The Data Protection Circle

Data Portability vs. Data Privacy

I must admit I have difficulties to understand the GDPR's provision on data portability (Article 20 – Right to data portability). When switching from service provider « A » to service provider « B », the data subject will have the right to transmit the data concerning him or her from « A » to « B » (a direct transmission is also envisaged, See Article 20 2. *In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible*). This right is a new right, created by the GDPR. The result is that the provider « B » will have access the data of its predecessor « A » and will have the right – if not the obligation – to process these data in the context of its own contract with the data subject.

This goes against one of the founding principles of the GDPR: data minimization. In a nutshell: « the less you know about me, the better it is ». The following rights are consistent with this idea:

– Right to erasure (Article 17) ;

– Right to restriction of processing (Article 18) ;

– Right to object (Article 21).

All these rights have one thing in common: they all tend to reduce the amount of data processed about the data subject.

The data minimization principle is explicitly mentioned in the GDPR (Recital 156 « *Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimization*«). It is closely related to the proportionality principle (« *Article 5 – Principles relating to processing of personal data – 1. Personal data shall be (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*«).

But the data portability right follows another logic, namely **data maximization**. Service provider « B » will be in a position to process data collected from two distinct sources: « B » and « A ». Without portability, « B » will have to start from scratch, which is preferable from a Data Privacy standpoint. Furthermore, the data portability right has been interpreted by WP29 as having a rather extended scope. WP29 considers that « *the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject, for example, on an online form*« .

The provision of data extends to metadata: « *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* » (FAQ, Question 10 – How must the portable data be provided?).

Surely the data subject's privacy would be better protected in a situation where the two databases would remain separated and segregated, under the authority of two distinct data controllers. Data protection rules basically set up barriers and create restrictions to the processing and sharing of data. But the GDPR in its Article 20 encourages the data subject to gather all data & metadata concerning him or her in one single database. After a certain period of time, situations will arise where a third data controller (« C ») will be processing data originally processed by « A » and « B ». The resulting personal (Big) data set will allow the data controllers (« B » and any subsequent data controller) to improve their evaluation of the data subject's personal aspects (profiling). This is not what the GDPR is made for...

One stupid question: the processing of the data transmitted from « A » to « B » by « B » is certainly legitimate because it results from a request made by the concerned data subject, but is it necessary for the performance of the contract entered into between « B » and the data subject? Probably not. Business models usually do not rely on using competitors' data! These data will not be necessary for the receiving data controller to fulfill its obligations under the contract.

I may be wrong but it seems to me that the right to portability is not consistent with the piece of legislation in which it is included. The data subject exercising this right will not play the role he/she is expected to play. This is also true for the data controller.

Not to mention several issues linked to intellectual property, this new right will likely have an **impact on various data protection compliance processes**, on the side of the data controller receiving the data, including:

- Privacy Impact Assessment – Article 35 (« Data protection impact assessment »)

Data controllers will have to anticipate two categories of data subjects: data subjects whose data include data transmitted by another data controller as a result of a data portability request, and data subjects without such data. This will mean two distinct scenarios, from a risk assessment perspective. The impact on privacy of any given processing will differ, based on whether data coming from the past (before agreement was signed) are present or not. The risk (severity) will be higher in cases where the processing includes/may include « portable data ».

By being forced to process data that is not necessary, the data controller will have to take an additional and unnecessary level of risk into account.

- Transfer to a third country – Chapter V (« Transfers of personal data to third countries or international organisations »)

What will happen in case the new data controller (« B ») is located in a third country outside the EU (Senegal, India, South Korea, USA, Morocco, China...), without an adequate level of protection? Will the two data controllers have to consider signing model clauses (Article 46 2 (d)) before transferring the data? One question before: who will be considered as « Exporter »? The data subject? Or the data controller to whom the request is directed?

- Documentation – Article 30 (« Records of processing activities »)

Where applicable, the data portability scenario will have to be mentioned in the documentation, by way of an additional category of recipients (the documentation of « A », and also the documentation maintained by its processors, in accordance with Article 30 2). Or should we consider such data transmission as a specific processing activity, to be identified as such in the documentation required by Article 30?

These issues are not addressed by the Guidelines on the right to portability adopted on 13 December 2016.

The idea of putting the natural person in control of his/her data is absolutely fine. But this control should not interfere with the control exercised by another stakeholder called the data « controller » on the whole process.

Having this distinction between data and process (« données » et « traitement » en français) in mind, the three above-mentioned issues could be addressed as follows:

- Privacy Impact Assessment

The risk resulting from the aggregation of data is taken by the data subject. The data controller should be allowed not to take the risk created by the data subject into account when preparing its PIA. The consequences (potential consequences) of a decision made by an individual must be accepted by that individual. The risks to be documented in a PIA are the risks created by the data controller's future products or services, neither more nor less.

As rightly mentioned in Article 35, the required assessment is « *the assessment of the impact of the envisaged processing operations on the protection of personal data*« , with « envisaged » meaning « envisaged *by the data controller*« . The impact of a transmission of data requested by a data subject on the overall protection of the data concerning him/her must certainly be assessed, but it must be assessed by that data subject when taking his/her decision, not by the data controller.

- Transfer to a third country

In such case, an explicit and specific consent should be given by the data subject. This consent will form the legal basis for the transfer between the two data controllers. The data will be transferred from the EU to a country outside the EU based on data subject's consent (Article 49 – Derogations for specific situations – 1.

In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards).

The data subject's consent will be given to the data controller transferring the data (« A »), irrespective of the legal basis adopted by the data controller receiving the data (« B »).

- Documentation

The data portability scenario should not be considered as a processing activity and should be mentioned in the description of the process in which the data will be included. « Processing activities » as mentioned in Article 30 are processing activities carried out by the data controller, under its responsibility, and should be documented under a data controller perspective, regardless of the initiatives which may be taken from time to time by some data subjects.

Conclusion...

The data controller is not just responsible for legal compliance, the data controller is also accountable, under the GDPR. The assumption here is that the data controller remains the decision maker (*) when it comes to the processing activities carried out under its responsibility. Like always, a company's scope of responsibility must not exceed its scope of control, and vice-versa it should have full control over its scope of responsibility.

This idea is somehow already present in the Guidelines released by WP29 (page 5: Controllership – *Data controllers answering data portability requests, under the conditions set forth in Article 20, are not responsible for the processing handled by the data subject or by another company receiving personal data*), but not sufficiently applied, in the guidelines. It should be reflected in the way the three compliance processes mentioned above should be followed by data controllers when confronted to data transferred to them as a result of a data portability request.