WP242 ANNEX – Frequently Asked Questions

1. What is the purpose of the right to data portability?

In essence, data portability provides the ability for data subjects to obtain 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. 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 control of the data subject.

2. What does the exercise of the right to data portability allow?

First it is a right **to receive personal data** ("in a structured, commonly used and machine-readable format") processed by a data controller, and to store it for further personal use on a private device, without transferring it to another data controller. This right offers an easy way for the data subjects to manage their personal data themselves.
Second, this right also provides data subjects with the possibility to transmit their personal data from one data controller to another data controller "without hindrance", and facilitates their ability to move, copy or transfer personal data easily from one IT environment to another.

3. What are the tools recommended to answer data portability requests?

First, data controllers should offer a direct download opportunity for the data subject and, second, they should allow data subjects to directly transmit the data to another data controller. This could for example be implemented by making available an Application Programming Interface.

Data subjects may 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 access and process the personal data as required, so data can be transferred easily from one controller to another.

4. To what extent data controllers are responsible for the data transferred or received through the exercise of the right to data portability?

Data controller that answer data portability requests are not responsible for the processing handled by the data subject or by another company receiving personal data. At the same time, the receiving data controller is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing, that they have clearly informed the data subject of the purpose of this new processing and, more generally, that they have respected the data protection principles applying to their processing in accordance with the GDPR provisions.

5. Does the exercise of the right to data portability affect the exercise of the other data subject's rights?

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 exercise his or her

rights as long as the data controller is still processing the data. For example, the data subject can continue to use and benefit from the data controller's service even after a data portability operation. Equally, if he or she wants to exercise his or her right to erasure, to oppose or to access his or her personal data, the previous or subsequent exercise of the right to data portability cannot be used by a data controller as a way of delaying or refusing to answer other data subject's rights. Furthermore, data portability does not automatically trigger the erasure of the data from the data controller's systems and does not affect the original retention period applying to the data which have been transmitted, according to the right to data portability.

6. When does the right to data portability apply?

This new right applies under **3 cumulative conditions**.
First, the personal data requested should be processed, by automatic means (i.e. excluding paper files) on the basis of the data subject's prior consent or on the performance of a contract to which the data subject is a party.

Second, the personal data requested should concern the data subject and be provided by him. WP29 recommends to data controllers to not take an overly restrictive interpretation of the sentence "personal data concerning the data subject", when third parties data are contained in a data set relating to the data subject and provided by him, and are used by the data subject making the request for personal purposes. Typical examples of data sets including third parties data are the telephone records (which contains incoming and outgoing calls) a data subject would like to receive, or a bank account history that includes incoming payments from third parties.

Personal data can be considered as provided by the data subject when they are knowingly and actively "provided by" the data subject, such as account data (e.g. mailing address, user name, age) submitted via online forms, but also when they are generated by and collected from the activities of users, by virtue of the use of the service or the device. By contrast, personal data that are derived or inferred from the data provided by the data subject, such as a user profile created by analysis of the raw smart metering, are excluded from the scope of the right to data portability, since they are not provided by the data subject, but created by the data controller.

Under the third condition, the exercise of this new right should not affect adversely the rights and freedoms of third parties. For example, if the data set transferred on the data subject request contains personal data relating to other individuals, the new data controller should process these data only if there is an appropriate legal ground to do so. Typically, processing under the sole control of the data subject, as part of purely personal or household activities will be appropriate.

7. How to inform data subjects about this new right?

Data controllers should inform data subjects about the existence of the right to data portability "in a concise, transparent, intelligible, and easily assessable form, using clear and plain language". In this regard, the 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, as well as to provide specific information about the right to data portability before any account closure, to enable the data subject to retrieve and store his or her personal data.

In addition, data controllers receiving portable data on the data subject request can, as a best practice, provide data subjects with complete information about the nature of personal data which are relevant for the performance of their services.

8. How can the data controller identify the data subject before answering his request?

WP29 recommends that data controller put 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 or her personal data or more generally exercising the rights granted by the GDPR.

9. What is the time limit imposed to answer a portability request?

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 specialize in automated processing of personal data, it is very unlikely that the answering of multiple data portability requests should be considered to impose an excessive burden. In these cases, WP29 recommends to define a reasonable time frame adapted to the context and to communicate it to data subjects.

10. How must the portable data be provided?

The personal data should be transmitted in a structured, commonly used and machine-readable format. These specifications applying to the means should guarantee the interoperability of the data format provided by the data controller, interoperability being the desired outcome. Nonetheless, this does not mean that data controllers should maintain compatible systems. In addition, data controllers should provide as many metadata with the data as possible at the best level of precision and granularity, to preserve the precise meaning of exchanged information.

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.

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.