ADVOCATEN
AVOCATS
ATTORNEYS

Jos Dumortier°
Geert Somers°
Edwin Jacobs°
Hans Graux°
Frederic Debusseré

Stefan Van Camp

Magali Feys
Eleni Kosta°°
Davide Maria Parrilli
Ruben Roex
Bernd Fiten
Pieter Gryffroy

° BVBA/SPRL
°° Bar of Heraklion

Legal memo with respect to the Article 29 Guidelines on the right to data portability

Executive summary

On 13 December 2016, the Article 29 Working Party published a set of Guidelines interpreting the notion of the right to data portability, as introduced by Article 20 of the General Data Protection Regulation (GDPR). While the Guidelines provide many useful additions and clarifications, they also contain some suggestions that are particularly problematic for the European telecommunications industry:

- The scope of the data portability right is expanded significantly. Specifically, the GDPR restricts the right to personal data "provided by" the data subject, while the Guidelines support an expansion of the concept to include "the personal data that are generated by and collected from the activities of users". This expansion is not in line with the text, spirit or the intentions of the legislator, and creates new privacy risks for data subjects by increasing the dissemination of personal data to recipients that may have no use for it.

- The interests of third parties whose personal data may also be revealed by a data portability request in a telecommunications context are insufficiently protected by the Guidelines. While suggestions are provided on how this challenge could be handled, these do not seem realistically feasible or effective in plausible data portability scenarios for the telecommunications industry.

- The Guidelines do not clarify how data portability requests should be dealt with when there is no interoperable data format available in a given industry or context. While cooperation between industry stakeholders and trade associations is encouraged (both by the GDPR and by the Guidelines), this does not ensure that a compliant option is available.

- Finally, the Guidelines do not consider the specific context of the European telecommunications industry. Specifically, they do not take into account the fact that this industry is already subject to portability rights and change obligation that achieve the goal of avoiding lock-in and increasing competition; nor do they consider the impact of the upcoming changes in European e-Privacy legislation that create a specific framework for data protection in the telecommunications context.

Context

The General Data Protection Regulation (EU) 2016/679 (hereafter the GDPR), which will become applicable across the EU on 25 May 2018, has formally introduced the concept of data portability into European data protection law. Briefly summarised, Article 20 of the GDPR 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".

The right is conditional and constrained by several requirements: it only applies where the processing is based on consent or on a contract; and only when the processing is carried out by automated means. Furthermore, the GDPR recognises that the transfer component of the data portability right – the right to demand that a controller transfers personal data directly to another controller – can only apply "where technically feasible". The right to data portability is without prejudice to the data subject's separate right to erasure, and the exercise of the data portability right may not adversely affect the rights and freedoms of others.

While the principles of this concept are thus relatively well defined, there is significant margin for interpretation on its scope and application in practice. To assist in this exercise, the Article 29 Working Party published a set of Guidelines on 13 December 2016[1], which provide a shared perspective of the European data protection authorities' on the right to data portability.

Upon analysis, some of the interpretation choices of the Guidelines seem subject to debate and may have negative repercussions on competition and innovation in the European market, specifically from the perspective of the European telecommunications industry, at whose request this memo was drafted[2]. Moreover, the Guidelines as written may not consider the potential negative impact of the current choices made on the privacy and security of European users of telecommunications services.

Therefore, the purpose of this note is to present a set of concerns for further consideration by the European data protection authorities, in order to contribute to a homogeneous and effective interpretation of the right to data portability, and to the effective protection of personal data.

---

[1] Article 29 Working Party Guidelines on the right to data portability (WP 242), adopted on 13 December 2016; see http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

[2] Specifically, at the request of the European Telecommunications Network Operators' Association ETNO.

In the sections below, four topics will be commented briefly:

- The scoping of the **concept of data provided by the data subject**;
- The consideration of **privacy and security interests of other data subjects**;
- The expectation of **interoperability**;
- And finally, the **unique context of the telecommunications sector** as a specifically regulated industry in the EU.

On each of these points, we hope to illustrate that the Guidelines may benefit from further scrutiny, and will attempt to provide useful suggestions that can contribute to the effectiveness and added value of the right to data portability in the future.

The scope of data portability in the GDPR

The scoping of the data portability right is addressed in a relatively explicit manner by the GDPR: it allows the data subject "to receive the personal data concerning him or her, which he or she has provided to a controller". As the Guidelines stress, the central purpose of this right is to empower the data subject, to support the free flow of personal data in the EU and to foster competition between controllers by facilitating the switching between service providers.

The examples of use cases where such a right is necessary to achieve these objectives are clear and manifold: data subjects may provide their data to a social network, to a cloud storage provider, to an e-mail service provider, and so forth. In each of these cases, there is a credible threat that the service provider effectively captures this information by refusing to make it available to the data subject, thus creating a lock-in effect and (more importantly from a data protection perspective) allowing data controllers to give data subjects a very unappealing choice: they can either continue to allow the current data controller to process their personal data – even if they would prefer to switch – or exercise a data erasure right and thereby lose their data. The new data portability adds a third option: the data subject can take his or her data back and/or place it elsewhere. This offers a solution to a real problem.

The spirit of the GDPR's text and its underlying idea can only be understood as relating to such data which the data subject has entrusted to the service operator for the duration of the service and for the purpose of receiving the service. In other words, it applies to cases where the service provider acts as a "trustee" for the data which has been given in stewardship to the provider by the customer, and which therefore must be given back to the customer (or handed over to a new provider) upon request. This approach is also echoed by recital (68), which emphasizes the goal of this right "To further strengthen the control over **his or her own data**,...").

However, the Guidelines expand this notion in a way that seems contrary both to the text of the GDPR and to the aforementioned context. 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 context described above. The Guidelines however argue in favour of an expansion of the concept to include "the personal data that are generated by and collected from the activities of users", which the Guidelines argue are metaphorically "provided" by the data subject by virtue of the use of the service or the device. Several examples of raw sensor data (smart meter use, search history, traffic data[3] and location data, heartbeat rates etc.) are provided by the Guidelines.

While the Guidelines explicitly exclude any inferred data and derived data – which are generated by the data controller in relation to the data subject, rather than being directly observed by the controller – the Guidelines none the less have opted to expand the law in a manner that seems contrary to the letter and spirit of the GDPR. In effect, the Guidelines rewrite the GDPR to state that the data portability right covers not only data provided by the data subject (as the law requires) but also data observed or measured by the data controller in relation to the data subject.

This expansion seems to have no basis in law. Indeed, other data subject rights that have a broader scope emphatically use the wording "personal data concerning him or her" (Article 15, on the right to access, Article 16, on the right to rectification, and Article 17, on the right to erasure). The addition of the restriction to data "provided to a controller" in the data portability right as written by the legislator therefore does not seem accidental, and a re-definition of this right does not seem appropriate.

Indeed, there is a clear indication that this limited scoping was intentional. The 2012 Proposal for a GDPR from the Commission[4] made a distinction between the data subject's right to obtain his or her personal data back – Article 18.1, without a limitation to data provided by the data subject – and the right to have it transferred from one controller to another – Article 18.2, including the limitation to data provided by the data subject. Thus, the final drafting of the GDPR entailed a reconsideration of the original text by the legislator, who made a

[3] The inclusion of traffic data in the Guidelines as an example of where an expanded data portability right can be applied may prove problematic for additional reasons. Firstly, most if this data relates to purely technical routing and timing data, which will not have any value or use, neither to the customer requesting it, nor to any receiving competing service provider. Traffic data which is potentially useful to a customer - such browsing history or call history – is already available to the customer via logs and invoices. Furthermore, this is also an example where a misalignment of this opinion towards the telecommunications industry is apparent, since the newly proposed e-Privacy Regulation – as discussed further below – abolishes this concept from telecommunications law in favour of the broader notion of 'metadata'. If any metadata relating to a data subject would fall under the expanded data portability right, this would greatly exacerbate the aforementioned problems of scoping and utility of the data portability right.

[4] Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

conscious decision to re-draft it by making the limitation to data provided by the data subject all-encompassing for the portability right.

An expansion of the scoping of the law thus amounts to gold plating of the legislation, which is a task that appears to exceed the interpretative role that the GDPR accords to the European Data Protection Board. Even overlooking the formal issue that the Working Party is provisionally assuming the tasks of the EDPB via the Guidelines, the role of the EDPB would be to "examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation" (Article 70, e of the GDPR). An expansion of the text of the law is not in line with this interpretative task.

Beyond the legal objection, this expansion of the scope of the portability right is not in line with the objective of the right as described above. Observed data in relation to a data subject does not create similar lock-in risks that limit competition in the internal market and threaten the data subject's right to data protection. To the contrary: while data subjects will provide more or less the same personal data to similar service providers – and should therefore also reasonably be able to port that data to competing providers as the GDPR requires – it is the service providers themselves who make implementation choices as to the scope of observed data. This observed data is not likely to be similar or comparable from one provider to the next.

The observed data provided to competitors is potentially of no use to the recipients since their own implementation choices may be different. More importantly, revealing observed data to a different service provider exposes data subjects to a real privacy threat 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. Since the examples shown by the Guidelines indicate cases where privacy sensitive data can be revealed – such as health data – an approach that relies on sharing first and verification afterwards does not seem like an advisable position. The downloading of indigestible amount of raw data (like all Call Data Records related to how many times a mobile phone has been connected to a mobile antenna) does not contribute to the creation of a safe and secure data sharing environment for customers. Thus, the expansion of the scope of the data portability right is not in line with the text of the GDPR, nor in line with its spirit and the intentions of the legislator, and creates new privacy risks for data subjects. An interpretation that is limited to the text of the GDPR – which unambiguously refers to data provided by the data subject, with no indication that the word "provided" may be taken as a metaphor – eliminates these privacy risks for data subjects, and therefore seems preferable.

The consideration of privacy and security interests of other data subjects

The text of the GDPR in Article 20.4 rightly states that the data portability right "shall not adversely affect the rights and freedoms of others". The legislator rightly recognised that a request to exercise this right could have negative repercussions on third parties, notably other data subjects whose personal data may also be revealed. The telecommunications industry is particularly vulnerable to this problem: since communications happen from one data subject to at least another data subject, data portability requests that would fall within the scope of Article 20 of the GDPR (e.g. a request to port the content of a mailbox, to the extent this is being retained by the telecommunications provider) would affect not only the personal data rights of one data subject, but of all participants in the communication.

An approach is therefore required that allows (and indeed, requires) data controllers to assess the impact of data portability requests in order to avoid revealing potentially sensitive personal data from a data subject that did not consent to this to a third party (e.g. enterprise customers or family services). This is required to protect the privacy and security of all participants in a communication. To give an example: if a user of an e-mail system wants to move his/her conversations to a new e-mail provider and choses an unreliable new recipient, then he/she is not only risking the privacy and confidentiality of her own telecommunications secrecy (which many would likely argue is well within their rights), but also the telecommunications secrecy of all participants in the conversations. One need only consider the difference between a service provider in the EU that fully respects the GDPR and a service provider outside the EU that may be ignorant of any such rules or which may be vulnerable to data claims from a national security body that does not align to EU fundamental rights to see the risk.

The Guidelines consider this issue, but only by noting that processing "by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs", and that the sending and receiving controllers are encouraged to implement technical filters that "enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data". It also suggests that controllers should "implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent".

In our view, these guidelines are not aligned with likely data portability scenarios. A data controller that chooses to follow them will still need to rely on the will of the data subject to select receiving data controllers and to use any provided filters; given that these users will have already decided to switch providers at that stage, they are unlikely to take a restrictive position on personal data to be ported. Furthermore, the suggestion of gathering the consent of other data subjects does not seem realistic, especially in telecommunications scenarios where a communications service provider might need to collect consents from potentially hundreds or thousands of individuals, for some of whom it may not even have contact information (like in the aforementioned cases of corporate communications or family

packages). Furthermore, even a single refused consent will impact many conversations and many other data subjects. The Guidelines provide no clarification on these points.

The approach presented by the Guidelines therefore does not seem realistically feasible, at least not for all industries or use cases. It may be preferable instead to require controllers to assess which personal data they can make available without impacting the data protection rights of other data subjects, and to implement data portability services accordingly, i.e. by excluding by default any personal data that also relates to persons other than the requesting data subject. While this of course reduces the scope of the data portability right, this seems like a more effective way to ensure that one data subject's rights are not harmed by the (potentially poor) choices made by another.

The expectation of interoperability

The text of the GDPR is somewhat ambiguous in relation to the data formats to be used to respond to data portability requests. As a principle, data must be provided "in a structured, commonly used and machine-readable format", while the GDPR also recognises that personal data transfers directly from one controller to another are only required "where technically feasible". Finally, recital (68) underlines that "The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible."

While the data transfer right thus does not require controllers to modify their systems to ensure compatibility with competitors' systems, the GDPR does not clarify to what extent (if at all) interoperability of personal data is required or expected. The text of the GDPR refers only to a "structured, commonly used and machine-readable format", but provides no indication of what should happen when no such format is in common use. Is there an obligation in such cases that industry aligns around a common format?

The Guidelines address this point by arguing that "structured, commonly used and machine readable are specifications for the means, whereas interoperability is the desired outcome". This seems like a reasonable assessment, considering that Article 20 does not refer to interoperability in relation to data portability, but recital (68) of the GDPR does. The Guidelines also provide guidance on selection criteria for a data format, recognising that these may differ depending on the industry or use case, but that preference should be given to formats that are interpretable, free from costly licensing requirements, and at a sufficiently high level of abstraction to permit processing by the recipient, including the relevant metadata.

The Guidelines however do not provide any clarification on the question what the data portability right entails when there simply is no appropriate interoperable data format in use in a given industry. The Guidelines – like the recital (68) – encourage cooperation between

industry stakeholders and trade associations to establish interoperable standards and formats, but this does not ensure that a compliant interoperable option is available to data controllers.

In our view, given the absence of any obligation on this point in the GDPR – and considering indeed that the recitals explicitly encourage but not mandate the development of interoperable standards - the only correct interpretation of the GDPR seems to be that data controllers must use such interoperable formats when they are reasonably available for the personal data in question, but that they have no obligation to commit to any specific development to create such as standard when none is available in order to comply with any data portability requests. In such cases, data portability requests can be satisfied through any digital format which is available to the controller. This point should be recognised in the Guidelines in order to provide more clarity on what needs to be done if no interoperable data formats exist.

The unique context of the telecommunications sector

The telecommunications industry occupies a very specific space in European data protection law, since it is presently also subject to a separate ePrivacy Directive 2002/58/EC (complementing and specifying the Data Protection Directive 95/46/EC), and will likely be subject in the future to a separate recently proposed ePrivacy Regulation[5].

However, the telecommunications industry is not exempt from the scope of the GDPR. Article 95 of the GDPR admittedly notes that the Regulation does not impose additional obligations in connection with the provision of publicly available electronic communications services in public communication networks in relation to matters for which they are subject to specific obligations with the same objective set out in the e-Privacy Directive; but data portability as such is not specifically addressed by the e-Privacy Directive. Therefore, the telecommunications industry is presently not specifically exempted from the data portability obligation of the GDPR.

However, the Guidelines correctly underline that "other types of portability already exist or are being discussed in other areas of legislation (e.g. in the contexts of contract termination, communication services roaming and trans-border access to services)." Even outside the context of services roaming, Article 30 of the Universal Service Directive 2002/22/EC (as modified in 2009) imposes a number portability regime, and more generally facilitates any change of provider. It does so by requiring operators to move a phone number from one

[5] Proposal of 10 January 2017 for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, see http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

operator to the next within the shortest possible time, and at any rate within a working day with no more than one working day's loss of service during the process.

Thus, the telecommunications industry is already subject to a portability and change obligation that achieves the goal of avoiding lock-in and increasing competition. At the national level, other portability rights can apply (such as e-mail hosting portability, internet services switching facilities, or portability of website hosting services).

While the data protection oriented data portability right of the GDPR has a different scoping and orientation, one should be careful not to impose cumulative, redundant and potentially contradictory portability obligations on the telecoms industry. This is also precisely why Article 20 of the GDPR should not be extended beyond its legal wording and why its scope should be limited to data that the data subject has provided to a controller. Any other interpretation would add a disproportionate obligation on telecommunications operators to transfer data to a new provider, without therefore further fostering the switching between operators, as this is to a large extent already dealt with by the provisions of existing telecommunications regulations.

Moreover, it would certainly be counterproductive if it would be possible to exercise a data portability right under the GDPR while leaving the original service contract (under which personal data is provided to the controller) intact, since this would make the transfer ineffective as soon as the telecommunications service is once again used.

***

Hans Graux 31 January 2017

Partner – Manager time.lex