GDPR in Context: Data Processor Accountability

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 introduces additional statutory compliance obligations directly on processors by expanding on their current obligations, and provides that a processor will be directly liable to data subjects where it does not comply with its obligations or acts outside instructions of the controller, and may be subject to direct enforcement by supervisory authorities, fines for non-compliance, and compensation claims by data subjects for any damage caused by breaching the GDPR.

Privacy by design and by default

The GDPR puts personal data protection front and centre as a fundamental right of the individual, and introduces the concept of data privacy "by design and by default", which is in effect a recasting of the data protection principles and security obligations under the current EU Data Protection Directive (which has been implemented into Irish law through the Data Protection Acts 1988 and 2003 (the "**DPA**")). Allied to the by design and by default theme, is an emphasis on transparency and accountability as fundamental GDPR concepts, necessitating that compliance with the relevant requirements be demonstrable. Accordingly, the GDPR imposes new requirements relating to the analysis and documenting of data processing activities as part of efforts to ensure both controllers and processors are accountable for and can demonstrate compliance with their respective obligations under the GDPR.

Identifying the processor

As is currently the case, identification of the controller of personal data (ie, the entity which determines the purposes and means of the processing) will ultimately be a question of fact, with the possibility that two or more entities might be joint controllers of the data, or separate controllers (for different purposes) of the same, or subsets of the, data. From the perspective of organisations which view themselves as processors, it is important to note that the GDPR specifies that where a processor infringes the GDPR by determining the purposes and means of processing, it will be treated as a data controller in respect of that processing. Having established that a particular organisation is intended to be a processer rather than a controller, it will be important for that organisation to have a clear definition of its remit with regard to the processing of the personal data in question, and to remain with the parameters of the agreed scope.

The increased requirements relating to processing contracts may prove of assistance in that regard, and processors should not process outside the scope of the relevant contract to avoid a risk of being deemed a controller.

[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.

Data Processor Accountability

Data processor obligations

Among the key processor obligations and impacts which processors need to consider are:

- the continuing obligation to process only on the documented **instructions** of the controller, but combined with the express statement under the GDPR that a processor which does not comply with the instructions of its controller, and independently makes determinations about the means and purposes of the processing, will be considered to be a controller in respect of that processing activity;
- the additional **contractual undertakings** to which processors must agree, as outlined below;
- the prohibition on the appointment of **sub-processors** absent specific or general written authorisation from the controller, and the requirement that any sub-processing agreements contain the same data protection obligations that are imposed on the lead processor by the controller. The requisite provisions are required to be reflected in the contracts throughout any chain outsourcings;
- the obligation, in most circumstances, to maintain **records** of all categories of processing activities which must contain details of the name and contact details of the processor, controller by controller details and the categories of processing, any transfers of personal data abroad, including documentation of suitable safeguards, and where possible, a general description of the technical and organisational security measures applied to the processing activities;
- the obligation to **cooperate** with the supervisory authorities;
- the obligation to notify controllers of a **data breach** without "undue delay" after becoming aware of it;
- the clear application of the **prohibition on transfers** outside the European Economic Area to processors, combined with a clear statement that only the European Commission may determine whether a third country or international organisation ensures an adequate standard of data protection.

  Organisations will still be able to rely on model clauses as a valid means of transfer and the GDPR provides a list of other valid transfer mechanisms, including the potential for approved codes of conduct and certification mechanisms, provided there are binding and enforceable commitments of the controller or processor in the third country. Helpfully, the GDPR also mentions the possibility of model clauses between data processors, which do not exist at present. The GDPR also specifically sets out clear provisions on requirements and procedures in relation to BCRs for the first time, which may simplify the current lengthy approval process with data protection authorities;
- the requirement to undertake pre-processing data protection or privacy impact assessments ("**PIAs**"), if the processing is likely to result in a high risk to an individual's rights, and which may require pre-processing consultation with the relevant supervisory authority. Such high risk processing includes profiling, large scale processing of sensitive categories of personal data, and may arise where there is innovative use of technological solutions.

  In addition, transfers of personal data outside the European Economic Area ("**EEA**"), while not specified in the GDPR as high risk per se, have been identified by the Article 29 Working Party as amongst the factors which may be indicative of high risk. Whether a PIA may be required will therefore be a relevant consideration in the context of any offshore outsourcings by service providers; and

Data Processor Accountability

- the potential requirement to appoint a data protection officer ("**DPO**"), inter alia, where the processing: (i) requires regular and systematic monitoring of data subjects on a large scale; or (ii) involves processing large amounts of sensitive data or personal data relating to criminal convictions and offences.

  Organisations are free to appoint DPOs even if not required to do so under the GDPR, but if they chose to do so, all DPO related provisions in the GDPR will apply.

Data processing agreements

As is currently the case, there is an express requirement under the GDPR that a written agreement be put in place between a controller and processor. This does not have to be a separate and specific processing agreement dealing exclusively with data processing activities, and the requisite provisions are generally embedded into the relevant services contract (eg, the administration agreement). However, the GDPR significantly expands the mandatory content of processing agreements, to include:

- a description of the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data and categories of data subjects; and the obligations and rights of the controller;
- contractual provisions obliging the processor to:
- not process other than on documented instructions, including with regard to transfers to a third country, or where required to do so by EU or EU member state law, to inform the controller in advance (unless prohibited);
- ensure that persons authorised to process have committed, or are subject under statute, to confidentiality obligations;
- comply with appropriate technical and organisational security measures, which may include encryption, pseudonymisation or other technical measures;
- comply with the sub-processing restrictions;
- assist the controller, by appropriate technical and organisational measures, insofar as possible, to comply with the controller's obligations with regard to data subject rights;
- assist the controller in complying with its obligations relating to security, notification of breaches and PIAs;
- at the controller's request, return or delete personal data when the agreement terminates; and
- provide the controller with all information necessary to demonstrate compliance with the processor related obligations in the GDPR and allow for and contribute to audits and inspections by the controller or its mandated auditor.

While processing agreements have tended, in more recent years, to include a broader range of processing obligations than those currently mandated under the DPA, including eg, in relation to breach notification assistance, it is unlikely that all current processing agreements will include all of the above requirements, and both controllers and processors will need to review and revise all relevant agreements between now and 25 May 2018.

Data Processor Accountability

Data processor liability

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 or contrary to lawful instructions from the data controller.

Data controllers and data processors may only escape liability 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. Separately, there is an administrative fines regime outlined in the GDPR, with the level of potential sanctions will depending on the breach. Sanctions 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 DPO) 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).

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. At a minimum, for processors, this will require a review in advance of 25 May 2018 of all processing activities, to ensure that the organisation is not overstepping its remit as processor, all associated processing agreements and data transfer agreements, and internal procedures and controls, to enable the processor to demonstrate compliance with its obligations under GDPR.

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