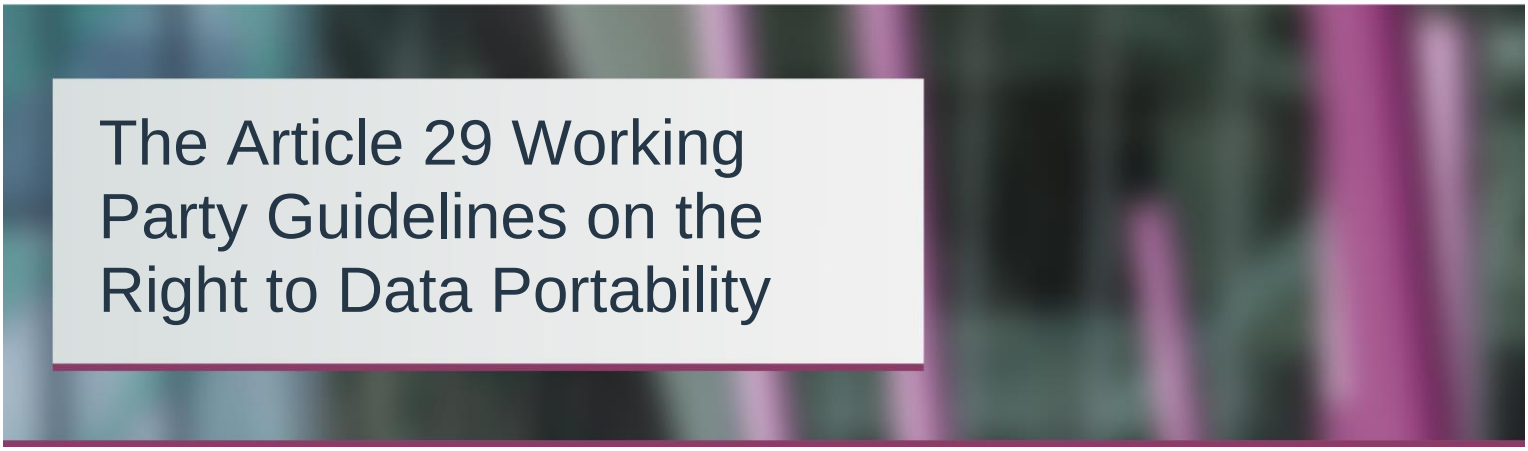
WILLIAM FRY

// PRIVACY SOURCE



The Article 29 Working Party Guidelines on the Right to Data Portability

The Article 29 Working Party (now called the European Data Protection Board ("**EDPB**") published its revised guidelines to assist organisations with the application and interpretation of certain chapters of the EU General Data Protection Regulation ("**GDPR**").

The EDPB released three guidelines in relation to:

- the Right to Data Portability;
- Data Protection Officers; and
- identifying a controller and processor's lead supervisory authority.

These revised guidelines were issued on 5 April 2017 following a public consultation that ran from December 2016 when the previous guidelines were released.

This InFocus article will detail the EDPB's guidelines concerning the right to **data portability**.

Background

The new right to data portability has been one of the most discussed elements of the GDPR as companies try to anticipate how it will operate in practice and the extent to which compliance with this new right will create significant cost implications. The right to data portability creates an ability for data subjects to require controllers to provide them with their personal data in a commonly used format and/or to transfer the data to another controller. This new right is the GDPR's response to addressing the concern from data subjects that companies were making it artificially difficult to move user data to a competing service provider.

The new guidelines address many of the queries raised by companies operating in big data, cloud computing and other sectors that will be affected by this new right, such as social media companies and utility providers.

The EDPB also provides a number of useful practical examples of how the new right arises and how it interacts with both the other rights contained in the GDPR and other areas such as intellectual property.

Core Elements of Data Portability

Data portability is considered by the EDPB to operate in a complementary nature to the right to access of personal data, which has been strengthened under the GDPR. The key goal of this new right is to allow data subjects to manage and reuse personal data, which has been provided to a controller. A natural extension of this is to allow the data subject to transmit the personal data from one controller to another without hindrance. This has raised queries as to how this type of interoperability will work in practice and whether it will impose a significant additional cost burden on companies.

This right aims not only to re-balance the relationship between organisations and data subjects by enhancing consumer empowerment over their personal data but also to foster innovation and to promote business models linked to more data sharing under the data subject's control. The free flow of personal data is at the core of this right and it is in line with the idea of a digital single market. However, the revised guidelines emphasise that the GDPR is not designed, as per se, to regulate competition. Nevertheless, this right facilitates greater competition between service providers.

Once a data portability request is made, the guidelines note that this does not automatically trigger erasure of the personal data on the existing controller's system. Equally, the right does not affect data retention requirements or any other data protection rights and can only be exercised as long as the controller is actually processing the personal data.

When Does Data Portability Apply?

In order to fall under the scope of data portability, the relevant processing operations must be based on:

- the **data subject's consent;** or
- a **contract to which the data subject is a party** pursuant to Article 6(1)(b).

This is a noteworthy provision as it effectively means that the right to data portability does not apply to controllers processing data pursuant to an official authority. However, the EDPB does comment that it is considered good data protection practice to have tools to allow for a right to portability to occur in such circumstances.

Additionally, the right to data portability only applies if the data processing is "carried out by automated means" meaning that the right to data portability does not cover paper files.

The right to transmit data from one controller to another is limited to conditions where this is "technically feasible" and this has been extensively highlighted in the guidelines.

Another aspect which has been clarified is that if the original controller does not have compatible systems in place to allow the direct transfer – it is up to the receiving controller to ensure that the direct transfer occurs, unless it is not technically feasible. If the original controller has any technical difficulties in relation to the transfer, this should clearly be explained to the data subject. The EDPB continue to stress the need for interoperable systems that will lessen the number of instances in which transfers are not technically feasible.

Conditions of the Right to Data Portability

Under the GDPR, the right to data portability will arise if three separate conditions are satisfied (outlined below).

First Condition: where the personal data "concerns the data subject"

The personal data requested should concern the data subject. Accordingly, data unrelated to the subject or anonymised data does not fall within the scope of the right to data portability under the GDPR as data should be clearly linked to a data subject.

The EDPB recommend that the term "personal data concerning the data subject" be interpreted as narrowly as possible.

Controllers will, from time to time, receive a data subject's request containing data relating to other individuals. In such circumstances, the EDPB states that the controller should only process these data if there is an **appropriate legal ground to do so** and such processing should not be processed in a manner that might adversely affect the rights and freedoms of third parties (discussed in further detail below).

Second Condition: where the personal data is "provided by the data subject"

The EDPB draws a critical distinction between two types of data:

- **Data Actively Provided**: the EDPB states that this includes data actively and knowingly provided by the data subject and observed data provided by the data subject by virtue of the service or the device (which **does fall within the scope** of data portability); and
- **Inferred Data**: the EDPB states that this is derived data or inferred data which is created by the controller on the basis of the data provided by the data subject (**which does not fall within the scope** of data portability).

To distinguish between "data actively provided" and "inferred data", the guidelines provide an example of credit scores stored by controllers as part of a user profile. Even though the data is inferred from data provided by the data subject, such data cannot be considered as data provided by the data subject and, accordingly, is not captured within this right.

The EDPB emphasises however, that the term "provided by the data subject" should be interpreted broadly and only excludes inferred data such as that described in the example above. The distinction in respect of observed data remains, despite a number of criticisms about considering this to be data that is actively provided during the consultation period.

Third Condition: where the right does not "adversely affect the rights and freedoms of others"

The EDPB sets out two scenarios in which the right to data portability might affect the rights and freedoms of third parties, where:

- the personal data concerns other data subjects; and
- the relevant data is covered by intellectual property law or trade secrets.

Regarding the first scenario, it should be demonstrated that the rights of the third party data subjects are not adversely affected by the data subject exercising their right to data portability. This can cause some difficulties in practice in order to determine precisely where the line falls, particularly in relation to social media and e-mail accounts.

In terms of the second scenario and the transmission of third party data that may adversely affect their intellectual property rights of third party data subject, these rights are defined under Recital 63 of the GDPR as, "the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting software". The application of this restriction in practice by companies is interesting and there is a very fine line to be followed. The EDPB appear to be aware of the potential for misuse of the exception as they have stated that a potential business risk cannot, of itself, serve as a basis for refusal of a portability request.

Application of Data Subjects Rights to Data Portability

How can the controller identify the data subject before answering his/her request?

The guidelines recommend that controllers implement an authentication procedure in order to ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR. The EDPB points out, however, that in many circumstances such procedures will already be in place in organisations e.g. username and password entry.

It is also recommended that data controllers implement procedures to assess the risks linked to data portability and take appropriate risk mitigation measures. Examples provided include end-to-end user encryption and authentication techniques.

In situations where the size of the data requested by the data subject makes internet transmission problematic, the controller may be required to consider alternative means of providing such data

(e.g. using streaming or saving the data to a CD or DVD). For example, if the data subject has a data cap or poor quality internet download speeds they may request the data on a CD.

What is the time limit imposed to answer a data portability request?

Article 12(3) of the GDPR requires that the controller provides the personal data to the data subject "without undue delay" and in any case "within one month of receipt of the request" or within a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay, although this extended period should, in the EDPB's view, not be relied upon commonly in practice.

The EDPB recommends that best practice for controllers is to define a timeframe in which a data portability request can typically be answered and communicate this to data subjects at the outset.

In what circumstances can a data portability request be rejected or a fee charged?

The guidelines indicate that there should only be limited circumstances in which a data portability request should be refused. It is difficult for information society services providers to prove that the answering of multiple data portability requests imposes an excessive burden as described above.

Additionally, the costs involved in putting in place the tools to allow for responsive answering of data portability requests and the number of requests made should not be used to determine its excessiveness and is not considered as reasonable means for justifying refusal.

How Must the Portable Data be Provided?

Controllers are required to provide the personal data requested by the data subject in a format that supports re-use. This is defined under Article 20(1) of the GDPR as a format that is provided in a "structured, commonly used and machine-readable format".

The terms "structured", "commonly used" and "machine-readable" are minimum requirements that should facilitate the interoperability of the data (interoperable data is data that can be used and reused by individuals across interoperable applications).

The guidelines note that the GDPR does not impose specific recommendations on the format of the personal data to be provided, recognising instead that the most appropriate format will differ across existing sectors, but, as a general rule, the format should always be chosen for the purpose of being interoperable as opposed to compatible. The guidelines state that formats subject to costly licensing constraints should not be considered an adequate approach.

The guidelines recommend that data controllers should explore two different and complementary paths: a direct transmission of the overall dataset of portable data and an automated tool that allows extraction of relevant dates. They recommend that data subjects should have the ability to access a personal data store where they can grant permission to data controllers to access and process their personal data as required.

Controllers should also aim to provide as much metadata with the data as possible at the best possible level of granularity, which preserves the precise meaning of the exchanged information. To demonstrate this particular point, the EDPB provides an example of an individual being provided with PDF versions of an email inbox and explains that this is not sufficiently structured as it could hinder re-use of the data.

In circumstances where it is possible for the data to be provided in different formats and the data subject is given a choice, it is advisable that the implications of each choice should be clearly communicated to the data subject before any such choice is made by them.

The EDPB strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability. This has also been recognised by the European Interoperability Framework (the "EIF") who recommend that a uniform approach to interoperability for organisations should be agreed. The might include vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.

How to deal with large or complex personal data collection?

This particular difficulty is not specifically addressed under the GDPR. However, the guidelines emphasise that it is crucial that the individual is in a position to fully understand the definition, scheme

and structure of the personal data which could be provided by the controller to a "new" controller. This might be achieved by providing the data in a summarised form using dashboards that would enable data subjects to port subsets of data as opposed to the entire catalogue.

It should be borne in mind that any overview or summary of large datasets should be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language".

The EDPB suggests Application Programming Interface ("API") as one of the ways controllers can answer portability requests from data subjects. This would enable individuals to make requests via their own third party software or grant permission to others to do so on their behalf. This, the EDPB suggests, offers a more sophisticated access system to data subjects.

How can portable data be secured?

According to Article 5(1)(f) of the GDPR, controllers should guarantee the appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, **using appropriate technical or organisation measures.**

The guidelines identify the transmission of data from one information system to another as a potential source of risk for controllers, who are responsible for **taking all security measures necessary** to ensure that personal data is securely transmitted to the right destination. The EDPB advises against using obstructive security measures which might prevent data subjects from exercising their rights.

The guidelines point out that, when individuals retrieve personal data from an online service, there is also a risk that this data will then be stored to a less secure system by the user. The guidelines recommend that controllers should inform the data subject of this risk and make them aware of steps that might be taken to effect more secure data storage e.g. encryption and the use of strong authentication measures and transparent procedures for dealing with possible data breaches. Data controllers are advised to assess any risks that may occur and take appropriate measures to mitigate those risks.

Conclusion

The guidelines from the EDPB on this area are certainly welcome as it has been one of the most uncertain areas under GDPR, particularly as controllers have been implementing procedures and policies to address such requests since the GDPR entered force.

Organisations should bear in mind that a breach of this right (Article 20 of the GDPR) could result in a potential fine of up to € 20 million or 4% of the total worldwide turnover in the case of an undertaking.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA