to obtain a file of personal data in structured and commonly used format.

As a result of a ruling by the Court of Justice of the European Union, a data subject will also have the right to be forgotten. This will allow data subjects to require businesses which hold their personal data to delete such data without delay. Data controllers in such cases will also have to inform third parties that the data subject has requested erasure of any links to, or copies of, the relevant data. Any request for the erasure of such personal data must be fulfilled within a month.

If you are a business which processes data of natural persons within the European Union, contact TIERNEY IP now for advice on how to prepare and implement procedures to ensure compliance with GDPR. Our Managing Director, Niall Tierney, is a qualified lawyer who has significant experience in advising businesses on matters of Data Protection law.

European Union, Personal Data, General Data Protection Regulation 2016/679, GDPR, Supervisory Authority, Member State, Data Controller, Data Protection Officer, Data Processor, European Economic Area, EEA, sensitive data, consent, parental consent, Data Protection Bill 2018, Data Impact Assessment, Right to be Forgotten, Court of Justice of the European Union, CJEU, ECJ, data protection law, TIERNEY, TIERNEY IP, data protection lawyer, privacy, privacy lawyer, transfers, adequacy decisions