GDPR in Context: Data Portability

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.

Data Portability – an overview of a new data protection right

The GDPR introduces a new right of data portability, which 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.

This new right of portability is aimed at empowering consumers by facilitating ease of movement between service providers and increasing the ease of price comparison, and is part of a broader theme in the GDPR of giving data subjects more control over their data.

Application and scope of the portability right

The right of data portability is limited in its application. Firstly, the right only applies to data processing carried out by automated means. Secondly, in order for the portability right to apply, the processing must be carried out (ie, legitimised) on the basis of either consent or contract. These limitations re-affirm that the portability right is aimed at consumer choice and impacts consumer-facing service providers, as consent and contract are the two most common bases for processing in a consumer context.

The scope of the right requires that the data subject receive the personal data concerning him or her "*which he or she has provided to a controller, in a structured, commonly used and machine-readable format*" combined with the right to transmit those data to another controller "*without hindrance from the controller to which the personal data have been provided.*"

It is worthwhile breaking down the right into its constituent parts.

1. The right to receive the personal data concerning the data subject
This is a standalone right in the sense that the data does not have to be transferred to a third party but can simply be provided to the data subject. It therefore aligns with the existing right of access, but differs in that data portability imposes clear obligations as to format and usability, which the right of access does not.

The Article 29 Working Party (the "**WP29**") guidance on data portability provides that controllers should not take an overly restrictive interpretation of what personal data "concerns the data subject". In this regard, the WP29 uses the example of bank statements and provides that the data subject exercising their portability right should be able to have the full statements transferred. The WP29 suggests that the full statements should include the details of the third parties making payments to the account.

However, it is important to note that the GDPR provides that the right of data portability should not adversely affect the rights and freedoms of others. As a result, the disclosure of third party data needs to be weighed against the third party's rights and freedoms, so as to avoid third parties being unfairly prejudiced if certain data is ported. This balancing exercise means that a 'one size fits all' approach to portability is unlikely to be a feasible solution, and it may be that each request which involves third party personal data has to be considered on its merits.

[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.

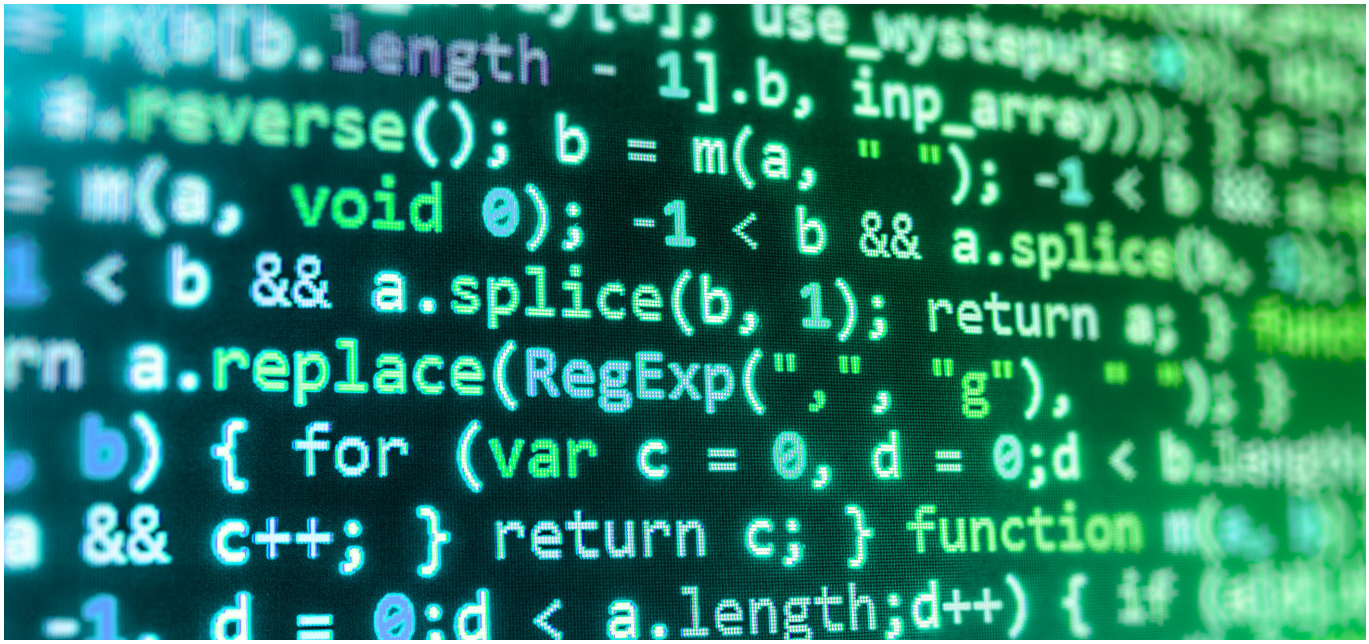
Data Portability

2. Which the data subject has provided to a controller
On a basic level, this covers data directly provided to a data controller, for example, information made available in online forms when a customer sets up an account or when they first use a service, such as their phone number, address, etc.

However, the WP29 has suggested that the term "provided by the data subject" must be interpreted broadly, and includes data that has been generated by and collected from the activities of the data subject (referred to as "observed data"). Observed data includes, for example, a person's search history, traffic data, smart metre data, location data, or for someone who uses a fitness tracker, their heartbeat.

By contrast, the WP29 guidance provides that data inferred or derived from further analysis of the personal data (eg, a credit score) provided by the data subject will not be subject to the right of portability.

Anonymous data will also not be subject to the portability right because it is not considered to be personal data. Pseudonymised data that can be clearly linked to the data subject (eg, via a username or other identifier), on the other hand, will be subject to the new right.



3. In a structured, commonly-used and machine-readable format
A data subject seeking personal data has the right to receive the data in a structured, machine readable and commonly used format. As an example, a request for email data must be provided in a format which preserves all the meta-data to allow for the effective re-use of the data. Therefore, when selecting a data format in which to provide the personal data, it is imperative that the data controller considers how this format would impact or hinder the individual's ability to re-use the data.

As regards the "machine-readable" requirement, other EU legislation prescribes that this means "open or proprietary file formats which are structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure."

What is considered "commonly used" will develop over time, but will depend on what industry your organisation operates in and links with the concept of interoperability (ie, the ability of computer systems or software to exchange and make use of the ported information).

4. The right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided
The portability right requires data controllers to ensure that, on request, data is transferred "*without hindrance*", which effectively means that the data must be interoperable. This is one of the most challenging aspects of the new right (and will impact on how effective and smooth its application may be) as it relies on competing organisations cooperating to ensure interoperability is achieved to facilitate customers moving between them. How any organisation will view this aspect invariably will depend on whether it takes the negative view that it is at risk of losing customers more easily, or conversely it adopts the positive view that an opportunity exists which could in fact make it easier to on-board new customers.

The data subject must be able to freely transfer his / her data to another controller. No fee can be charged for the exercise of the right unless a data controller can show that the request is manifestly unfounded or excessive, in particular due to the repetitive character of the requests.

In addition, the data must be provided without undue delay and in any case within one month of receipt of the request. This deadline can be extended to a maximum of three months for complex cases.

Data Portability

Risks to consider

One of the most significant risks associated with the new data portability right is identity theft. The GDPR recognises that a controller cannot comply with a data portability request if it is not in a position to identify the data subject and that it may request additional information in order to confirm the identity of the data subject. In this regard, WP29 recommends that controllers should implement an authentication procedure in order to confirm the identity of the data subject. This could be achieved by, for example, using passwords or digi-passes, which are common in the banking sector.

From a data protection compliance perspective, there are a number of clear risks. Firstly, a failure to comply with a data portability request could expose your organisation to investigation which brings with it the potential of a fine being levied. Secondly, there is a risk of misuse of the personal data once it is ported. In this circumstance, the WP29 guidance is clear that liability rests with the receiving data controller. This means that the data controller that responds to the data portability request will not be responsible for the subsequent processing of the data which it ports at the request of the data subject. Accordingly, the receiving data controller needs to be conscientious in ensuring that they have policies and procedures in place to deal with the data they receive (including making the requisite data privacy statement information available to the data subject).

Next Steps

As a first step, organisations need to think carefully about whether data portability applies to data held by them. Key questions are whether the data:

- processed by automated means;
- on the basis of either consent or contract; and
- has been "provided to" the controller by the data subject.

Where an organisation holds such data, it will need to consider the processes that need to be put in place both from a technical and operational perspective. It would be helpful for controllers to ask themselves what format the data is held in now, and whether this is a commonly used, structured and machine readable format? How will interoperability be achieved in the relevant industry? Are there trade or industry associations with which the organisation should be engaging to try and influence this so it aligns with its systems?

Finally, when embarking on technology refresh projects in the future, emphasis should be placed on privacy by design, and on utilising technology that will allow compliance with data portability requests.

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