ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 242

Guidelines on the right to data portability

Adopted on 13 December 2016

TABLE OF CONTENTS

Executive summary

Article 20 of the GDPR creates a new right to data portability, which is closely related to but differs from the right of access in many ways. It allows for data subjects to receive the personal data, which they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit them 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 the new right of data portability. This right allows for data subjects to receive the personal data, which 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 consumer 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 to provide the requested information. **The new right to data portability aims at empowering 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**. Indeed, the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers). It also enables the creation of new services in the context of the digital single market strategy[1].

This right also represents an opportunity to "re-balance" the relationship between data subjects and data controllers, through the affirmation of individuals' personal rights and control over the personal data concerning them.

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). Some synergies and even benefits to individuals may emerge between these 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

First, data portability is a **right to receive personal data** processed by a data controller, and to store it for further personal use on a private device, without transmitting it to another data controller.

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 "*in a structured, commonly used and machine-readable format"*. For example, a data subject might be interested in retrieving his current playlist from a music streaming service to find out how many times he listened to specific tracks in order to check which music he wants to purchase on another platform. He

[1] 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".

may also want to retrieve his contact list from his webmail application to build a wedding list, or get information about purchases using different loyalty cards, to assess his or her carbon footprint.[2]

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

Second, Article 20(1) provides data subjects with the **right to transmit personal data from one data controller to another data controller** "without hindrance". 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. This right facilitates the ability of data subjects to move, copy or transmit personal data easily. 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 control of the data subject.

This right aims to foster innovation in data uses and to promote new business models linked to more data sharing under the data subject's control[3]. Data portability can promote the controlled sharing of personal data between organisations and thus enrich services and customer experiences[4]. Data portability may facilitate user mediated transmission and reuse of personal data concerning them among the independent services they are interested in.

- **Data portability tools**

On a technical level, data controllers should offer different implementations of the right to data portability. For instance**, they should offer a direct download opportunity for the data subject but should also allow data subjects to directly transmit the data to another data controller.** This could be implemented by making an API[5]available. Data subjects may also wish to use of a personal data store or a trusted third party, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required, so data can be transferred easily from one controller to another.

- **Controllership**

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.

---

[2] In these cases, the processing performed on the data by the data subject falls within the scope of household activities and therefore no longer falls within the scope of the GDPR.

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

[4] 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.

[5] An application programming interface (API) is a set of subroutine definitions, protocols, and tools for building software and applications. It refers to 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

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[6]. Importantly, there is no additional requirement to commence retention of such data simply to service a potential data portability request.

At the same time, a receiving data controller[7] 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 request applying to a webmail service, where the right to data portability is used to retrieve emails and when the data subject decides to send them to a secured storage 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. Similarly, in the case a data subject request transmission of details of his or her bank transactions to a service that assists in managing his or her budget, the new data controller does not need to retain all the details of the transactions once they have been labelled.

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' data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data[8].

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

When an individual exercises his or her right to data portability (or other right within the GDPR) he or she does so without prejudice to any other right. A data subject can continue to use and benefit from the data controller's service even after a data portability operation. Equally, if the data subject wants to exercise his or her right to erasure, data portability cannot be used by a data controller as a way of delaying or refusing such erasure.

Data portability does not automatically trigger the erasure of the data from the data controller's systems and does not affect the original retention period applying to the data which have been transmitted, according to the right to data portability. The data subject can exercise his or her rights as long as the data controller is still processing the data.

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.

III. <u>When does data portability apply?</u>

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

[6] 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.

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

[8] 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.

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 other 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[9].

In addition, the right to data portability only applies if the data processing is "carried out by automated means", and therefore does not cover 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.

<u>First condition: personal data concerning the data subject</u>

Only personal data is in scope of a data portability request. Therefore, any data, which is anonymous[10] 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 well 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 must not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an

[9] 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).

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

example, telephone 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. 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, **the data controller must also include the personal data that are generated by and collected from the activities of users in response to a data portability request** such as raw data generated by a smart meter. This latter category of data does not include data that are exclusively generated by the data controller 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 are included** in the scope of the right to data portability (for example, mailing address, user name, age, etc.)
- **Observed data are "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 fitness or health trackers.

In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". These personal data do not fall within the scope of the right to data portability. For example, a credit score or the outcome of an assessment regarding the health of a user is a typical example of inferred data. 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.[11]

In general, given the policy objectives of the right to data portability, **the term "provided by the data subject" must be interpreted broadly, and only to exclude "inferred data" and "derived data",** which include personal data that are generated by a service provider (for example, algorithmic results). **A data controller can exclude those inferred data but**

[11] 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).

should include all other personal data provided by the data subject through technical means provided by the controller[12].

Thus, the terms "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour but not subsequent analysis of that behaviour. By contrast, any personal data which have been generated 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 intends to avoid 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).[13]

Such an adverse effect would occur, for instance, if the transmission of data from one data controller to another, under the right to data portability 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 them. Where personal data of third parties are included in the data set, another ground for lawfulness of processing must be identified. For example, a legitimate interest under Article 6(1)(f) may be pursued by the data controller to whom the data is transmitted, 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.

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 are relating 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 the data subject.

A similar situation occurs when a data subject exercises his or her right to data portability on his or her bank account, since it can contain personal data relating to the purchases and transactions of the account holder but also information relating to transactions, which have been "provided by" other individuals who have transferred money to the account holder. In

[12] 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

[13] 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."

this context, the rights and freedoms of the third parties are unlikely to be adversely affected in the webmail transmission or the bank account history transmission, if their data are used for the same purpose in each processing, i.e. as a contact address only used by the data subject, or as a history of one of the data subject's bank account. Conversely, their rights and freedoms will not be respected if the new data controller uses the contact directory for marketing purposes.

Therefore, to prevent adverse effects on the third parties involved, the processing of such a directory 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 data subjects. 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.

To further help reduce the risks for other data subjects whose personal data may be ported, all data controllers (both the 'sending' and the 'receiving' parties) should implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data. Additionally, they 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. because they as well want to move their data to some other data controller. Such a situation might arise with social networks.

With respect to data covered by intellectual property and trade secrets:
The rights and freedoms of others mentioned in Article 20(4) can also refer to "*the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software*" mentioned in recital 63, in order to protect the business model of data controllers (Article 15). 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*".

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 transfer the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.

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 the data subjects regarding the availability of the new right to portability**, as required by Articles 13(2)(b) and 14(2)(c) of the GDPR[14].

In providing the necessary clear and comprehensive 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 using the portability right or the access right.

In addition, the Working Party recommends that data controllers always include information about the right to data portability before any account closure. 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 a best practice for "receiving" data controllers, the WP29 recommends that they provide data subjects with complete information about the nature of personal data which are relevant for the performance of their services. 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 does provide 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 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.

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,

[14] 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."
Article 12 also requires that data controllers "facilitate the exercise of data subject rights under Articles 15 to 22" and "not refuse to act on the request of the data subject" when such a request is received ("unless the controller demonstrates that it is not in a position to identify the data subject").

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[15], 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 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 within one month of the original request.

Data controllers operating information society services are technically able to comply with requests within a very short time-period. To meet user's 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 indicate to the data subject "*the reasons for not taking action and on the possibility of lodging a 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*". 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. For information society or similar online services that specialise in automated processing of personal data, it is very unlikely that the answering of multiple data portability requests should generally be considered to impose an excessive burden.

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

[15] Article 12(3)

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 is the expected data format?**

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-readable format".* Recital 68 provides a further clarification that this format should be *interoperable,* a term that is defined[16] 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 the Directive 2013/37/EU[17] 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, but should always be chosen to achieve the purpose of being interpretable. 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*

[16] 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

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

maintain processing systems which are technically compatible." **Thus, portability aims to produce interoperable systems, not compatible systems.**[18]

Personal data are expected to be provided in formats, which have a high level of abstraction. 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 user passwords, payment data, biometric patterns, etc.). This additional data processing will be considered as an accessory to the main data processing, since it is not performed to achieve a new purpose defined by the data controller.

Data controllers should provide as many metadata with the data as possible at the best possible level of granularity, which preserves the precise meaning of exchanged information. As an example, providing an individual with .pdf versions of an email inbox would not be sufficiently structured. E-mail data must be provided in a format which preserves all the meta-data, 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 meta-data on the only assumption 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). EIF has created "An interoperability framework", 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."[19]

- **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, which 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, which 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 entire catalogue. The data controller should provide an overview "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" preferably (see Article 12(1)) of the GDPR) in such a way that data subject can use software applications to easily identify, recognize and process specific data from it.

[18] 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."
[19] Source : http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

One of the ways in which a data controller can answer requests for data portability is by offering an appropriately secured and documented Application Programming Interface (API). This would enable individuals to make requests 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 API, it may 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, the 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 ('integrity and confidentiality')" 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:

<u>How to ensure that personal data are securely delivered to the right person?</u>
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 that personal data is securely transmitted (e.g. by use of encryption) to the right destination (e.g. by use of additional authentication information). Such security measures mustn't be obstructive in nature and must not prevent users from exercising their rights, e.g by imposing additional costs.

<u>How to help users in securing the storage of their personal data in their own systems?</u>
By retrieving their personal data from an online service, there is always also the risk that users may store them in a less secured system than the one provided by the service. The data subject should be made aware of this in order to take steps to protect the information they have received. The data controller could also, as a best practice, recommend appropriate format(s) and encryption measures to help the data subject to achieve this goal.

* * *

Done in Brussels, on 13 December 2016

For the Working Party,
The Chairman