

## Data Protection and Ireland

Ireland is a centre point of data protection law and policy in Europe, and our Data Protection Commission (DPC) is internationally respected. With Ireland home to the EMEA headquarters of some of the world's leading technology companies, the DPC plays a leading role in regulating GDPR compliance, and in helping businesses and consumers become more informed of their data protection obligations and rights.

### Why choose Irish law and Irish lawyers for enforcement of Data Protection law?

- Irish data protection legal practitioners offer world class experience in advising on the most complex and cutting-edge data protection issues. Over the last 20 years Ireland has established itself as the data capital of Europe; with an impressive array of leading technology companies serving the EMEA from Ireland; including Apple, Google, Microsoft, Facebook, LinkedIn, Twitter, and Airbnb, with many investing in substantial data centre infrastructure here.
- The EU General Data Protection Regulation (**GDPR**) applies in Ireland and protects the privacy of individuals with regard to the processing of their personal data. The Irish Data Protection Act 2018 gives further effect to the GDPR. The GDPR became applicable in Ireland (and across the EU) on 25 May 2018. It ensures that a uniform set of data protection rules applies across the EU. This makes it easier for multinational companies operating across the EU to comply with data protection law.
- In addition, the GDPR provides for a 'one stop shop'. While supervisory authorities in other EU Member States can be involved in certain cases, generally multinational companies are regulated by the data protection supervisory authority which is located in the EU Member State where they have their main establishment. This means that instead of having to deal with data protection supervisory authorities from each EU Member State in which they operate, multinational companies only have to deal with one lead supervisory authority.
- The GDPR has an extra-territorial scope. It applies to all data controllers and data processors in the EU, but also to those outside the EU, where they offer goods or services to, or monitor the behaviour of, EU data subjects. Like other EU data protection authorities, the DPC has the power to impose fines under the GDPR, of up to €20 million or 4% of an undertaking's global turnover of the preceding financial year.

## How does BREXIT impact on data protection?

Since 1 January 2021, the UK no longer applies the EU GDPR to the processing of personal data. Instead, a separate UK legal framework regarding data protection and privacy is in force in the UK.

**Data Transfers:** Whilst personal data can flow freely between Ireland and other EU/EEA Member States, the GDPR prohibits the transfer of personal data from the EU/EEA to third countries outside the EEA, unless that country benefits from an adequacy decision or the transfer is subject to appropriate safeguards or a GDPR derogation applies.

- For the purposes of the GDPR, the UK became a third country from 1 January 2021 and the European Commission granted an adequacy decision in respect of data transfers from the EU/EEA to the UK in June 2021. While the decision brought a degree of welcome legal certainty regarding EU-UK transfers, the adequacy decision includes a ‘sunset clause’, meaning that it will automatically expire after four years unless renewed. In addition, the European Commission is closely monitoring any divergence in UK data protection laws and policies from those in the EU and can revoke the decision at any point in the meantime.

Transfers of personal data from the UK to the EU/EEA can continue without additional safeguards. This is provided for in the UK Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, as amended.

**One Stop Shop:** As noted above, the one stop shop mechanism in the GDPR means that multinational companies only have to deal with their lead data protection supervisory authority, namely the supervisory authority where their main establishment is located in the EEA. As of 1 January 2021, the one stop shop mechanism no longer applies to the UK. This means that multinational companies whose main establishment is located in the UK are now subject to regulation by the data protection supervisory authority in each Member State in which they operate.

**EU/UK Representatives:** Multinational companies who are not established in the EU, but whose processing activities are subject to the application of the GDPR as they offer goods or services to or monitor the behavior of EU data subjects, are required to designate an EU representative. The EU representative may be addressed by data protection supervisory authorities and data subjects on all issues related to processing activities in order to ensure compliance with the GDPR. Similarly, multinational companies that are not established in the UK, but offer goods or services to or monitor the behaviour of UK data subjects, must appoint a UK representative.

The UK’s decision to leave the EU, and the single market, has caused parties to international contracts to consider a different choice of law and/or submission to jurisdiction clause. With the departure of the United Kingdom from the European Union, Ireland is now the

only member of the European Union that operates a court system that is both English speaking and based on the common law and the doctrine of precedent. At present, there is uncertainty as to whether judgments of English Courts will be easily enforceable in the EU. English Courts will not be able to make a reference to the Court of Justice of the European Union (CJEU).

