ENSHRINING A RIGHT TO NON-PERSONAL DATA PORTABILITY

SUMMARY

After the introduction of a data portability right with the general Data Protection Regulation (RGPD), the European Commission announced its intention to launch a legislative initiative in autumn 2017 to create a right to non-personal data portability, in the context of its digital single market strategy.

The introduction of this right must be supported. It can in fact be considered as part of the larger framework of implementing new tools to trigger innovation and value creation in the digital economy, which mostly occurs when data is contextualized and combined with data from other data sets. In the context of a platform economy, the non-personal data portability indeed becomes a crucial tool for economic development and innovation in Europe. **The right would indeed open up the possibility for companies to recover data they have generated and stocked by a service provider and transfer it to another one.** This would address the problem of the persistence of market imbalances at the detriment of European actors - small and medium enterprises in particular. It hence would facilitate a "cross-platform" and not only a "cross-border" data flow. **The establishment of the right to non-personal data portability would allow to efficiently fight against lock-in effects and to encourage the development of an innovation-friendly environment while restoring companies' control over their data.** At this stage, both contractual means and competition law seem to be insufficient for this purpose.

In order to be efficient, the introduction of the right to non-personal data portability must be supported by a deep study on interoperability standards and technical strategies to access data, in particular via Application Programming Interfaces (API). The outline of the right is yet to be settled. The following points remain notably open:

- **The right's holder**: in order for the right to serve its purposes - that of spreading innovation in particular - the right's holder must be clearly defined. The notion of "data generating co-contractor" should be further elaborated.
- **The juridical basis of the right of data portability**: it seems advisable to avoid building the portability right onto the concept of property right recognized to a right's holder. A property right of non-personal data would go against the initial objectives of the principle, as it would make transactions and sharing mechanisms even more complex.
- **The concerned data**: the spectrum of data affected by the right to non-personal data portability is forcibly at the center of the discussion and must be clearly defined. It might be useful to take inspiration form the Bill for a Digital Republic. The alignment with the other types of portability rights must be included into the discussion.
- **Conditions for technical implementation:** they determine the real reach of the right. The definition of a common set of interoperability standards and formats of technical access tools must be precise, so as to fulfill the requirements of the right to data portability.
- **The territorial scope of application:** to enable the right to be more effective, when european law is applicable to contractual obligations, the right to non-personal data portability should have an extraterritorial application.

By autumn 2017, the European Commission has announced a legislative proposal to introduce the principle of porting non-personal data in the Digital Single Market. The aim of this initiative, alongside with the proposal to abolish data localisation obligations, is to foster the development of a European Data Economy.

The introduction of a right to non-personal data portability would follow a right to personal data portability, provided for by article 20 of the General Data Protection Regulation (GDPR) and applicable from 25 May 2018.

A RIGHT TO NON-PERSONAL DATA PORTABILITY MUST BE INTRODUCED AT THE EUROPEAN LEVEL

In accordance with its previous opinion, the Council wishes to recall that the value created by data use mostly derives from the cross-referencing of datasets. The issue that arises is therefore not so much that of the protection of investment for the constitution of large databases, it is rather that of the incentives to cross-referencing of datasets between various actors. In many instances, data collection and categorization is done as a by-product activity of an industrial process: data is a mean, not an end in itself. On the other hand, the cross-referencing of datasets serves a new purpose. It is this essential phase, which covers the true potential of Big Data and the emergence of new services that should be promoted by new incentives according to the Council.

Fight bolting systems and support the European digital economy

In a digital economy increasingly marked by platform domination and closed systems, a right to non-personal data portability will facilitate a "cross-platform" rather than a "cross-border" data flow only. It follows two main objectives : to encourqge competition between digital services and to give companies control back over their data.

- **Encourage competition between digital services**

This right will enable a company to recover data which has been generated and which is stored and processed by a service provider. It will then be allowed to transfer the recovered data to another service provider, or to use it internally or as part of commercial and industrial partnerships for instance. This right will concern non-personal data, i.e. non-identifying data and, as such, mainly economic and financial, agricultural or industrial data[1]. By facilitating the switching of service providers, the right to data portability is intended to promote competition between cloud services.

- **Giving companies control over their data**

Beyond the first objective of at facilitating switching of services providers like cloud computing, the right to non-personal data portability will also give companies control over their data. Indeed, the right to non-personal data portability will allow companies to retain control over their data in the context of a platform economy, where value is tendentially created and captured by external actors offering services based on their users' data. Such a right will then make it possible to tackle lock-in effects and value leakages by making it possible to develop in-house services or at the level of a professional sector.

The portability of industrial data - an example

Many industrial SMEs have begun a transition of their business and production models, notably in the context of the "Industry of the Future" initiative in France. Several companies have already connected machines producing data via sensors. Generally, such data is captured and stored by a service provider (i.e. a machine manufacturer or a cloud provider). However, it is among its service providers, through data analysis, that more and more services are produced, potentially leading to a leakage of value and dependence.

A right to portability should enable these SMEs to easily retrieve their data and transfer it to another provider without interrupting their service. It will also allow them to use data internally or with other players in their sector to develop innovative new services.

Moreover, it seems that data portability would favour the cross-fertilization of data from third-party services and thus the emergence of new business models, such as *Personal Information Management Services* (PIMS) for personal data. The value is now in cross-referencing of datasets between various actors. For instance, smart building is a relevant example where a lot of data can be crossed : temperature data could be crossed with data about the persons' circulation and data relative to the maintenance of the local for example.

By fighting against data silos, the right to non-personal data portability is intended to support the development of a European data industry, for the benefit of the most innovative players - able to challenge the dominant positions acquired by others.

The legal basis of the right to data portability

In the French Bill for a Digital Republic, the legal basis of the right to data portability is both the control over data by the individual and the support of competition. In this regard, data portability is a proactive mechanism as it takes note of the new importance of cloud computing services. In this regard, data portability originates in the same legal basis as the Council Directive 91/250 / EEC of 14 May 1991 on the legal protection of computer programs, which allows the decompilation of software while derogating from the protection of computer program.

Finally, data portability is generally associated with low switching costs and thus the weakening of barriers to entry the market. Thus, the legal basis of the right to portability is competition. Personal data portability enshrined in the GPPR is based on the principle of informational self-determination and ultimately on human dignity. Similarly, the right to non-personal data portability is based on another fundamental freedom: the freedom to conduct a business and in particular free competition.

Critics to the introduction of such right must be overcome

The idea of enshrining a right to portability is subject to several critics that must be overcome.

- **The contractual approach would be sufficient**

Critics claim that cases where companies could lose control over their data when it is stored by a service provider are very limited. In general, the contractual approach would hence be sufficient to provide with the possibility of recovering data. Moreover, if contractual law fails to achieve this objective, competition law would have the appropriate mechanisms to respond to abusive data lock-in situations.

However, if for a large company the use of contractual law is an appropriate instrument and allows for the pre-contractual negotiation to assert its rights, **the situation is different for smaller companies, which can be subject to unbalanced contractual terms**. Some actors have in fact proved the existence of unclear and unbalanced reversibility clauses in cloud computing contracts[2]. They have also noticed that the portability of their data was subject to changing contractual terms. In this regard, the risk of non-reversibility or "lock-out" is considered significant, particularly insofar as it is difficult to assess the service provider's ability to return the data in a usable format. These standard contractual terms make it difficult to retrieve data[3]. In addition, procedures can be costly and time-consuming. The consecration of a right to non-personal data portability could be in favour of more balanced contractual terms.

- **The problem would not be of juridical origin**

It has been pointed out that it is already possible for a company to recover non-personal data it has supplied to a service provider. Nevertheless, few companies venture there, especially when they use a provider that allows a significant personalization of the service, a CRM service[4] for example. Indeed, retrieving and carrying data is long, complicated and expensive. Thus, the introduction of a new right would not solve the problem and would be ineffective.

This is particularly true as sectors-specific standards encoding access and portability rules are few and have not yet succeeded in guaranteeing an effective flow of data. **This is why the right to non-personal data portability must be accompanied by a thorough reflection on interoperability standards by granting access to data via an Application Programming Interface (API).**

- **Tools enabling portability would be too expensive**

Implementation requirements for data portability can be technically complex and costly mainly for reasons of basic architecture. From a strictly technical point of view, operators will have to develop a functionality to query their databases and extract relevant information.

The cost seems to be extremely low for small companies: many tools are at their disposal to allow them to export data easily. Moreover, a threshold logic could be introduced in order to safeguard the smallest companies on the model of Article 48 of the French Bill for a Digital Republic.

For larger companies, the cost mainly relies on the architecture of the database or on organizational complexities. The cost is not necessarily prohibitive (it is not a matter of building a new database, but of developing extraction tools). It should not be an excessive burden as many companies will already have set up the portability of personal data under the GDPR. In addition, companies are already exporting their data for different purposes (including backups). The emergence of format standards for the export of data may also be able to reduce the cost of data portability.

THE OUTLINE OF THE RIGHT TO NON-PERSONAL DATA PORTABILITY MUST STILL BE DEFINED

Although the objectives and foundations of this right seem to be conducive to the development of an innovative European data economy and of an open and competitive environment, it is nevertheless still necessary to clarify certain aspects.

The right's holder

The right's holder should be the firm contracting with a service provider in order to implement a device generating data. In other words, the right's holder of non-personal data portability is the one who contracts with a digital service provider, who could then extract the data to contract with a new operator or exploit data in the framework of industrial or commercial partnerships.

The right's holder - an exemple

In the case of data produced by a sensor in a smart building, the holder of the right to portability would be the one who generates data and neither the installer of the device nor the manufacturer.

Right to portability vs. property right

The right to portability of non-personal data must be clearly distinguished from a property right over the data. By no mean it seems necessary to link these two rights. On the contrary it is quite possible to recognize a right to portability on the basis of freedom to conduct a business, which is not connected to a property right. The creation of a property right over the data would be contrary to the sought objectives. By freezing right holders and making transactions more complex, it would limit the exchange of data and its circulation. Moreover, it would ultimately lead to a greater risk of dispossession of the players due to the possible inclusion of mandatory transfer clauses in the contracts.

The data concerned

The right of data portability should apply to all non-personal data generated by the right's holder. Companies should have the right to receive all non-personal data concerning them, meaning the data they provided in the context of a contractual relationship. Similar to the provisions foreseen by the GDPR, these data could include actively and consciously reported data by the company, such as data provided to create an online account. Data generated by the company's activity when using a connected service or device should also be concerned (raw data collected by communicating meters, for instance).

On the model of the existing legislation on portability, the new right could include limitations for certain type of data. For instance, Article 48 of the Bill for a Digital Republic excludes from the scope of portability significantly enriched data and data prejudicing the provisions protecting secrecy in commercial, industrial and intellectual property matters. More generally, the exercise of the right to non-personal data portability should not adversely affect the rights and freedoms of others. Last but not least, metadata should also be provided as as they are often essential to contextualize the data.

The relationship to other forms of data portability

Conflicts between the different rights to data portability enshrined or contemplated by different French and European legislations[5] may occur. Given the difficult distinction between personal data and non-personal data, it is not excluded that certain situations will relate to both the portability of personal data and the portability of non-personal data. For example, a data portability conflict could occur in heterogeneous databases (i.e., databases that include both personal and non-personal data). It is therefore a question of thinking in advance about possible ways to solve these potential conflicts. **As such, difficulties in defining the boundaries between personal data and non-personal data could justify aligning the regimes of these rights with portability.**

Harmonize the portability of data with existing legislation

The Council encourages the Commission to adopt similar approaches on data portability as those that that already exist as an impact assessment for any treatment aimed at the free flow of data, or security and protection of data through the tools set by privacy by design and privacy by default (such as encryption). Harmonization of rights to data portability would also prevent economic actors from having to set up separate architectures to organize data restitution. Furthermore, the exercise of the right to data portability should be proposed through free functionality or at least through the cost of implementation. Similarly, for reasons of legal security, the failure or non-compliance to the non-personal data portability should be subject to the same sanctions as those established by the GDPR.

Data portability tools

Standardization of technical access modalities is essential. Data should be returned in a structured, commonly used and machine-readable format. In addition, it is necessary to define clear technical standards for interoperability (but not full system compatibility).
As recommended by the guidelines of the Article 29 Data Protection Working Party on data portability, industry stakeholders and trade associations should work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability[6]. The use of Application Programming Interfaces (APIs) to transfer data directly from one operator to another and to automatically query large databases should be encouraged, as the creation of data ontologies for instance.

The territorial scope of the right to non-personal data portability

Inspiration: API and data portability according to the French Digital Republic Bill

On the example of Article 48 of the French Bill for a Digital Republic, the Council considers that suppliers may be required to take all necessary measures to enable the recovery of data and files. It could imply establishing an API and transmitting all information necessary for the change of supplier.

To guarantee the effectiveness of the right to portability of non-personal data, it would be necessary to define its territorial scope. When the European law is applicable to contractual obligations, the Council considers that this right should have an extraterritorial scope. The portability of non-personal data should apply to the processing of non personal data regardless of whether the processing takes place in the Union or not.

[1] Mid-Term review of the Digital Single Market (DSM) – a good moment to take stock : https://ec.europa.eu/digital-single-market/en/content/mid-term-review-digital-single-market-dsm-good-moment-take-stock) : Examples of non-personal data include tax records such as invoices, accounting documents or documents supporting company registration. Other examples include data on precision farming (helping to monitor and optimise the use of pesticides, nutrients and water) or from sensors communicating the data it records such as temperature or wind conditions in, for instance, wind turbines, or data on maintenance needs for industrial robots for example when they are out of paint.

[2] COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy - Accompanying the document Communication Building a European data economy {COM(2017) : 9 final} : https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy, page 47 "Anecdotal evidence suggest that clauses on data portability are often left out of contracts, and that smaller business actors can experience difficulties in getting their data back e.g. upon termination of the contract." Comments made by participants at the EC workshop on Building the European Data Economy on 21 September 2016; findings published at: http://ec.europa.eu/newsroomitem-detail.cfm?item_id=34617/just/ and on the public consultation : https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-building-european-data-economy

[3] Autorité de contrôle prudentiel, The risks associated with cloud computing : https://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/analyses-syntheses/201307-The-risks-associated-with-cloud-computing.pdf

[4] Customer relationship management.

[5] The right to data portability :
- for data subject a right to receive the personal data concerning him or her, which he or she has provided to a controller, a right introduced by Article 20 of the General Data Protection Regulation,
- for the consumer of all the data associated with the consumer's user account of an online public communication service and applicable only to the most important service providers - enshrined in Article 48 of the Bill for a Digital Republic.

The right to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content in Articles 13 and 16 of the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content

[6] ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on the right to data portability ; https://www.cnil.fr/sites/default/files/atoms/files/ld_portabilite_eng.pdf