Document 11.

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]

The concept of data portability ...

This opinion provides guidance on the way to interpret and implement the right data portability as introduced by the GDPR.

I. Introduction

The General Data Protection Regulation (GDPR) introduces a new right for individuals to receive the personal data which they have provided to a data controller in an electronic format, in certain circumstances, free of any restriction on its re-use by the data subject. This right complements those found in competition legislation and supports user choice, user control and consumer empowerment.

Individuals making use of their right to obtain a copy of personal data under the subject access provisions of the Data Protection Directive 95/46/EC were constrained by the format chosen by the data controller to create the "permanent copy" of the personal data which had been requested.

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 subject and data controller alike. Indeed, some data controllers may have developed a structure which promotes their exclusive use regarding the personal data which have been provided by data subjects which they then process to provide their services. 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 individual's personal right over their personal data.

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

The right to personal data portability can be seen additionally as a way to enhance competition between services 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 is aimed at data controllers who are subject to the obligations of the GDPR and provides guidance on this important new right so that they can be in a position to update their

[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"

practices, processes and policies and to enable individuals to make the best available use of their new right.

II. What is the scope of data portability?

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

As with the Data Protection Directive 95/46/EC, general compliance with GDPR requires data controllers to have a clear legal basis for the processing of personal data and must ensure that they comply with all the necessary legal obligations of this basis.

Article 20(1)-a of the GDPR describes which data processing operations are within scope of the right of data portability. The legal basis of such processing operations should be based :

- either on the data subject consent :
    - pursuant to point (a) of Article 6(1) relating to the lawfulness of the processing ;
    - or to point (a) of Article 9(2) regarding the exceptions to the general prohibition applying to the processing of special categories of personal data ;
- or on a contract to which the data subject is or is going to be a party pursuant to point (b) of Article 6(1).

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 on the basis of the consent of the data subject. The title of books purchased by an individual from an online bookstore, or the songs listened on a music streaming service are other examples of personal data that generally is 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 processing of personal data is based on a legal ground other than consent or contract[2]. For example, Article 20(3) and Recital 68 state that data portability can't legitimise a demand to a data controller when the data processing is exclusively occurring for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or when a data controller is exercising its public duties or complying with a legal obligation.

Therefore, there is no obligation for controllers to provide for portability in these cases. However, developing processes to automatically answer access requests, by following the principles governing the right to data portability, can be considered as a good practice. 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 does not cover paper files.

---

[2] See recital 68 and Article 20(3). For data portability as a good practice in case of processing on legitimate interest ground and for existing voluntary schemes, see pages 47 & 48 of WP29 Opinion 6/2014 on legitimate interests (WP217).

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

Under the provisions of the Data Protection Directive 95/46/EC, data controllers were already familiar with the right to subject access. This can be a request for all personal data held about an individual. In contrast, the personal data within scope of a request under the right to data portability may not include *all* personal data held by a data controller.

Article 20(1) states that to be within scope, data must be:
- Personal data concerning him or her, and
- Which he or she has *provided* to the data controller

1st condition: personal data concerning the data subject

The first of these statements makes it clear that only personal data is in the scope of a portability request. By corollary, any data which is anonymous[3] or does not relate to the individual making the request will not be in scope.

Data controllers which 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 will exist in telephone records where the account 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.

2nd 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. mail, user name, age) submitted via online forms. But it may not be clear to the individual that personal data is generated and collected from their activities (as opposed to generated by the data controller) and should then be included in response to a data portability request.

We can distinguish between:
- Observed data which for example may include our search history, traffic data and location data, or raw data such as our 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 also included in an individual's profile, such as, for example, his credit score or the outcome of an assessment regarding his state of health. Based on context, this data will probably not be considered portable data.

The term "provided by the data subject", in the context of the policy objective, should be interpreted as aiming to exclude "inferred data" only, that is, personal data and generated by a

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

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 provided by the data subject, and including all data observed about the data subject during the normal activity for the purpose of which data is collected.

Thus, the phrase "provided by" includes personal data relating to the data subject activity or resulting from the observation (but not subsequent analysis) of an individual's behaviour.

As a consequence, data collected through the tracking and recording of the data subject's actions should also be considered as "provided by" him even if they are not actively or consciously transmitted. Such personal data can include a transaction history or access log including those which have been collected through observation or monitoring of the data subject. To be clear, not all transaction or log data will be within scope of the right of data portability. Any personal data which has been generated by the data controller as a part of its 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 and therefore not within scope of data portability. However, such data may still be within scope of other rights, for example, subject access.

3rd condition: the right to data portability shall not adversely affect the rights and freedoms of others

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

Article 20(4) states that compliance with this right shall not adversely affect the rights and freedoms of others and ensure that the data communicated do not concern third party (see above : data portability is about getting personal data, but not third parties personal data).

In this respect, it is worth stressing that portable data might include in some cases information relating to the data subjects' relatives and family. For example, a webmail service may allow creation of a directory of the complete picture of a data subject's relationships, close relatives and more generally of his environment. Transferring such an electronic directory from one webmail service to another may be considered as a common operation under the new right to data portability. In this case, the directory as a whole can be qualified as personal data set relating to an identifiable individual. Nonetheless, the processing of this directory by a third party, such as a webmail provider, is acceptable to the extent that it is kept under the sole control of the user and it is only managed for purely personal or household needs. Third party data included in a set of information transferred by a data subject shall not be used by the "receiving" data controller for his own purposes. Otherwise, such processing might be considered as illegal and unfair, especially if the third party concerned are not informed and cannot exercise their rights.

Article 20(4) intends to avoid situations where the data portability right will cause retrieval and transmission to a third party if the data contains the personal data of another (non-consenting) data subject, and that these third party data are processed in a way that would prevent that third parties from further exercising their rights.

- **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 on recital 63, ir order to protect data controllers business model when answering a right of access. 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*".

Some data controllers fear that the data set transferred in accordance with the right to data portability might be used by competitors to understand or steal the know-how and expertise supporting their business model. Any confidential business information which provides a data controller with a competitive advantage may be also considered a trade secret. In these cases, answering portability requests may be seen by some as a business risk to unveil trade secret information or to jeopardize intellectual property rights. However, 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 can constitute a violation of intellectual property rights, and a consideration of this should 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 although there are explicit references to the right throughout other provisions and articles which are discussed in this opinion. Further guidance is also offered in Recital 68. 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 being that it provides better transparency and an easy way for the data subject to manage his personal data on its own. For example, a data subject might be interested in retrieving his current playlist and check 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 purchases information from different loyalty cards database to assess their 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, the GDPR clearly states that data portability provides **the possibility to transmit personal data from one data controller to another data controller** "without hindrance". In essence, data portability provides the ability for data subjects to obtain, transfer and reuse the data they have provided for their own purposes and across different services. This right

facilitates their ability to move, copy or transfer personal data easily (or "without hindrance" according to art. 20 of the GDPR) from one IT environment to another, without obstructing its reuse. In addition to providing consumer empowerment by preventing "lock-in", it is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the permanent control of the data subject.

In this respect, the right to data portability should not be considered by data controllers only as a way to facilitate the export of their customer's data to direct competitors. It is clearly intended at fostering innovation in data uses and promoting new business models linked to more data sharing under the data subject's control[4]. Data portability can create new business models by promoting user controlled sharing of personal data between organizations, to 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 from a single location. 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, a data portability response received by a data subject could be provided to a new data controller by later uploading or transmitting the contents as provided by the original data controller. Alternatively the portability requirement could be exercised by using an API[5] made available by the original data controller. An individual can also 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 process the personal data as required.

If the first data controller is responsible for answering data portability requests, under the conditions stated by article 20 of the GDPR, he is not responsible for the further processing handled by another company receiving personal data on the initiative of the data subject. This means that the first data controller is not responsible for data that have been ported. However, a receiving controller is responsible for ensuring that the portable data provided is 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 attached documents to 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.

A "receiving" organization becomes the new data controller regarding these personal data and must respect the principles stated in article 5 of the GDPR. As a consequence, the purpose of the new processing should be clearly and directly indicated to the users before any transmission of portable information. The new data controller should not process personal data which are not relevant and processing must be limited to what is necessary for the new purposes, even if the data is part of a more global data-set transmitted through a portability process. Personal data which are not useful to achieve the purpose of the new processing should be deleted immediately.

---

[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

Data controllers must also bear in mind that **when an individual exercises his right to data portability (or other right within the GDPR) he 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 erasure. In addition, it's worth noting that data portability does not automatically trigger the erasure of the data from the data controller's systems and does not impact the original retention period applying to the data, of which a copy has been transferred. The data subject can exercise his rights as long as the data is kept by the data controller.

Eventually, should an individual discover that personal data requested under data portability does not fully address their request, any further request for personal data under a right of access should be fully complied with, in accordance with article 15, as though the original request for data portability had not taken place.

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?

The first important part of compliance with the new right to data portability will be for the data controller to inform individuals regarding the availability of this right, as required by Articles 13(2)(b) and 14(2)(c).

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 this 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. As a consequence, 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, such that they are in a position to understand which right is most appropriate for them to achieve the outcome being sought.

In addition, the data controller should consider communicating additional information about the right to data portability and its effects before any account closure, since exercising this right can be useful in the case of contract termination, allowing a user to take stock of their personal data and to easily move to another service provider.

Finally, as a best practice for "receiving" data controllers WP29 recommends providing data subjects with complete information about the nature of personal data which are deemed to be

relevant for the performance of their services. WP29 also recommends the implementation of tools enabling the data subject to select the relevant data and exclude third party data.

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

Article 11(1) states that the data controller may refuse to comply with a request for data 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 10). This does not however prevent either the data subject providing, or the data controller requesting, additional information to confirm the identity of the individual and it may be requested if necessary (Article 12(4a)).

Where the data subject, for the purpose of exercising his rights, provides additional information enabling his or her identification, the data controller shall answer his request. Where information and data collected online might not be directly linked to the civil identity of the data subject, but to pseudonyms or unique identifiers, WP29 recommends to each data controller to list the identifiers enabling an individual making a data portability request to only receive the data relating to him.

An authentication procedure should be in place in order to strongly ascertain the identity of the data subject requesting his personal data. However, identifying the data subject is a reasonably limited obligation. The data controller will be held accountable essentially for the collection of evidence proving that the personal data transferred relate to the individual making the request.

- **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, it will be expected that the data controller will be able to comply with requests immediately or within a few hours. Where is arises, it is up to the data controller to demonstrate why he cannot answer a data portability request within a short period.

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.

Respecting these delays and answering portability requests, even to reject them for some reasons that must be notified, are part of the data controller's obligations under the GDPR. 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*". As with providing information within a timely manner, there should be no excessive burden in the provision of multiple data portability requests.

In the case of data portability, and especially where a data controller operates an information society or similar online service with automated processing of those personal data, there should be very few cases where the data controller would be able to justify his refusal to deliver information, by using the criteria of excessiveness, 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 focuses on the requests made by one data subject and not on the overall requests received by one data controllers. 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 also provides a further clarification that this format might 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 according to the goal 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.*"

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 from 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 pattern, etc.). This additional data processing will not be considered as a new data processing operation but as an accessory to the main data processing, since it's not performed to achieve a new purpose defined by the data controller.

Data controllers should also be encouraged to provide data along with metadata, 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 to comply with the legislation. It would be better provided in a format which will preserve all the email meta-data. As such, when selecting a data format in which to provide the personal data, the data controller should consider how this will impact or hinder the individual's right to re-use the data. In cases where a choice is given to the data subject regarding the preferred format of the personal data a clear explanation of the impact of their decision 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 which may be used 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) to propose "An interoperability framework", which is an agreed approach to interoperability for organizations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices."[8]

---

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

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

The GDPR does not 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 be first be provided in a summarised form through the use of dashboards allowing the data subject to port interesting subsets of the personal data rather than the entire catalogue. The data controller may also need to provide supporting documentation explaining or describing the format selected in order to support the individuals use of the portability right. This should be provided in such a way that data subject can use software applications to easily identify, recognize and process specific data from it. When personal data are transmitted directly from one controller to another, the user should be in position to obtain the precise list of information which is available from the first controller and select those he wishes to transmit to the other.

A data controller could also provide access to the results of a request for data portability through an appropriately secured and documented Application Programming Interface (API). The individual could therefore 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 is specified in Article 20(2). By granting access to data via an API it may be possible to offer a more sophisticated access system where by an individual can make subsequent requests for data, either as a full download or 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 allow for the personal data to be transmitted directly to another data controller (as per Article 20(2) where technically feasible).

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

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

- How to ensure that personal data is securely delivered to the right person?

As data portability aims to get personal data out of the information system of the data controller, it 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 its personal data from an online service, the user 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 and may reuse. The data controller could also recommend appropriate format(s) and encryption measure 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 [to be deleted in final version, probably]

Current national legal framework :

1/ [FR] « Projet de loi République numerique » (in discussion in 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

+ projects around MiData initiative :

- 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