



TECHNOLOGY

GDPR: One Year On

by Jane O'Grady

GDPR: One Year On

24th May 2019 | by Jane O'Grady

On 25 May 2019 it will be one year since the General Data Protection Regulation (GDPR) came into force. This article considers its impact so far in Ireland, the EU and beyond.

Awareness

In the EU, the public are more aware than ever of their data protection rights and the obligations of those who process their personal data. According to a recent European Commission survey, 67% of EU citizens have heard of the GDPR and 57% are aware of the existence of a data protection supervisory authority in their own country. This increased awareness is reflected in the volume of communications that EU supervisory authorities have received from data subjects since the GDPR came into force. According to the European Data Protection Board (EDPB), over 144,000 queries and complaints and over 89,000 data breach notifications have been made to EU supervisory authorities since May 2018.

The GDPR has also paved the way for the introduction of enhanced data protection legislation beyond the EU. Brazil, Japan, the state of California and a number of other jurisdictions have introduced, or are considering the introduction of, GDPR-like data protection measures. It is clear that the introduction of the GDPR marked the beginning of a new age of enhanced data protection rights and obligations, and increased public awareness of those rights and obligations, around the globe.

Cooperation and Consistency

The EDPB promotes cooperation between EU supervisory authorities and maintains consistency in the application of data protection law throughout the EU. Established under the GDPR, the EDPB replaced the Article 29 Working Party (WP29) and is comprised of representatives from each EU supervisory authority and the European Data Protection Supervisor. In the past year, the EDPB has endorsed a number of the WP29's data protection guidelines, and has itself adopted six further guidelines in relation to the GDPR.

The GDPR's "one-stop-shop" mechanism enables multinational companies, which engage in cross-border processing, to deal with the supervisory authority of their "main establishment", even where they have a number of establishments across the EU. According to the EDPB, 446 cross-border cases are currently logged in its cross-border case register, 205 of which have led to "one-stop-shop" procedures.

Enforcement

Enforcement under the GDPR is in its very early stages. Supervisory authorities throughout the EU are still dealing with the backlog of pre-GDPR issues, and investigations take time.

While the Irish Data Protection Commission (DPC) is conducting a number of statutory inquiries in respect of Irish established multinational technology companies (including its recently announced inquiry into Google Ireland's online Ad Exchange), it has yet to issue an administrative fine. The expectation is that more decisions and enforcement actions will be issued by supervisory authorities in 2019, as many ongoing investigations reach their conclusion. The most recent annual report published by the DPC stated that a number of inquiries concerning multinational technology companies' GDPR compliance "should reach the decision and adjudication stage later this year".

But there has been some significant enforcement in other jurisdictions.

In February 2019, the EDPB released its first 'GDPR overview'. In it, the EDPB noted that eleven supervisory authorities had issued administrative fines under the GDPR, totalling €55,955,871. The majority of this total relates to the massive €50 million fine issued to Google in January 2019 by the CNIL, in France. This fine is expected to be appealed.

The Dutch supervisory authority, Autoriteit Persoonsgegevens, published its GDPR fining policy on 14 March 2019, and is the first supervisory authority to do so. The policy categorises fines into 4 tiers, and identifies base fines within each category which can then be increased or decreased within the category band based on the nature, seriousness and duration of the breach. It is unclear whether other national supervisory authorities will follow suit with their own fining policies, but the introduction of the Dutch policy certainly indicates that further fines are on the way.

Compensation

Any person who suffers material or non-material damage as a result of infringement of the GDPR has a right to receive compensation from the controller or processor for the damage suffered. The introduction of the right to compensation for non-material damage (e.g. emotional distress) was a significant departure from the Irish pre-GDPR regime. However, the development in Irish law in relation to non-material damage under the GDPR is in its infancy. Important issues need to be clarified such as a consistent view on what constitutes non-material damage (this is not defined in the GDPR or the Data Protection Act 2018) and how non-material damages should be quantified.

International Transfers

Under the GDPR, the personal data of EU data subjects can only be transferred outside the EEA where a lawful transfer mechanism is in place. The ongoing Schrems II action threatens the validity of one such transfer mechanism, the European Commission approved standard contractual clauses (SCCs).

Following a complaint made by Max Schrems about Facebook's use of SCCs to legitimise the transfer of personal data from the EU to the United States, the DPC commenced proceedings in the Irish High Court. In October 2017, the High Court delivered its judgment in the proceedings, holding that certain issues regarding the validity of SCCs under EU law should be referred to the Court of Justice of the European Union (CJEU). In April 2018, Facebook applied for a stay on the reference to the CJEU pending its appeal against the High Court's decision to make the reference. This application was refused by the Court. In May, Facebook applied for leave to appeal to the Supreme Court in relation to both the High Court's reference to the CJEU and the refusal of its application for a stay on that reference. The Supreme Court granted leave to bring the appeal, which was heard in January 2019.

The Supreme Court's judgment on this is eagerly anticipated. Until that time, the High Court's reference remains pending before the CJEU.

Business compliance

While businesses invested heavily in the advent of GDPR, and in the proceeding months, to implement new privacy notices, processing contracts and internal procedures, one must remember that compliance is an ongoing requirement. The principle of accountability, introduced by the GDPR, means that those measures must be monitored and enforced. Also, policies and procedures implemented last year may no longer fully reflect a business's current processing activities. Whilst some businesses may be suffering from "GDPR fatigue", compliance has moved on from a simple check-box exercise and therefore one must be willing to reviewing their measures and enhancing them when necessary.

Conclusion

In its first year in force, the GDPR has seen record levels of awareness and engagement with data protection issues at an EU and global level. During the next year, one can expect supervisory authorities to make greater use of their enforcement powers, with the issuance of more and greater administrative fines, coupled with the inevitable challenges to those fines which will follow.

If you would like to know more on any of the above issues, or advice on your on-going GDPR compliance measures, please contact a member of our IP/IT team.

About the Authors



Jane O'Grady
Partner

Jane is dual qualified as a solicitor and a trade mark and design attorney, with many years' experience advising on commercial contracts, intellectual property, commercial agency and all aspects of technology law.

T: +353 1 637 1554 E: jogrady@lkshields.ie