GDPR in Context: Data Subject Rights

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.

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.[1]

Overview of individual rights

The GDPR extends a number of existing individual rights which individuals can exercise against controllers, as well as introducing a number of new rights. The focus on individual rights, and on the transparency and accountability principles which underpin all of the GDPR, put individuals and their rights at the heart of the GDPR. Controllers will need to consider all aspects of their processing activities in light of the rights afforded to individuals, so that they will ultimately be in a position to demonstrate compliance not only when individuals seek to exercise those rights, but with their overall obligations under the GDPR.

Right of access

An individual has continuing rights under the GDPR to establish whether a controller processes information relating to him / her, and to access and obtain a copy of that data and certain additional information in relation to the processing, such as its purposes, the categories of data, the recipients of the data, and the existence of additional rights such as the rights to erasure and objection. As is the case currently, the exercise by an individual of his / her access rights cannot prejudice the rights and freedoms of other individuals, and the right of access is not an absolute right

[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 Subject Rights

Right to be forgotten

The right to have personal data rectified, blocked or erased already exists under existing data protection rules. However, enforcing those rights involves a relatively high threshold for individuals, and requires a demonstration that the data controller has contravened data protection principles. Partly as a result of the *Google Spain* decision of the Court of Justice of the European Union, however, there has been much more emphasis on the right of erasure or "the right to be forgotten", and this focus is reflected in the provisions of the GDPR.

Under the GDPR, every individual has the right to have his / her data erased, or the "right to be forgotten", in circumstances where:

- the data is no longer necessary for the purpose for which they were collected;
- processing is based on consent, but the individual has withdrawn consent and there is no other legal ground for continued processing available to the controller;
- an individual has exercised his / her right to object, and there is no overriding legitimate interest on which the controller can continue to legitimise its processing;
- the data is unlawfully processed;
- the erasure is required by a law applicable to the controller; or
- the data was collected in connection with the offer of information society services to a child.

Taking account of available technology and the cost of implementation, the controller is required to take reasonable steps, including technical means, to inform other controllers processing the data that the individual has requested erasure of links to, or copies or replication of, the data.

The right, however, is not an absolute right, and a controller will be in a position to continue processing the data on the basis of freedom of expression and information, where the controller is required to comply with the legal obligation which requires processing (bearing in mind that this has to arise under EU or member state laws), or if the processing is required to establish, exercise or defend legal claims.

Right to restrict processing

Individuals have the right to require that a controller restricts its processing of his / her data in some circumstances, including where the data is inaccurate (for the period during which the controller is verifying the data), the data is no longer required in light of the purposes of the processing but the individual requires the data in connection with legal claims, or the data subject has exercised his / her right to object (pending verification of any legitimate grounds of the controller which override those of the data subject).

Data Subject Rights

Right to object

As with the right to be forgotten, the right to object to processing already exists in connection with eg, direct marketing or processing based on a legitimate purpose of the controller, where an individual has the right to object to the processing for specified purposes or in a specified manner on the ground that, for specified reasons, it causes or is likely to cause unwarranted substantial damage or distress.

Under the GDPR, the existing right to object to processing continues, along with some clarifications and expansion. As is currently the case, any individual has the right to object to direct marketing at any time, and in that event, the controller must stop using the information for marketing purposes. However, an individual can also object where:

- retaining the data is no longer necessary for the purposes for which collected;
- consent has been withdrawn and there is no other legitimate ground for processing;
- processing is based on a public interest or a legitimate interest of the controller, in which case, unless there are overriding legitimate interests, the controller must cease the processing. In this regard, there is no longer any reference to their being "*unwarranted substantial damage or distress to the data subject*", and instead, controllers must take into account "*grounds relating to the data subjects particular situation*", which is a broader concept;
- the data has been unlawfully processed;
- erasure is required under a legal obligation to which the controller is subject under EU or member state law; or
- the data was collected in the context of the provision of information society services to a child.

Automated decision making and profiling

There is an existing right not to be subjected to processing which is wholly automated and which produces legal effects or otherwise which significantly affects an individual, and which is intended to evaluate certain personal matters, such as creditworthiness or performance at work, unless one of a limited number of exemptions applies.

Under the GDPR, individuals will continue to have the right not to be subject to decisions based solely on automated processing in a similar manner, with additional restrictions applying in relation to automated processing of special categories of data. Interestingly, the GDPR specifically references profiling, which is defined as "*any form of automated process to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

The exceptions to automated decision making are more narrowly drawn than under current rules. Whereas previously, such processing was permitted in the course of considering whether to enter into a contract, or with a view to entering into a contract or for the performance of a contract, under the GDPR, automated processing will only be permitted, in the context of contract, where it is a "*contractual necessity*". In addition, where a controller seeks to rely on consent, it must be explicit consent. In both cases, the controller is obliged to implement a minimum set of suitable safeguards, so "at least" the right to obtain human intervention, to express views and to contest the decision should be built into the process.

Data Subject Rights

Portability

The right to data portability is a new right introduced by the GDPR, and allows individuals to obtain and, importantly, reuse their personal data. A data subject can either obtain the data him / herself and, in turn, provide it to a third party (if he / she so wishes), or require the data controller to transfer the personal data directly to a third party. Please refer to our separate note on Data Portability for further information.

Restrictions

None of the individual rights under GDPR are intended to be an absolute right. In addition to the specific limitations set out in the GDPR, EU and member state law can provide for additional restrictions in certain circumstances, such as safeguarding of national and public security and defence or of criminal investigations and the enforcement of civil law claims, where those restrictions are necessary and proportionate measures in a democratic society. Further detail on the scope of the restrictions will await relevant national and EU legislation.

Compliance with individual requests

Individuals must be in a position to exercise their rights free of charge, and a controller obtaining a request in connection with an individual right must comply without undue delay, which means within one month, with a maximum two month extension depending on complexity and the number of requests. The GDPR does not mandate any particular means by which requests must be facilitated, but does indicate that controllers should provide means for electronic requests, in particular where the data is processed by electronic means.

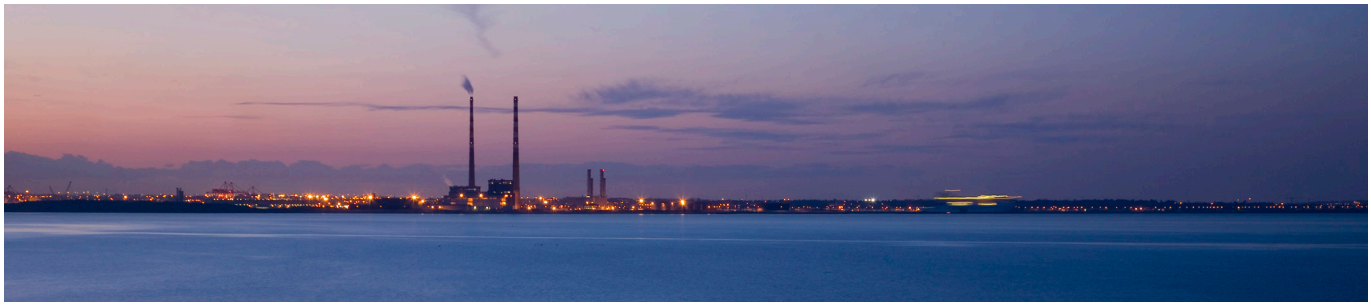
Transparency

The increased transparency required under the GDPR means that individuals are required to be clearly informed by the existence of their rights. In light of the burden of proof on controllers to demonstrate compliance, this will have an impact on notifications and privacy statements.

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.

Taking into account the additional and extended rights under the GDPR, data controllers will need to review their privacy policies and to ensure that appropriate disclosures are included. In that regard, the basis of processing, and the associated individual rights, need to be considered and identified, and specifically addressed in those policies. In relation to each of the individual rights set out in the GDPR, a data controller will also need to implement appropriate processes and procedures for managing requests from individuals within the specified timelines, and may need to consider system changes to implement revised procedures.



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