GDPR in Context: Remedies and Sanctions

Background

The General Data Protection Regulation (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

Overview

The GDPR takes a multi-layered approach to remedies and sanctions for breach of its provisions, and while setting out the high level principles and maximum administrative fine amounts, leaves some latitude to the EU member states as to how the remedies and sanctions regime will operate in practice.

At a principles level, EU member states are required to provide effective judicial remedies against both the legally binding decisions of that EU member state's supervisory authority, and against data controllers and data processors in the case of breach of the GDPR.

In the case of proceedings against data controllers and data processors, proceedings may be taken either where the data controller or data processor has its establishment or in the place of habitual residence of the complainant data subject. Individuals also have the right to be represented by public interest bodies and not-for profits.

Individual remedies against data controllers and data processors

Individuals have the right to lodge complaints directly with the supervisory authority in respect of infringement of the GDPR by either data controllers or data processors, and have the right to compensation for damage suffered arising in respect of both material and non-material damage (which differs from current case law in Ireland, where pecuniary loss has to be shown).

Data controllers are liable for damage caused by processing which infringes the GDPR. Data processors, on the other hand, are liable only where they have not complied with obligations specifically directed at them under the GDPR, or have acted outside of or contrary to lawful instructions from the data controller. In general, data processors have fewer obligations under the GDPR than data controllers (although more than currently apply to data processors). Those obligations include the implementation of appropriate technical and organisational measures ensuring appropriate security, compliance with data controller instructions, and documenting and recording of processing activities.

Data controllers and data processors may only escape liability for where they prove they are not 'in any way' responsible for the event giving rise to the damage. This is combined with a "joint and several" style provision, which holds each involved data controller and data processor liable for the entire damage caused by the processing, in order to ensure effective compensation of the data subject, although any controller or processor which has paid the full amount of compensation is then entitled to claim back from the others involved for their corresponding part in the damage.

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Remedies and Sanctions

Administrative sanctions against data controllers and data processors

Separately, there is an administrative fines regime outlined in the GDPR, with the requirement, again, that the sanctions be effective, proportionate and dissuasive.

The level of potential sanction will depend on the breach, and will range from fines of up to €10 million or 2% of total worldwide annual turnover in the previous financial year (for breach of principles such as "*by design and by default*", non-compliance with the processing related obligations, or failure to appoint a Data Protection Officer) to fines of up to €20 million or 4% of total worldwide annual turnover in the previous financial year (for breaches including breaches of the principles relating to processing or of the lawful processing requirements, and for breach of data subject rights).

A summary of the administrative fines associated with breaches of various GDPR articles is set out here:

Administrative Sanctions	**Relevant Articles of GDPR**
Up to €10 million or 2% of total worldwide annual turnover in the previous financial year	Article 8 (Conditions applicable to a child's consent in relation to information society services)
	Article 11 (Processing which does not require identification)
	Article 25 (Data protection by design and by default)
	Article 26 (Joint controllers)
	Article 27 (Representatives of controllers or processors not established in the Union)
	Article 28 (Processor)
	Article 29 (Processing under the authority of the controller or processor)
	Article 30 (Records of processing activities)
	Article 31 (Cooperation with the supervisory authority)
	Article 32 (Security of processing)
	Article 33 (Notification of a personal data breach to the supervisory authority)
	Article 34 (Communication of a personal data breach to the data subject)
	Article 35 (Data protection impact assessment)
	Article 36 (Prior consultation)
	Article 37 (Designation of the data protection officer)
	Article 38 (Position of the data protection officer)
	Article 39 (Tasks of the data protection officer)
	Article 42 (Certification)
	Article 43 (Certification bodies)

Remedies and Sanctions

Administrative Sanctions	Relevant Articles of GDPR
Up to €20 million or 4% of total worldwide annual turnover in the previous financial year	Article 5 (Principles relating to processing of personal data)
	Article 6 (Lawfulness of processing)
	Article 7 (Conditions for consent)
	Article 9 (Processing of special categories of personal data)
	Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)
	Article 13 (Information to be provided where personal data are collected from the data subject)
	Article 14 (Information to be provided where personal data have not been collected from the data subject)
	Article 15 (Right of access by the data subject)
	Article 16 (Right to rectification)
	Article 17 (Right to erasure ('right to be forgotten'))
	Article 18 (Right to restriction of processing)
	Article 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing)
	Article 20 (Right to data portability)
	Article 21 (Right to object)
	Article 22 (Automated individual decision making, including profiling)
	Articles 44 - 49 (Transfers of personal data to third countries or international organisations)
	Infringements of obligations under Member State law adopted under Chapter IX (Provisions relating to specific processing situations)
	Non-compliance with access in violation of Articles 58(1) and of orders under Article 58(2) (Article 58 sets out the powers of the supervisory authorities)

The administrative sanction regime does not impose liability on a strict liability basis, but will require a case by case assessment of the circumstances of each individual infringement, taking into account factors such as the nature, gravity and duration of the infringement, the intentional or negligent nature of same, any damage mitigation steps which have been implemented, the technical and organisational (ie security) measures which had been implemented, and how the supervisory authority became aware of the issue.

The GDPR also refers to a third level of 'penalties' (which again must be effective, proportionate and dissuasive), in particular for infringements of the GDPR which are not subject to administrative fines. When read in combination with some of the recitals to the GDPR, they point to an expectation that EU member states would implement a criminal sanctions regime for some breaches.

Role of the European Data Protection Board

Under the GDPR, the European Data Protection Board (the "**EDPB**") is given certain powers in relation to monitoring and ensuring the correct application of the GDPR, including through is advisory remit and the power to issue guidelines, recommendations and best practice procedures on various matters ("**EDPB guidance**"). Among its tasks is dispute resolution where there are disagreements on findings as between supervisory authorities, or as between the EDPB and a supervisory authority, with the EDPB having the ability to issue binding decisions in those circumstances. Those decisions are required to be provided to the relevant court in cases taken against supervisory authorities, but will also, together with EDPB guidance, be of relevance in civil actions and in assessing the level of administrative fines in appropriate cases.

Remedies and Sanctions

Next steps

The significant strengthening of data protection rules which is inherent in the GDPR, and in particular the sanctions under the GDPR, emphasise the need to ensure that each organisation has full insight into the data flows concerning customer data and other personal data which it controls, and that it puts appropriate notifications, processing agreements, transfer arrangements and security arrangements in place.

The starting point for any GDPR compliance project is therefore an understanding of the "*what, why, how and where*" of current personal data processing by each organisation, and where appropriate by department or business line within the organisation. What personal data is held and used, why the organisation needs and uses it (which may not necessarily be the same thing), how the personal data is processed and shared, where it is stored and from where it is accessed – all of these are important questions to be answered before it will be possible to undertake the necessary gap analysis.

Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com

12.10.17