Document 10.

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 obtain access to the personal data which they have provided to a data controller in an electronic format, free of any restriction on its re-use. 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 – specially 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 (eg in the contexts of contract termination, communication services roaming and transborder access to services). Some synergies may emerge between these types of portability and even benefits to individuals 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 practices, processes and policies in advance of the GDPR coming into force and to enable individuals to make the best available use of their new right.

[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

II. What does data portability permits? / What can be done in accordance with the right to 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 retrieve 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 transferred is covered by the household exemption stated in article 2 (2) of the GDPR and falls out of the scope of the regulation.

Second, the GDPR clearly states that data portability provides **the right 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 "their" data for their own purposes and across different services. This right facilitates their ability to move, copy or transfer personal data easily from one IT environment to another, without hindrance to their "usability". 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 only be considered by data controllers 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 control[2]. Data portability can create new business models by sharing personal data between organizations, 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.

---

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

On a technical level, a data portability response could be provided to a new data controller by uploading or transmitting the contents as provided by the original data controller or alternatively the portability requirement could be exercised by using an API[3] 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.

In any cases, if the first data controller is responsible for answering to 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 does not have to control whether or not the portable data provided is relevant and not excessive with regard to the new data processing.

On the opposite, the "receiving" company 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.

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. Therefore, should an individual discover that personal data requested under data portability does not fully address their need, a 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.

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.

In addition, the new data controller should not keep information which are not relevant and limited to what is necessary for the purposes of the new processing, even if these data is part of a more global data-set transmitted through a portability process. Data which are not useful to achieve the purpose of the new processing should be deleted immediately.

III. How does 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).

---

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

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 gain access to 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, to take stock of the user situation and to easily move to another service provider.

Finally, if the data is transferred to another data controller, WP29 recommends as a best practice for the "receiving" data controllers to provide a complete information about the nature of 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 but 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. Since many 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 controllers to list the indicators helping to verify that an individual making a data portability request only access to the data relating to him. In any case, identifying the data subject is a best-efforts obligations. The data controller should be held accountable essentially for the collection of evidences 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.

Nonetheless, in many cases, especially 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.

According to the same provisions, 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.

If the data controller consider data portability requests to be manifestly unfounded or excessive, he will bear the burden of demonstrating it according to article 12. In that case, the controller may charge a reasonable fee consistent with the nature of the request, or refuse to act on the request.

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 global cost of the processes created to answer data portability should not be taken into account to appreciate 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 global implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests.

IV. What is the scope of data portability?

- **Which processings are potentially concerned by the right to data portability?**

Article 20 (1) of the GDPR provides further information on determining the data processing which is within scope of the right of data portability stating that it 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).

This further restricts the data that may be within the scope of a portability request to the information being processed with the consent of the individual (or explicit consent in the case of special categories of data) or for the performance of a contract.

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.
As an example, data collected by a fitness tracking device and provided by the individual to a data controller for further analysis 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 seems to be within data portability scope, 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[4]. For example, Article 20(3) and Recital 68 state that data portability can't legitimate 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 their public duties or complying with a legal obligation

Therefore, from a legal perspective, 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, as for example government service providing easy downloading of past tax filings.

- **<u>What personal data must be included?</u>**

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

[4] 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).

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[5] 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 is narrowing 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 (mail, user name, age, ...), 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. Based on the text of the GDPR, these data "observed" is actually data "provided" by the data subject.
- Inferred data also includes 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, for example because they are the results of a specific data processing that can be legitimately protected from transparency.

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, data that have specific added value generated by a service provider (for example, algorithmic results...). Data controller can exclude those inferred data but should include all other personal data relating to the data subject, whether directly or indirectly, willingly or unwillingly, knowingly or unknowingly provided by the data subject, including all data observed about the data subject during the normal activity for the purpose of which data is collected.

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.

---

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

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 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 created by the data controller as a part of its data processing, e.g. personalisation or recommendation process, user categorisation or profiling are data which are derived from the personal data provided by the data subject and not within scope of data portability but may still be within scope of other rights, such as 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 :**

Data controllers must remain mindful of Article 20 (4) which 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, not third parties 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, transferring an electronic directory created by the data subject from one webmail service to another will undoubtedly 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. The directory offers a complete picture of his relationships, close relatives and more generally of his environment. 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 to respond to his 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.

In addition, it may be necessary to limit the volume or details of some personal data made available where others are integral to the data portability response. This paragraph intends to avoid situations where data portability will induce retrieving and transmitting data to a third party if the data are also personal data of another (non-consenting) data subject, in a way that would prevent them from further exercising their rights.

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

The rights and freedom of others mentioned in art. 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, 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 and steal their know-how and expertise supporting their business model. Any confidential business information which

provides data controller with a competitive edge can be also considered a trade secret. In these cases, answering portability requests is seen by some as a business risk to unveil trade secret information or to jeopardize intellectual property rights.

Data controllers can address this concerns by two means. First, intellectual property rights and trade secret aim at sanctioning any unfair use of the information held by a data controller. It is not designed to restrict personal rights benefiting to individuals and consumers, acting for personal purposes. The protection offered by these rights result in prohibiting the unauthorized use of information. Misusing portable data can still be sanctioned as an unfair practice or as a breach to the protection of confidential trade information. As a consequence, answering a data portability request does not prevent the data controller to take legal action to defend or assert his interests, if the portable data is used unfairly by the data subject. Second, the communication of the data processed does not reveal in itself the nature of the processing performed to provide a specific service. Therefore, data controllers can adapt the format of their answer to portability requests, in order to circumvent any violation of trade secrets.

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 also provides a further clarification that this format must 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 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*

---

[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

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.

It should be noted that Recital 68 clarify 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 aim 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.

The expected data format requires a high level of abstraction from the enforcing platform. It aims at producing system able to communicate amongst themselves through well-defined and mutually known interfaces/data format and protocols. In this way, data controller should be encouraged to provide data along with metadata, at the best level of precision and granularity, which preserve the precise meaning of exchanged information. Metadata should contain precise identification and description on personal data transmitted without containing personal data itself in order to preserve syntactic interoperability on formats. The WP29 would strongly encourage 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.
A data controller could also provide access to the results of a request to data portability through an appropriately secured and documented Application Programming Interface (API). The individual could therefore make requests for their personal data via 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 also 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.

Given that the format of the data is required to be machine-readable it may make sense for many data controllers to provide access to requested data through existing online systems, (while observing the need for authentication and identification of those making the requests). Where this is not possible the data controller need to create such systems or provide an alternative means of providing the data such as using CD, DVD or other physical media.

The European Interoperability Framework (EIF) has already addressed this goal 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]

Furthermore, it is crucially important that the individual is in a position to be able to make further use of the personal data and therefore he or she understands the data definition, schema and structure of the personal data that is provided in such a way that they can use software applications to easily identify, recognize and process specific data from it. As an example, providing an individual with .pdf versions of an email inbox would not be sufficiently structured to comply with the legislation. The data controller may need to provide supporting documentation explaining or describing the format selected in order to support the individuals use of the portability right.

When selecting a data format in which to provide the personal data, the data controller should also consider how this will impact or hinder the individual's right to re-use the data. As an example, an email inbox would be better provided in a format which will preserve all the email meta-data. In cases of online file sharing services, this may be best achieved by providing it in the same format as provided by the user (eg .docx, .odt, and .jpg). In other cases, it will be best achieved by giving the user the choice which is most compatible with their intended purpose, eg exporting an address book from a social networking service in vCard, LDIF, CSV or other. 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 GDPR does not address the challenges of large or complex data structures or other technical issues which might create difficulties for data controllers, not least if the size of data requested by the data subject makes transfer via the internet problematic, other than potentially allowing for an extended time period of a maximum of three months to comply with the request[9]. In these scenarios the data controller may also need to consider an 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). It may also be the case that large data collections could 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.

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

The transmission of personal data to the data subject raises some security issues:

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

The idea of data portability being to get personal data out of the information system of the data controller, it's a possible source of risks regarding those data (in particular of data breaches during the transfer). The data controller is responsible to take all the security measure to ensure that personal data is securely transferred, (e.g. use of encryption) to the right destination (eg. use additional authentication information) in the view of the sensitiveness of the data. The data controller should also considered the period of time

[8] Source : http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf
[9] Article 12(3)

personal data should be retained in that format and location, once the personal data is ready for download/ transfer and once the retrieval by the user is successful. This would raise the question of responsibility that should be supported by the original data controller in the event of a problem during data transfer and how shall it be communicated to relevant parties and acted on.

- How to help user for securing 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 proposed by the service. The data subject should be aware of this and take steps to protect the information they have received and may reuse. The data controller should also chose the appropriate format(s) and encryption measure to ensure that data are securely stored in the local system of the data subject.

- How to preserve the data controller from revealing internal mechanism of their systems?

The topology of data retrieved may reveal some internal mechanisms on the data controller's services, which could potentially also expose their vulnerabilities. For instance, allowing the extraction from a data processing may raise security and technical issues, especially for old data processing practices or operations that were not designed to take this into account.

The data controller should also considered personal data outside the scope of portability, as they could produce hazards for the information system of the data controller, the user account or trade secrets (such as user passwords, payment data, biometric pattern, etc.).

As such, data portability might imply an additional layer of data processing from the data controller. Nevertheless, it would not be considered as a new data processing since it's not performed to achieve a new purpose defined by the data controller. The operations needed to answer data portability requests are not different from those needed to address more classical data subjects rights (such as the right to access), even if it should be done with automated means. Such automated operations remain under the responsibility of the data controller.

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