4.

POSITION PAPER

FEB
Federation of Enterprises in Belgium

FEB Position paper on the Working Party 29 guidelines regarding data portability

The General Data Protection Regulation (GDPR) introduces the data subject's right to data portability. Article 20 of the GDPR basically grants data subjects "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 personal data have been provided". Working Party 29 drafted up guidelines to clarify the signification of this new right.

FEB requests that the following matter(s) be addressed urgently:

1. The scope of data portability: in the GDPR the right to data portability is first and foremost a right of the data subject and not an instrument to encourage competition
2. Need for clarification concerning the liability of the controller and need to ensure proper security once the data has left the safe environment of the controller
3. A right to data portability is not equal to an obligation to import data
4. Privacy of third parties should be taken into account when applying the right to data portability

Arguments

1. **The scope of data portability: in the GDPR the right to data portability is first and foremost a right of the data subject and not an instrument to encourage competition**

The GDPR explicitly limits the scope of the data portability right to data "*which [the data subject] has provided to a controller*", a scoping choice by the legislator which is perfectly in line with the objective of the right to data portability, i.e. strengthening the control of the data subject over his or her own data and **avoid customer lock-in** (recital 68 GDPR).

The Working Party 29 Guidelines state that the data portability right covers not only data provided by the data subject (as the GDPR foresees) but also data observed or measured by the data controller in relation to the data subject. It is FEB's opinion that in this manner the Guidelines are extending the legal scope of the right to data portability.

FEB underlines that data portability should first and foremost be a right of the data subject and **not** become **an instrument that aims to encourage competition**. The GDPR is about data protection and protection of the data subject's rights, not about competition between controllers. Moreover, revealing observed data from one controller to another controller potentially exposes data subjects to a breach of their privacy since their observed personal data is actively revealed to a controller that may have no direct use for it, other than to learn what the competition is doing. Data subjects then must rely on the good faith of the receiving service provider not to misuse this personal data.

2. **Need for clarification concerning the liability of the controller and the need to ensure proper security once the data has left the safe environment of the controller**

When a data subject receives its personal data, following a request for data portability, the controller loses all control about what the data subject does with this data. Therefore FEB asks for a clarification of the liability of the controller and of the data subject.

Once the data subject has received the data he has to ensure the **security** of this data himself. **It is far from certain that the data subject will be able to do this**. Chances are very high that the data subject will store the personal data he obtains in a less secure environment. This is especially problematic when the transferred data is sensible personal data and/or contains personal data of third parties (e.g. bank transfers or calling lists).

It is clear that the controller can no longer be held liable for any damages that can affect the customer or third parties due to improper use of the data.

3. **A right to data portability is not equal to an obligation to import data**

The status of the data for the receiving controller in terms of responsibility, retention period, structure and security measures is unclear. FEB underlines that there is no clear legal ground on which a data subject will be entitled to oblige a service provider to import his data. As the responsibility of the **receiving controller** can be engaged, it should be **his decision to import data sets on the request of a data subject, or not**.

4. **Privacy of third parties should be taken into account when applying the right to data portability**

FEB fears that the interests of third parties whose personal data may also be revealed by a data portability request are insufficiently protected on the basis of the GDPR. The Working Party 29 Guidelines are limited to a number of suggestions on how this challenge could be handled, but there are **no concrete, practical solutions for controllers**.

There are different examples of possible third parties personal data that could be transferred in case of a request of data portability. E.g. banking sector: transaction details contain the banking accounts and names of third parties; telecom sector: the call lists contain telephone numbers of third parties.

Contact

FEB ASBL, rue Ravenstein 4, 1000 Brussels - T 02 515 08 11 - www.feb.be - Twitter: @VBOFEB