



COCIR

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

HEALTHCARE

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

COCIR comments on Art 29 Data Protection Working Party (WP29) Guidelines on the Right to Data Portability

COCIR welcomes the draft Guidelines on the Right to Data Portability. The document clarifies some important questions on how to interpret and implement the right to data portability as introduced by the General Data Protection Regulation (GDPR). It also provides very useful examples to understand under which circumstances this right applies. However, we would like to share our views on certain aspects covered by the draft Guidelines, with a view to contribute to improve the current version and clarify the obligations of data controllers.

In particular, COCIR considers that further clarification is needed on the following aspects included in the Guidelines:

1. Rationale of the right and when consumers will be entitled to exercise it
2. Interpretation of affected rights and freedoms
3. Security breaches and mitigating measures
4. Observed and inferred data
5. Common data formats

1. Rationale of the Data Portability Right

The wording of the current draft Guidelines correctly implies that the right to data portability is a consumer oriented right (*"This right, which applies subject to certain conditions, supports user choice, user control and consumer empowerment"*). Therefore, to determine if this new right can be exercised the initial question should always be whether the data subject (consumer) has a legitimate interest to transmit the data to another controller. In our view, the data subject can exercise this new right only when such a legitimate interest exists.

In this regard, COCIR believes that this "legitimate consumer interest" does not exist in the case of employees' personal data (with the exception of application files), as there is no legitimate interest to transmit data collected in an employment relationship to the next employer of the data subject. Moreover, if employers were to be required to transfer such data, their confidentiality interests might result adversely affected (Art. 20.4).

COCIR agrees with the view expressed by WP29 regarding the rationale that underpins the data portability right *"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 our view this implies that a legitimate interest only exists when data portability contributes to encourage competition and prevents "lock-in". Therefore, we consider that the legitimate interest condition is only met when a consumer requests to transfer his or her personal data between products or services that complement or substitute each other.

COCIR calls WP29 to further reflect on the ultimate aim of this new right and provide additional guidance regarding the context in which data subjects are entitled to exercise the data portability right. It should also be noted that further guidance on what constitutes "legitimate interest" will also



COCIR

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

HEALTHCARE

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

help to strike a fair and reasonable balance between the exercise of the data portability right and the costs to be borne by data controllers to satisfy legitimate requests.

2. Affected rights and freedoms (Recital 63 and article 20.4)

In reference to the exercise of the access right, Recital 63 of the GDPR states that “(access) right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software”. We believe that further clarification with regards to third parties “affected rights and freedoms” is needed in the context of the new data portability right.

In particular, we consider that the exercise of the new data portability right should not only be limited if it affects trade secrets and IP rights, but also when it affects confidentiality rights of the data controller.

For example, in the research domain the costs of obtaining and building valuable datasets are often high. However, these datasets are not always protected by intellectual property rights. Eventually, groups of data subjects included on the same dataset could be motivated to jointly request the transfer of their data to competitors, potentially limiting or adversely affecting competition and innovation. In this regard, COCIR believes that the exercise of the new data portability right should not only be limited when it affects trade secrets and IP rights, but also confidentiality rights of the data controller or contractual obligations.

3. Preventing security breaches

COCIR believes that securing portable data is critical. In this regard, WP29 notes that “*The data controller is responsible for taking all the security measures needed to ensure that personal data is securely transmitted (e.g. by use of encryption) to the right destination (e.g. by use of additional authentication information). Such security measures mustn’t be obstructive in nature and must not prevent users from exercising their rights, e.g by imposing additional costs*”. At the same time, WP29 recommends the use of APIs to enable the transmission of data from one controller to another. However, by introducing features such as APIs, that provide access to data that was previously not accessible, new security weaknesses can be introduced. Moreover, there is a risk that single identity fraud can turn into a long-lasting breach of personal data, since a hacker can easily port his false identity to other platforms.

In order to guarantee an adequate level of security, mitigating measures to reduce potential security breaches may need to be implemented including advanced authentication mechanisms, maximum number times to execute a portability request within a timeframe, notification of the data subject, a timeframe between the request and the execution, maximum amount of data transfer. Unfortunately, these measures by its very nature will be obstructive. COCIR calls WP29 to acknowledge the complexity of securely transferring personal data and provide further guidance on what constitutes “obstructive measures”.

4. Observed and Inferred Data

As the draft Guidelines clarify, so-called “observed data” will be covered by the data portability right only if *observed data are “provided” by the data subject by virtue of the use of the service or the device.* (e.g. for example with a health tracker app). Conversely, inferred data and derived data



COCIR

CO-ORDINATING COMMITTEE OF THE RADIOLOGICAL, ELECTROMEDICAL AND HEALTHCARE IT INDUSTRY

HEALTHCARE

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

created by the data controller on the basis of the data “provided by the data subject” do not fall within the scope of the right to data portability.

In our view, making an extensive interpretation of what data falls under the category of “observed data” (e.g. tracking data in an employment relationship or on a website)” will be too broad and not in line with the rationale behind this right. We call WP29 to provide further guidance on what type of data falls under the category of “observed data” and what data is to be considered “inferred and derived data”.

5. Commonly used format

COCIR believes that the Guidelines fail to effectively clarify what constitutes a “commonly used format”. Specially in the health IT domain it may not always be clear when formats are “sufficiently structured” and “commonly used”. Moreover, in our view, WP29 should clarify that data portability will be “technically feasible” when data conversion to “commonly used formats” can be easily performed and data conversion tools are available (e.g. available libraries must exist).