Document 13.

00xxx/xx/EN
WP xxx

Opinion/Guidelines/Guidance x/2016 on the concept of "data portability"

DRAFT VERSION

Adopted on XXX 2016

TABLE OF CONTENTS

Executive summary [TO BE DONE] **3**
I. Introduction **3**
II. What is data portability and when does it apply? **4**
III. What are the main elements of data portability? **8**
IV. How do the general rules governing the exercise of data subject rights apply to data portability? **10**
V. How must the portable data response be provided? **12**
VI. Conclusions **15**

Executive summary [TO BE DONE]

Article 20 of the GDPR creates a new right to data portability which differs from the right of access in many ways and allows for individuals to receive the personal data previously provided to a data controller, in a structured, commonly used and machine-readable format. The purpose of this new right is to support user choice, control and empowerment, through the affirmation of individuals' personal right over their personal data.

Since it allows the direct transfer of personal data from one service provider to another, under the data subject control, the right to data portability is an important tool that will helps to ensure the free flow of data in the EU and to raise competition between controllers. It will make it easier for individuals to switch between different providers, and enhance the development of services in the context of the digital single market strategy. Actually, it can promote the controlled sharing of personal data between organisations and thus enrich services and customer's experiences.

This opinion provides guidance on the way to interpret and implement the right to data portability as introduced by the GDPR. It is presented in a question-answer format to guide readers to a better understanding of this new right. It aims at providing a clear definition of 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 appreciate whether or not data should be considered as "provided" by the data subject and are, as such, subject to data portability.

The opinion stresses in addition that the right to data portability may involve two data controllers, the first one providing the data to answer the data subject request and the second one receiving the data according to the data subject's wishes. The guidance helps data controllers to clearly understand their obligations and recommends best practices and tools that guarantee its full effectiveness to the right to data portability. Finally, the opinion 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. The opinion is not over-prescriptive in this respect, given the wide range of potential data types that could be processed by a data controller. The key element to define the most appropriate format is to ensure that the data requested are still interpretable.

I. Introduction

The General Data Protection Regulation (GDPR) introduces the new right of data portability. This right allows for individuals to receive the personal data, which they have provided to a data controller, in a structured, commonly used and machine-readable format. They also have the right 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 to obtain a copy of their personal data under the subject access provisions of the Data Protection Directive 95/46/EC were constrained, among others, by the format chosen by the data controller to provide the requested information.

While, as the volume of personal data – especially transactional data - processed has increased in recent years the subject access rights of the Data Protection Directive 95/46/EC have not kept pace with the needs of data subjects. The right to data portability can be described as a way to "rebalance" the relationship between data controllers and data subjects, through the affirmation of individuals' personal right over their personal data.

Although data portability is a new right in the context of personal data, other types of portability may 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.

Additionally, the right to personal data portability can be seen as a way to enhance competition between services (by making it easier for individuals to switch between different providers) and to enable the creation of new services in the context of the digital single market strategy (this strategy might itself include some other forms of portability[1]).

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 individuals to make the best available use of this new right.

II. What is data portability and when does it 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.

Article 20(1)(a) of the GDPR describes which data processing operations are within scope of the right to data portability. In order to come under the scope of data portability, processing operations should be based:

- either on the data subject's consent (pursuant to Article 6(1)(a) relating to the lawfulness of the processing of personal data , Or pursuant to Article 9(2)(a) when it comes to special categories of personal data);
- or, alternatively, on the necessity to perform a contract to which the data subject is a party pursuant to Article 6(1)(b).

As an example, data collected by a fitness-tracking device and provided by the individual to a data controller would be within the scope of a request for data portability as they are processed based on the consent of the data subject. The titles of books purchased by an individual from an online bookstore, or the songs listened to via a music streaming service are

[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".

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 party.

The GDPR does not establish a right to data portability for cases where the processing of personal data is not based on consent or contract[2]. For example, 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 access 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 tax filings.

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?**

Under the provisions of the Data Protection Directive 95/46/EC, data controllers are already familiar with the right to subject access. This can be a request for any and all personal data held about an individual.

In contrast, the personal data within the scope of a request under the right to data portability is subject to further conditions. Pursuant to Article 20(1), to be within scope, data must be:

- personal data concerning him or her, and
- which he or she has *provided* to the 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 portability request. Therefore, any data, which is anonymous[3] or does not relate to the individual making the request, will not be in scope.

Data controllers that provide services across a community where individuals can interact with one another, should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, a bank account will 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 deposited money to the account holder. A similar situation occurs with telephone records where the account

[2] See recital 68 and Article 20(3) of the GDPR. 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).

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

history of a subscriber will include details of third parties involved in incoming and outgoing calls. Each of these records will concern the individual making the data portability request and would therefore need to be provided to comply with a data portability request. However, where such records are then transferred to a new data controller, they should not be processed for any purpose which would adversely affect the rights and freedoms of the third-parties (see below: 3rd condition).

Second condition: data provided by the data subject

The second statement narrows the scope to data "provided by" the data subject. There are many examples of personal data, which will be knowingly, intentionally and directly "provided by" the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, the data controller should also include the personal data that are generated by and collected from the activities of users in response to a data portability request. This latter category of data does not include data that are exclusively generated by the data controller.

A distinction can be made between observed data and inferred data.

- Data knowingly provided by the data subject are included in the scope of the right to data portability
- Observed data may for example include a person search history, traffic data and location data. It may also include raw data such as the heartbeat tracked by fitness or health trackers. Such "observed" data are actually "provided" by the data subject by virtue of the use of the service or the device.
- Inferred data and derived data in contrast, are created by the data controller. For example, a credit score or the outcome of an assessment regarding the state of 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, depending on the context, these data will not be considered as "provided by the data subject" and thus not within scope.

Given the policy objectives of the right to data portability, the term "provided by the data subject" should be interpreted broadly, and only to exclude "inferred data", that is, personal data that are generated 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, whether directly or indirectly. 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.

Thus, the phrase "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. 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 from the personal data provided by the data subject. These data are therefore not within the scope of the right to data portability. However, such data may still be within the scope of other rights, for example, subject access.

Therefore, data collected through the tracking and recording of the data subject should be considered as "provided by" him or her even if the data are not actively or consciously transmitted.

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

- **With respect to third parties' personal data:**

The third statement intends to avoid:

- the retrieval and transmission of data, containing the personal data of another (non-consenting) data subject, to a new data controller; and

- the processing of that third party data in a way that would prevent the third party from further exercising their rights.

Indeed, Article 20(4) of the GDPR provides that compliance with the right to data portability shall not adversely affect the rights and freedoms of others third parties personal data. Recital 68 states "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."

A clear example of such an adverse effect is a situation in which the exercise if data portability would prevent third parties from exercising their rights.

The data subject initiating the transfer of his data to another data controller, either gives consent to the new data controller for processing or enters into an agreement with them. Where personal data of third parties are included in the data set, another ground for lawfulness must be identified. In this respect, the initiating data subject may have legitimate reasons to transfer data relating to third parties to a new data controller. The context and purpose of the portability request should be taken into account when applying art. 6(1)(f) to recognize the legitimate interest of the new data controller as a legal ground allowing the processing of third party data. A legitimate interest may also be pursued by the data controller to whom the data is transferred, in particular when the purpose of the data controller is to provide a service to the data subject which allows the latter to process personal data for a purely personal or household activity.

For example, a webmail service may allow creation of a directory of a data subject's contacts, friends, relatives, family and broader environment. This is for example the case with a webmail service. Since these data are relating to, and are created by the identifiable individual that wishes to use the right to data portability, data controllers should transfer the entire directory of incoming and outgoing e-mails to the data subject.Nonetheless, to prevent adverse effects on the third parties involved, the processing of such a directory by a third party, such as a webmail provider, is allowed only to the extent that the data are kept under the sole control of the requesting user and it are only managed for purely personal or household needs. A receiving 'new' data controller (to whom the data can be transferred at the request of the user) may not use the transferred third party data for their own purposes. Otherwise, such processing is likely to be illegal and unfair, especially if the third parties concerned are not informed and cannot exercise their rights.

To further help reduce the risks for third parties whose persona data may be ported, the Working Party recommends that all data controllers (both the 'sending' and the 'receiving'

parties) implement tools to enable the data subject to select the relevant data and exclude third party data.

- **With respect to data covered by intellectual property and trade secrets:**

The rights and freedom 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 when answering a request to exercise the right to access (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 may therefore not be the basis for a refusal to answer the portability request.

III. What are the main elements of data portability?

The GDPR defines the right of data portability in Article 20, but this opinion will also address explicit references to this right in other recitals and provisions. Article 20(1) of the GDPR states that:

> *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 [...]*

First, data portability can be seen as a **right to receive personal data** processed by a data controller, and to store it for further personal use on a private device, without transferring it to another data controller.

In this case, data portability can be compared to the right of access. The difference between the two rights is that data portability offers an easy way for the data subjects to manage their personal data themselves, in so far these data should transferred "*in a structured, commonly used and machine-readable format*". For example, a data subject might be interested in retrieving his current playlist 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 may also want to retrieve his contact book from his webmail application to build a wedding list, or get information about purchases from different loyalty cards, to assess his or her consumption carbon footprint. In these cases, the secondary processing performed on the data received by the data subject is no longer the responsibility of the data controller and may fall under the "household exemption".

Second, Article 20(1) provides data subjects with the **possibility to transmit their 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 to obtain, transfer and reuse the data they have provided to different services. This right facilitates their ability to move, copy or transfer personal data easily ("without hindrance" according to art. 20 of the GDPR) from one IT environment to another, without obstruction to such reuse. 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.

In this respect, the right to data portability should not only be considered by data controllers as a risk that facilitates the export of customer's data to direct competitors. 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[4]. Data portability can promote the controlled sharing of personal data between organisations and thus enrich services and customer's experiences. The so-called quantified self and IoT industries have shown the benefit 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. Data portability may facilitate such user mediated transfer and reuse of their personal data among the independent services they are interested in.

On a technical level, data controllers should offer two different implementations of the right to data portability. They should offer a direct download opportunity for the data subject but should also allow data subjects to directly transfer the data to a third party. This could for example be implemented by making available an API[5]. Data subjects should be enabled to make use of a personal data store, 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.

Data controller that answer data portability requests, under the conditions stated by Article 20 of the GDPR, are not responsible for the further processing handled by another company receiving personal data. However, a receiving data controller 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. This information is not relevant with regard of the purpose of the new processing and should not be kept and processed. Similarly, in the case a data subject request transmission of details of his 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 the 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 states the purpose of the new processing before any transmission of the portable data. 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

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

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

purposes, even if the data is 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 immediately.

Data controllers must also bear in mind that **when an individual exercises his right to data portability (or other right within the GDPR) he or she does so without prejudice to any other right**.

The 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 right to erasure, data portability cannot be used by a data controller as a way of delaying or refusing such erasure. In addition, 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, of which a copy has been transferred. The data subject can exercise his or her rights as long as the data controller keeps the data.

Should an individual 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..

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 individuals regarding the availability of the new right to portability, as required by Articles 13(2)(b) and 14(2)(c) of the GDPR.

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*").

In providing the necessary clear and comprehensive information data controllers must ensure that they distinguish the right to data portability from other privacy rights, and especially the right of access. Therefore, WP29 recommends 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. Data subjects must be in a position to understand which right is the most appropriate for them to achieve the desired results.

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 tke stock of their personal data, and to easily transfer 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 (in combination with the recommendation mentioned above that all data controllers should implement tools that allows users to select and exclude data) to limit the risks for third parties.

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

Article 11(2) of the GDPR states that the data controller may refuse to comply with a request for data when the processing does not "require the identification of a data subject" and if he is unable to identify the data subject or if he is not able to identify which data relate to the individual making the request (Article 12(2)). This does not however prevent the data subject from providing additional information to confirm his or her identity. The data controller may request additional information if necessary (Article 12(6) of the GDPR).

Where the data subject, for the purpose of exercising his or her rights, provides additional information enabling his or her identification, the data controller shall answer the request. Where information and data collected online is linked to pseudonyms or unique identifiers, WP29 recommends data controller putting in place appropriate procedures enabling an individual to make a data portability request and receive the data relating to him or her. Data controllers must have an authentication procedure in place in order to strongly ascertain the identity of the data subject requesting his personal data or more generally exercising the rights granted by the GDPR. In many cases, such authentication procedure is already in place. For example, usernames and passwords are often used to allow individuals to access their data held 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.

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

Article 12 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*" 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.

Where the data controller operates an information society service, data controllers are technically able to comply with requests within a very short time-period. To meet the user's expectation, it might be recommended to define the delay in which a data portability request can be answered and to communicate this delay to the 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 he is asked to answer a data portability request.

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

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 or similar online services that specialise in automated processing of personal data, answering multiple data portability requests will not be soon be considered to impose an excessive burden.
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 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 overall 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 response 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[6] 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 guarantee 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[7] 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*

[6] 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.
[7] Amending Directive 2003/98/EC on the re-use of public sector information.

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.

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. 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.

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 level of precision and granularity, which preserve 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.

The 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 is a challenge that has already 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."[8]

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

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

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 interesting 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 (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.

As mentioned above, 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 unable 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.

If the size of data requested by the data subject makes transfer via the internet problematic, rather than potentially allowing for an extended time period of a maximum of three months to comply with the request[9], 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).

- **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.

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

- How to 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 transfer may become a possible source of risk regarding those data (in particular of data breaches during the transfer). The data controller is responsible for taking all the security measures needed to ensure that personal data is securely transferred (e.g. by use of encryption) to the right destination (e.g. by use of additional authentication information).

[9] Article 12(3)

- How to help user in securing the storage of their personal data in their own system?

By retrieving their personal data from an online service, 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 recommend appropriate format(s) and encryption measures to help the data subject to achieve this goal.

VI. Conclusions

* * *

Done in Brussels, on day Month 2016

For the Working Party,
The Chairman

Annex

Examples of applicable national law:

1/ [FR] « Projet de loi République numérique » (in discussion in the French Parliament)

2/ UK: Enterprise and Regulatory Reform Act 2013
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/294798/bis-11-749-better-choices-better-deals-consumers-powering-growth.pdf

Examples of projects around Midata initiative in EU Member States:

- Personal current accounts: an effort to enable individuals to download a CSV file of 12 months current account data

- An information website: http://www.pcamidata.co.uk/

- A price comparison website where individuals can upload their CSV file to compare across existing current account providers: https://money.gocompare.com/currentaccounts/midata#/

- Another website which can process a midata file to determine potential financial issues: https://www.accountscore.co.uk/

- Some energy companies are also providing a similar service but there is no price comparison website: https://www.eonenergy.com/for-your-home/help-and-support/midata

-