ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 242 rev.01

Guidelines on the right to data portability

Adopted on 13 December 2016
As last Revised and adopted on 5 April 2017

TABLE OF CONTENTS

Executive summary

Article 20 of the GDPR creates a new right to data portability, which is closely related to the right of access but differs from it in many ways. It allows for data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller. The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.

Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers. It will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy.

This opinion provides guidance on the way to interpret and implement the right to data portability as introduced by the GDPR. It aims at discussing the right to data portability and its scope. It clarifies the conditions under which this new right applies taking into account the legal basis of the data processing (either the data subject's consent or the necessity to perform a contract) and the fact that this right is limited to personal data provided by the data subject. The opinion also provides concrete examples and criteria to explain the circumstances in which this right applies. In this regard, WP29 considers that the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject, for example, on an online form.

As a good practice, data controllers should start developing the means that will contribute to answer data portability requests, such as download tools and Application Programming Interfaces. They should guarantee that personal data are transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request.

The opinion also helps data controllers to clearly understand their respective obligations and recommends best practices and tools that support compliance with the right to data portability. Finally, the opinion recommends that industry stakeholders and trade associations work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.

I. Introduction

Article 20 of the General Data Protection Regulation (GDPR) introduces a new right of data portability. This right allows for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance. This right, which applies subject to certain conditions, supports user choice, user control and user empowerment.

Individuals making use of their right of access under the Data Protection Directive 95/46/EC were constrained by the format chosen by the data controller when providing the requested information. **The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another** (whether to their own systems, the systems of trusted third parties or those of new data controllers).

By affirming individuals' personal rights and control over the personal data concerning them, data portability also represents an opportunity to "re-balance" the relationship between data subjects and data controllers[1].

Whilst the right to personal data portability may also enhance competition between services (by facilitating service switching), the GDPR is regulating personal data and not competition. In particular, article 20 does not limit portable data to those which are necessary or useful for switching services[2].

Although data portability is a new right, other types of portability already exist or are being discussed in other areas of legislation (e.g. in the contexts of contract termination, communication services roaming and trans-border access to services[3]). Some synergies and even benefits to individuals may emerge between the different types of portability if they are provided in a combined approach, even though analogies should be treated cautiously.

This Opinion provides guidance to data controllers so that they can update their practices, processes and policies, and clarifies the meaning of data portability in order to enable data subjects to efficiently use their new right.

II. What are the main elements of data portability?

The GDPR defines the right of data portability in Article 20 (1) as follows:

> *The data subject shall have the right to 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 and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided […]*

- A right to receive personal data

Firstly, data portability is a **right of the data subject to receive a subset of the personal data** processed by a data controller concerning him or her, and to store those data for further personal use. Such storage can be on a private device or on a private cloud, without necessarily transmitting the data to another data controller.

[1] The primary aim of data portability is enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem.
[2] For example, this right may allow banks to provide additional services, under the user's control, using personal data initially collected as part of an energy supply service.
[3] See European Commission agenda for a digital single market: https://ec.europa.eu/digital-agenda/en/digital-single-market, in particular, the first policy pillar "Better online access to digital goods and services".

In this regard, data portability complements the right of access. One specificity of data portability lies in the fact that it offers an easy way for data subjects to manage and reuse personal data themselves. These data should be received "*in a structured, commonly used and machine-readable format"*. For example, a data subject might be interested in retrieving his current playlist (or a history of listened tracks) from a music streaming service, to find out how many times he listened to specific tracks, or to check which music he wants to purchase or listen to on another platform. Similarly, he may also want to retrieve his contact list from his webmail application, for example, to build a wedding list, or get information about purchases using different loyalty cards, or to assess his or her carbon footprint[4].

- **A right to transmit personal data from one data controller to another data controller**

Secondly, Article 20(1) provides data subjects with the **right to transmit personal data from one data controller to another data controller** "without hindrance". Data can also be transmitted directly from one data controller to another on request of the data subject and where it is technically feasible (Article 20(2)). In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability[5] but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible[6]. The GDPR does, however, prohibit controllers from establishing barriers to the transmission.

In essence, this element of data portability provides the ability for data subjects not just to obtain and reuse, but also to transmit the data they have provided to another service provider (either within the same business sector or in a different one). In addition to providing consumer empowerment by preventing "lock-in", the right to data portability is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the data subject's control[7]. Data portability can promote the controlled and limited sharing by users of personal data between organisations and thus enrich services and customer experiences[8]. Data portability may facilitate transmission and reuse of personal data concerning users among the various services they are interested in.

[4] In these cases, the processing performed on the data by the data subject can either fall within the scope of household activities, when all the processing is performed under the sole control of the data subject, or it can be handled by another party, on the data subject's behalf. In the latter case, the other party should be considered as data controller, even for the sole purpose of personal data storage, and must comply with the principles and obligations laid down in the GDPR.

[5] See also section V.

[6] As a consequence, special attention should be paid to the format of the transmitted data, so as to guarantee that the data can be re-used, with little effort, by the data subject or another data controller. See also section V.

[7] See several experimental applications in Europe, for example MiData in the United Kingdom, MesInfos / SelfData by FING in France.

[8] The so-called quantified self and IoT industries have shown the benefit (and risks) of linking personal data from different aspects of an individual's life such as fitness, activity and calorie intake to deliver a more complete picture of an individual's life in a single file.

- **Controllership**

Data portability guarantees the right to receive personal data and to process them, according to the data subject's wishes[9].

Data controllers answering data portability requests, under the conditions set forth in Article 20, are not responsible for the processing handled by the data subject or by another company receiving personal data. They act on behalf of the data subject, including when the personal data are directly transmitted to another data controller. In this respect, the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient. At the same time the controller should set safeguards to ensure they genuinely act on the data subject's behalf. For example, they can establish procedures to ensure that the type of personal data transmitted are indeed those that the data subject wants to transmit. This could be done by obtaining confirmation from the data subject either before transmission or earlier on when the original consent for processing is given or the contract is finalised.

Data controllers answering a data portability request have no specific obligation to check and verify the quality of the data before transmitting it. Of course, these data should already be accurate, and up to date, according to the principles stated in Art 5(1) of the GDPR. Moreover, data portability does not impose an obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period[10]. Importantly, there is no additional requirement to retain data beyond the otherwise applicable retention periods, simply to serve any potential future data portability request.

Where the personal data requested are processed by a data processor, the contract concluded in accordance with Article 28 of the GDPR must include the obligation to assist "the controller by appropriate technical and organisational measures, (…) to respond to requests for exercising the data subject's rights". The data controller should therefore implement specific procedures in cooperation with its data processors to answer data portability requests. In case of a joint controllership, a contract should allocate clearly the responsibilities between each data controller regarding the processing of data portability requests.

In addition, a receiving data controller[11] is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing. For example, in the case of a data portability request made to a webmail service, where the request is used by the data subject to obtain emails and send them to a secured archive platform, the new data controller does not need to process the contact details of the data subject's correspondents. If this information is not relevant with regard to the purpose of the new processing, it should not be kept and processed. In any case, receiving data controllers are not obliged to accept and process personal data transmitted following a data portability request. Similarly, where a data subject requests the transmission of details of his or her bank transactions to a service that assists in managing his or her budget, the receiving data controller does not need to accept all the data, or to retain all the details of the transactions once they have been labelled for the

[9] The right to data portability is not limited to personal data that are useful and relevant for similar services provided by competitors of the data controller.

[10] In the example above, if the data controller does not retain a record of songs played by a user then this personal data cannot be included within a data portability request.

[11] i.e. that receives personal data following a data portability request made by the data subject to another data controller.

purposes of the new service. In other words, the data accepted and retained should only be that which is necessary and relevant to the service being provided by the receiving data controller.

A "receiving" organization becomes a new data controller regarding these personal data and must respect the principles stated in Article 5 of the GDPR. Therefore, the "new" receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14[12]. As for any other data processing performed under its responsibility, the data controller should apply the principles laid down in Article 5, such as lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, integrity and confidentiality, storage limitation and accountability[13].

Data controllers holding personal data should be prepared to facilitate their data subject's right to data portability. Data controllers can also choose to accept data from a data subject, but are not obliged to.

- **Data portability vs. other rights of data subjects**

When an individual exercises his or her right to data portability he or she does so without prejudice to any other right (as is the case with any other rights in the GDPR). A data subject can continue to use and benefit from the data controller's service even after a data portability operation. Data portability does not automatically trigger the erasure of the data[14] from the systems of the data controller, and does not affect the original retention period applying to the data which have been transmitted. The data subject can exercise his or her rights as long as the data controller is still processing the data.

Equally, if the data subject wants to exercise his or her right to erasure ("right to be forgotten" under Article 17), data portability cannot be used by a data controller as a way of delaying or refusing such erasure.

Should a data subject discover that personal data requested under the right to data portability does not fully address his or her request, any further request for personal data under a right of access should be fully complied with, in accordance with Article 15 of the GDPR.

Furthermore, where a specific European or Member State law in another field also provides for some form of portability of the data concerned, the conditions laid down in these specific laws must also be taken into account when satisfying a data portability request under the GDPR. First, if it is clear from the request made by the data subject that his or her intention is not to exercise rights under the GDPR, but rather, to exercise rights under sectorial legislation

[12] In addition, the new data controller should not process personal data, which are not relevant, and the processing must be limited to what is necessary for the new purposes, even if the personal data are part of a more global data-set transmitted through a portability process. Personal data, which are not necessary to achieve the purpose of the new processing, should be deleted as soon as possible.

[13] Once received by the data controller, the personal data sent as part of the right to data portability can be considered as "provided by" the data subject and be re-transmitted according to the right to data portability, to the extent that the other conditions applicable to this right (ie. the legal basis of the processing, …) are met.

[14] as stated in Article 17 of the GDPR

only, then the GDPR's data portability provisions will not apply to this request[15]. If, on the other hand, the request is aimed at portability under the GDPR, the existence of such specific legislation does not override the general application of the data portability principle to any data controller, as provided by the GDPR. Instead, it must be assessed, on a case by case basis, how, if at all, such specific legislation may affect the right to data portability.

III. When does data portability apply?

- Which processing operations are covered by the right to data portability?

Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data.

In accordance with Article 20(1)(a) of the GDPR, **in order to fall under the scope of data** portability, processing operations must be based:

- either on the data subject's consent (pursuant to Article 6(1)(a), or pursuant to Article 9(2)(a) when it comes to special categories of personal data);

- or, on a contract to which the data subject is a party pursuant to Article 6(1)(b).

As an example, the titles of books purchased by an individual from an online bookstore, or the songs listened to via a music streaming service are examples of personal data that are generally within the scope of data portability, because they are processed on the basis of the performance of a contract to which the data subject is a party.

The GDPR does not establish a general right to data portability for cases where the processing of personal data is not based on consent or contract[16]. For example, there is no obligation for financial institutions to answer a data portability request concerning personal data processed as part of their obligations obligation to prevent and detect money laundering and other financial crimes; equally, data portability does not cover professional contact details processed in a business to business relationship in cases where the processing is neither based on the consent of the data subject nor on a contract to which he or she is a party.

When it comes to employees' data, the right to data portability typically applies only if the processing is based on a contract to which the data subject is a party. In many cases, consent will not be considered freely given in this context, due to the imbalance of power between the

[15] For example, if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in the Payment Services Directive 2 (PSD2) such access should be granted according to the provisions of this directive.

[16] See recital 68 and Article 20(3) of the GDPR. Article 20(3) and Recital 68 provide that data portability does not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, or when a data controller is exercising its public duties or complying with a legal obligation. Therefore, there is no obligation for data controllers to provide for portability in these cases. However, it is a good practice to develop processes to automatically answer portability requests, by following the principles governing the right to data portability. An example of this would be a government service providing easy downloading of past personal income tax filings. For data portability as a good practice in case of processing based on the legal ground of necessity for a legitimate interest and for existing voluntary schemes, see pages 47 & 48 of WP29 Opinion 6/2014 on legitimate interests (WP217).

employer and employee[17]. Some HR processings instead are based on the legal ground of legitimate interest, or are necessary for compliance with specific legal obligations in the field of employment. In practice, the right to data portability in an HR context will undoubtedly concern some processing operations (such as pay and compensation services, internal recruitment) but in many other situations a case by case approach will be needed to verify whether all conditions applying to the right to data portability are met.

Finally, the right to data portability only applies if the data processing is "carried out by automated means", and therefore does not cover most paper files.

- **What personal data must be included?**

Pursuant to Article 20(1), to be within the scope of the right to data portability, data must be:

- personal data concerning him or her, and
- which he or she has *provided* to a data controller.

Article 20(4) also states that compliance with this right shall not adversely affect the rights and freedoms of others.

First condition: personal data concerning the data subject

Only personal data is in scope of a data portability request. Therefore, any data that is anonymous[18] or does not concern the data subject, will not be in scope. However, pseudonymous data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier, cf. Article 11 (2)) is within the scope.

In many circumstances, data controllers will process information that contains the personal data of several data subjects. Where this is the case, data controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties (see below: third condition).

Second condition: data provided by the data subject

The second condition narrows the scope to data "provided by" the data subject.

There are many examples of personal data, which will be knowingly and actively "provided by" the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, data "provided by" the data subject also result from the observation of his activity. As a consequence, the WP29 considers that to give its full value to this new right, "provided by" should also include the personal data that are observed from the

[17] As the WP29 outlined in its Opinion 8/2001 of 13 September 2001 (WP48).
[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

activities of users such as raw data processed by a smart meter or other types of connected objects[19], activity logs, history of website usage or search activities.

This latter category of data does not include data that are created by the data controller (using the data observed or directly provided as input) such as a user profile created by analysis of the raw smart metering data collected.

A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":

- **Data actively and knowingly provided by the data subject** (for example, mailing address, user name, age, etc.)
- **Observed data provided by the data subject by virtue of the use of the service or the device**. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.

In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right[20].

In general, given the policy objectives of the right to data portability, the term "provided by the data subject" must be interpreted broadly, and should exclude "inferred data" and "derived data", which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller[21].

Thus, the term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been

[19] By being able to retrieve the data resulting from observation of his or her activity, the data subject will also be able to get a better view of the implementation choices made by data controller as to the scope of observed data and will be in a better situation to choose what data he or she is willing to provide to get a similar service, and be aware of the extent to which his or her right to privacy is respected.

[20] Nevertheless, the data subject can still use his or her "right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data" as well as information about "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject", according to Article 15 of the GDPR (which refers to the right of access).

[21] This includes all data observed about the data subject during the activities for the purpose of which the data are collected, such as a transaction history or access log. Data collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track browsing behaviour) should also be considered as "provided by" him or her even if the data are not actively or consciously transmitted.

created by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.

Third condition: the right to data portability shall not adversely affect the rights and freedoms of others

With respect to personal data concerning other data subjects:

The third condition is intended to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects (Article 20(4) of the GDPR)[22].

Such an adverse effect would occur, for instance, if the transmission of data from one data controller to another, would prevent third parties from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.).

The data subject initiating the transmission of his or her data to another data controller, either gives consent to the new data controller for processing or enters into a contract with that controller. Where personal data of third parties are included in the data set another legal basis for the processing must be identified. For example, a legitimate interest may be pursued by the data controller under Article 6(1)(f), in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for a purely personal or household activity. The processing operations initiated by the data subject in the context of personal activity that concern and potentially impact third parties remain under his or her responsibility, to the extent that such processing is not, in any manner, decided by the data controller.

For example, a webmail service may allow the creation of a directory of a data subject's contacts, friends, relatives, family and broader environment. Since these data relate to (and are created by) the identifiable individual that wishes to exercise his right to data portability, data controllers should transmit the entire directory of incoming and outgoing e-mails to that data subject.

Similarly, a data subject's bank account can contain personal data relating to the transactions not just of the account holder but also those of other individuals (e.g., if they have transferred money to the account holder). The rights and freedoms of those third parties are unlikely to be adversely affected by the transmission of the bank account information to the account holder once a portability request is made—provided that in both examples the data are used for the same purpose (i.e., a contact address only used by the data subject or a history of the data subject's bank account.

Conversely, the rights and freedoms of third parties will not be respected if the new data controller uses the personal data for other purposes, e.g. if the receiving data controller uses

[22] Recital 68 provides that "where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation."

personal data of other individuals within the data subject's contact directory for marketing purposes.

Therefore, to prevent adverse effects on the third parties involved, the processing of such personal data by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs. A receiving 'new' data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other third party data subjects. For example, this information should not be used to enrich the profile of the third party data subject and rebuild his social environment, without his knowledge and consent[23]. Neither can it be used to retrieve information about such third parties and create specific profiles, even if their personal data are already held by the data controller. Otherwise, such processing is likely to be unlawful and unfair, especially if the third parties concerned are not informed and cannot exercise their rights as data subjects.

Furthermore, it is a leading practice for all data controllers (both the "sending" and "receiving" parties) to implement tools to enable data subjects to select the relevant data they wish to receive and transmit and exclude, where relevant, data of other individuals. This will further assist in reducing the risks for third parties whose personal data may be ported.

Additionally, the data controllers should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. if they also want to move their data to some other data controller. Such a situation might arise, for example, with social networks, but it is up to data controllers to decide on the leading practice to follow.

With respect to data covered by intellectual property and trade secrets:
The rights and freedoms of others are mentioned in Article 20(4). While not directly related to portability, this can be understood as "including trade secrets or intellectual property and in particular the copyright protecting the software. However, even though these rights should be considered before answering a data portability request, "the result of those considerations should not be a refusal to provide all information to the data subject". Furthermore, the data controller should not reject a data portability request on the basis of the infringement of another contractual right (for example, an outstanding debt, or a trade conflict with the data subject).

The right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights.

A potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request and data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.

[23] A social networking service should not enrich the profile of its members by using personal data transmitted by a data subject as part of his right to data portability, without respecting the principle of transparency and also making sure they rely on an appropriate legal basis regarding this specific processing.

IV. How do the general rules governing the exercise of data subject rights apply to data portability?

- **What prior information should be provided to the data subject?**

In order to comply with the new right to data portability, data controllers must inform data subjects of the existence of the new right to portability. Where the personal data concerned are directly collected from the data subject, this must happen "at the time where personal data are obtained". If the personal data have not been obtained from the data subject, the data controller must provide the information as required by Articles 13(2)(b) and 14(2)(c).

"Where the personal data have not been obtained from the data subject", Article 14(3) requires the information to be provided within a reasonable time not exceeding one month after obtaining the data, during first communication with the data subject, or when disclosure is made to third parties[24].

When providing the required information data controllers must ensure that they distinguish the right to data portability from other rights. Therefore, WP29 recommends in particular that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability.

In addition, the Working Party recommends that data controllers always include information about the right to data portability before data subjects close any account they may have. This allows users to take stock of their personal data, and to easily transmit the data to their own device or to another provider before a contract is terminated.

Finally, as leading practice for "receiving" data controllers, the WP29 recommends that data subjects are provided with complete information about the nature of personal data which are relevant for the performance of their services. In addition to underpinning fair processing, this allows users to limit the risks for third parties, and also any other unnecessary duplication of personal data even where no other data subjects are involved.

- **How can the data controller identify the data subject before answering his request?**

There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. Nevertheless, Article 12(2) of the GDPR states that the data controller shall not refuse to act on request of a data subject for exercising his or her rights (including the right to data portability) unless it is processing personal data for a purpose that does not require the identification of a data subject and it can demonstrate that it is not able to identify the data subject. However, as per Article 11(2), in such circumstances the data subject can provide more information to enable his or her identification. Additionally, Article 12(6) provides that where a data controller has reasonable doubts about the identity of a data subject, it can request further information to confirm the data subject's identity. Where a data subject provides additional information enabling his or her identification, the data controller shall not refuse to act on the request. Where information and data collected online is linked to pseudonyms or unique identifiers, data controllers can implement appropriate procedures

[24] Article 12 requires that data controllers provide "any communications […] in a concise, transparent, intelligible, and easily assessable form, using clear and plain language, in particular for any information addressed specifically to a child."

enabling an individual to make a data portability request and receive the data relating to him or her. In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.

These procedures often already exist. The data subjects are often already authenticated by the data controller before entering into a contract or collecting his or her consent to the processing. As a consequence, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for portability purposes[25].

While in these cases, the data subjects' prior identification may require a request for proof of their legal identity, such verification may not be relevant to assess the link between the data and the individual concerned, since such a link is not related with the official or legal identity. In essence, the ability for the data controller to request additional information to assess one's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.

In many cases, such authentication procedures are already in place. For example, usernames and passwords are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals chose to use without revealing their full name and identity.

If the size of data requested by the data subject makes transmission via the internet problematic, rather than potentially allowing for an extended time period of a maximum of three months to comply with the request[26], the data controller may also need to consider alternative means of providing the data such as using streaming or saving to a CD, DVD or other physical media or allowing for the personal data to be transmitted directly to another data controller (as per Article 20(2) of the GDPR where technically feasible).

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

Article 12(3) requires that the data controller provides "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request". This one month period can be extended to a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request.

Data controllers operating information society services are likely to be better equipped to be able to comply with requests within a very short time period. To meet user expectations, it is a good practice to define the timeframe in which a data portability request can typically be answered and communicate this to data subjects.

Data controllers who refuse to answer a portability request shall, pursuant to Article 12(4), inform the data subject "the reasons for not taking action and on the possibility of lodging a

[25] For example, when the data processing is linked to a user account, providing the relevant login and password might be sufficient to identify the data subject.
[26] Article 12(3): "The controller shall provide information on action taken on a request".

complaint with a supervisory authority and seeking a judicial remedy", no later than one month after receiving the request.

Data controllers must respect the obligation to respond within the given terms, even if it concerns a refusal. In other words, the data controller cannot remain silent when it is asked to answer a data portability request.

- **In which cases can a data portability request be rejected or a fee charged?**

Article 12 prohibits the data controller from charging a fee for the provision of the personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, "in particular because of their repetitive character". For information society services that specialise in automated processing of personal data, implementing automated systems such as Application Programming Interfaces (APIs)[27] can facilitate the exchanges with the data subject, hence lessen the potential burden resulting from repetitive requests. Therefore, there should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests.

In addition, the overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request. In fact, Article 12 of the GDPR focuses on the requests made by one data subject and not on the total number of requests received by a data controller. As a result, the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests.

V. How must the portable data be provided?

- **What are the expected means the data controller should implement for data provision?**

Article 20(1) of the GDPR provides that data subjects have the right to transmit the data to another controller without hindrance from the controller to which the personal data have been provided.

Such hindrance can be characterised as any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller. For example, such hindrance could be: fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demands[28].

Article 20(2) also places obligations on data controllers for transmitting the portable data directly to other data controllers "when technically feasible".

[27] Application Programming Interface (API) means the interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems.

[28] Some legitimate obstacles might arise, as the ones, which are related to the rights and freedoms of others mentioned in Article 20(4), or the ones that relate to the security of the controllers' own systems. It shall be the responsibility of the data controller to justify why such obstacles would be legitimate and why they do not constitute a hindrance in the meaning of Article 20(1).

The technical feasibility of transmission from data controller to data controller, under the control of the data subject, should be assessed on a case by case basis. Recital 68 further clarifies the limits of what is "technically feasible", indicating that "it should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".

Data controllers are expected to transmit personal data in an interoperable format, although this does not place obligations on other data controllers to support these formats. Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way[29], and when the receiving system is technically in a position to receive the incoming data. If technical impediments prohibit direct transmission, the data controller shall explain those impediments to the data subjects, as his decision will otherwise be similar in its effect to a refusal to take action on a data subject's request (Article 12(4)).

On a technical level, data controllers should explore and assess two different and complimentary paths for making portable data available to the data subjects or to other data controllers:

- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);
- an automated tool that allows extraction of relevant data.

The second way may be preferred by data controllers in cases involving of complex and large data sets, as it allows for the extraction of any part of the data-set that is relevant for the data subject in the context of his or her request, may help minimising risk, and possibly allows for use of data synchronisation mechanisms[30] (e.g. in the context of a regular communication between data controllers). It may be a better way to ensure compliance for the "new" data controller, and would constitute good practice in the reduction of privacy risks on the part of the initial data controller.

These two different and possibly complementary ways of providing relevant portable data could be implemented by making data available through various means such as, for example, secured messaging, an SFTP server, a secured WebAPI or WebPortal. Data subjects should be enabled to make use of a personal data store, personal information management system[31] or other kinds of trusted third-parties, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required.

- **<u>What is the expected data format?</u>**

The GDPR places requirements on data controllers to provide the personal data requested by the individual in a format, which supports re-use. Specifically, Article 20(1) of the GDPR states that the personal data must be provided "in a structured, commonly used and machine-

[29] Through an authenticated communication with the necessary level of data encryption.
[30] Synchronisation mechanism can help reaching the general obligations under Article 5obligation of the GDPR, which provides that "personal data shall be (…) accurate and, where necessary, kept up to date"
[31] On personal information management systems (PIMS), see, for example, EDPS Opinion 9/2016, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

readable format". Recital 68 provides a further clarification that this format should be interoperable, a term that is defined[32] in the EU as:

> *the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.*

The terms "structured", "commonly used" and "machine-readable" are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way, "structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome.

Recital 21 of Directive 2013/37/EU[33,34] defines "machine readable" as:

> *a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.*

Given the wide range of potential data types that could be processed by a data controller, the GDPR does not impose specific recommendations on the format of the personal data to be provided. The most appropriate format will differ across sectors and adequate formats may already exist, and should always be chosen to achieve the purpose of being interpretable and affording the data subject with a large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach.

Recital 68 clarifies that "*The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.*" **Thus, portability aims to produce interoperable systems, not compatible systems**[35].

Personal data are expected to be provided in formats that have a high level of abstraction from any internal or proprietary format. As such, data portability implies an additional layer of data processing by data controllers, in order to extract data from the platform and filter out personal data outside the scope of portability, such as inferred data or data related to security of systems. In this way, data controllers are encouraged to identify beforehand data which are within the scope of portability in their own systems. This additional data processing will be

[32] Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20

[33] Amending Directive 2003/98/EC on the re-use of public sector information.

[34] The EU glossary (http://eur-lex.europa.eu/eli-register/glossary.html) provides further clarification on expectations related to the concepts used in this guideline, such as *machine-readable, interoperability, open format, standard, metadata.*

[35] ISO/IEC 2382-01 defines interoperability as follows: "The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."

considered as ancillary to the main data processing, since it is not performed to achieve a new purpose defined by the data controller.

Where no formats are in common use for a given industry or given context, **data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with** useful **metadata at the best possible level of granularity,** while maintaining a high level of abstraction. As such, suitable metadata should be used in order to accurately describe the meaning of exchanged information. This metadata should be enough to make the function and reuse of the data possible but, of course, without revealing trade secrets. It is unlikely therefore that providing an individual with PDF versions of an email inbox would be sufficiently structured or descriptive to allow the inbox data to be easily re-used. Instead, the e-mail data should be provided in a format which preserves all the metadata, to allow the effective re-use of the data. As such, when selecting a data format in which to provide the personal data, the data controller should consider how this format would impact or hinder the individual's right to re-use the data. In cases where a data controller is able to provide choices to the data subject regarding the preferred format of the personal data a clear explanation of the impact of the choice should be provided. However, processing additional metadata for the sole purpose that they might be needed or wanted to answer a data portability request poses no legitimate ground for such processing.

WP29 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 challenge has also been addressed by the European Interoperability Framework (EIF) which has created an agreed approach to interoperability for organizations that wish to jointly deliver public services. Within its scope of applicability, the framework specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices[36].

- **How to deal with a large or complex personal data collection?**

The GDPR does not explain how to address the challenge of responding where a large data collection, a complex data structure or other technical issues arise that might create difficulties for data controllers or data subjects.

However, in all cases, it is crucial that the individual is in a position to fully understand the definition, schema and structure of the personal data that could be provided by the data controller. For instance, data could first be provided in a summarised form using dashboards allowing the data subject to port subsets of the personal data rather than the entirety. The data controller should provide an overview "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (see Article 12(1)) of the GDPR) in such a way that data subject should always have clear information of what data to download or transmit to another data controller in relation to a given purpose. For example, data subjects should be in a position to use software applications to easily identify, recognize and process specific data from it.

As referenced above, a practical way by which a data controller can answer requests for data portability may be by offering an appropriately secured and documented API. This may

[36] Source : http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

enable individuals to make requests of the data controller for their personal data via their own or third-party software or grant permission for others to so do on their behalf (including another data controller) as specified in Article 20(2) of the GDPR. By granting access to data via an externally accessible API, it may also be possible to offer a more sophisticated access system that enables individuals to make subsequent requests for data, either as a full download or as a delta function containing only changes since the last download, without these additional requests being onerous on the data controller.

- **How can portable data be secured?**

In general, data 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 organisational measures" according to Article 5(1)(f) of the GDPR.

However, the transmission of personal data to the data subject may also raise some security issues:

How can data controllers ensure that personal data are securely delivered to the right person?

As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission). The data controller is responsible for taking all the security measures needed to ensure not only that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures), but also continuing to protect the personal data that remains in their systems, as well as transparent procedures for dealing with possible data breaches[37]. As such, data controllers should assess the specific risks linked with data portability and take appropriate risks mitigation measures.

Such risk mitigation measures could include: if the data subject already needs to be authenticated, using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password; suspending or freezing the transmission if there is suspicion that the account has been compromised; in cases of a direct transmission from a data controller to another data controller, authentication by mandate, such as token-based authentications, should be used.

Such security measures must not be obstructive in nature and must not prevent users from exercising their rights, e.g. by imposing additional costs.

How to help users in securing the storage of their personal data in their own systems?

By retrieving their personal data from an online service, there is always the risk that users may store them in less secured systems than the one provided by the service. The data subject requesting the data is responsible for identifying the right measures in order to secure personal data in his own system. However, he should be made aware of this in order to take steps to protect the information he has received. As an example of leading practice data controllers

[37] In conformance to the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

may also recommend appropriate format(s), encryption tools and other security measures to help the data subject in achieving this goal.

* * *

Done in Brussels, on 13 December 2016

For the Working Party,
The Chairwoman
Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

For the Working Party
The Chairwoman
Isabelle FALQUE-PIERROTIN