24.

MEMO

To : Article 29 Working Party
From : Ecommerce Europe
Date : 14 February 2017
Subject : Ecommerce Europe's feedback on Guidance Article 29 WP on Data Portability

Ecommerce Europe welcomes the opportunity for public comment on the Article 29 Working Party's draft guidelines on the implementation of the General Data Protection Regulation (GDPR). Ecommerce Europe, which is a member of the ICDP[1] as well, also in the paper sent by the Coalition in February 2017 acknowledges that there is a greater debate about data portability underway in the European Union and its member states, as well as globally. A right to retrieval of data/digital content, including non-personal data, is currently under discussion in the context of the Directive for certain contract rules for the supply of digital content (Digital Content Directive). In addition, the communication for the "building of the European data economy" also provides for discussion on a right to portability, including for non-personal data. Ecommerce Europe that the data portability right in the GDPR should not be interpreted to accommodate political positions on portability expressed in the ongoing debate. Moreover, Ecommerce Europe considers that the discussions on broader and conflicting rights to data portability could risk undermining the coherence and solidity of the compromises reached in the GDPR. Ecommerce Europe is particularly concerned about the Article 29 WP's excessively broad interpretation of the right to data portability, far beyond the adopted text of the GDPR.

Goals of Article 20 GDPR

Throughout the guidelines, the Article 29 WP mentions several times that enhancing competition would be one of the goals of the right to data portability. For example, on page 4 of the guidelines on data portability, it is stated that: "Indeed, the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services (by making it easier for individuals to switch between different providers). It also enables the creation of new services in the context of the digital single market strategy."

As the right to data portability is not meant to enhance competition it is also not meant to foster innovation and the emergence of new business models based on data sharing, as mentioned in the guidelines on page 3: "This right aims to foster innovation in data uses and to promote new business models linked to more data sharing under the data subject's control"; page 4: "Data portability can promote the controlled sharing of personal data between organizations and thus enrich services and customer experiences. Data portability may facilitate user mediated transmission and reuse of personal data concerning them among the independent services they are interested in"; or page 5 where the right is "expected to foster opportunities for innovation".

According to recital 68 however, the only goal of data portability is "to further strengthen the control over his or her own data" by the data subject. So, it is clearly not a tool to enhance competition, to stimulate innovation or to enable new business models. In the same way, it isn't a tool to support user choice or consumer empowerment (page 3, 4 and 5). Therefore, in the view of Ecommerce Europe, the Article 29

[1] ICDP is comprised of 21 associations representing thousands of European and international companies who are building, delivering, and advancing the digital experience. The paper to which Ecommerce Europe refers is the "ICDP comments on the Article 29 Working Party's guidance on data portability", February 2016

WP excessive interpretation of the aims of the right to data portability should be revised and restricted to the goal explicitly outlined by the European legislator and not be broadened up to side effects of the right to data portability that in practice might appear, like innovation, new business models, support of user choice, consumer empowerment and enhanced competition, but were never explicitly expressed as a goal of data portability.

Automated data processing and paper files

According to Article 20 GDPR, the right to data portability is restricted to personal data processing carried out by automated means. The Article 29 WP indicates that the right of data portability therefore does not cover paper files. Although, in practice, most automated processing of personal data will be digital and not on paper and although most paper files are not processed without any human intervention, automated processing of personal data on paper, for instance with printed QR or bar codes, is technically possible without any human intervention and without digital filing of this personal data.

Ecommerce Europe wants to warn the it is difficult to foresee what future developments in data management models and privacy by design will bring on automated paper filing. As Ecommerce Europe does not favor unnecessary obstacles for future innovation, it suggests the Article 29 WP to revise its guidance on this point, so that it is perfectly clear that "processing of personal data carried out by automated means" covers all processing of personal data operating without human intervention.

Pseudonymous data

According to the Article 29 WP, pseudonymous data that can be clearly linked to a data subject (e.g. by providing the respective identifier) will (see page 7) fall in the scope of the portability request. In the view of Ecommerce Europe, it is unclear how to interpret this guideline. Does it state that all pseudonymous data can clearly be linked to a data subject by an identifier and thus all pseudonymous data fall under the scope of article 20 GDPR, which is in the view of Ecommerce Europe a wrong interpretation? Or does it mean, like it should, that only pseudonymous data that are clearly linked to a data subject because the identifier is also provided, fall under the scope of Article 20 GDPR and all other pseudonymous data do not? Because of this lack of clarity, Ecommerce Europe asks for a clear statement that only pseudonymous data that are clearly linked to a data subject, because the identifier is also provided, will fall under the scope of Article 20 GDPR and that all other pseudonymous data will not.

Personal data provided by the data subject and observed data

According to Article 20 GDPR, only personal data that the data subject has provided to a data controller are subject of the right to data portability, which, *a contrario* interpreted, also means that all personal data not supplied by the data subject is not portable.

In the opinion of the Article 29 WP provided by the data subject to the data controller not only covers data provided knowingly and actively by the data subject, but also personal data generated by his or her activity (page 3), the so called "observed data", which are data "provided" by the data subject by virtue of the use of the service or device (page 8).

As this extension finds no basis in the wording of recital 68 and Article 20 GDPR, Ecommerce Europe strongly opposes these extensions of the right to data portability to data obtained by the data controller by observing the behavior of the data subject in the use of the service or device (for instance, meta data), as they were never meant to fall in the scope of the right to data portability, that as such, is only limited to user generated content, which means actively and knowingly provided personal data by the data subject. Ecommerce Europe strongly advises the Article 29 WP to explicitly restrict the scope of

Article 20 GDPR to those personal data that are user generated, which means actively and knowingly provided by the data subject to the data controller. This also means that the examples given by the Article 29 WP of portable data falling within the scope of article 20 on page 4 (playlist from a streaming music service), page 5 (contact list from users' webmail application), page 6 (retrieve emails from a webmail service and request for transmission of details of bank transactions), page 7 (titles of books purchased or the songs listened to via a music streaming service), page 14 (email data and meta data) must be revised. Apart from the question of whether they are personal data, this data should not fall under the scope of Article 20 GDPR as they are not actively provided personal data and therefore should not be referred to as relevant examples of data subject to data portability.

Data related to third parties

In many circumstances, data controllers will process information that contains data of several data subjects. In the opinion of the Article 29 WP (pages 9 and 10), when this is the case, data controllers must not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". "Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests. However, when such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties."

Ecommerce Europe strongly opposes the position of the Article 29 WP on two points:

- Firstly, the fact that the right to data portability of the data subject in the vision of the Article 29 WP seems to prevail above the general and fundamental right of third parties involved to protection of their personal data and respect for their privacy. As Ecommerce Europe is convinced that the fundamental rights and freedoms of third parties, as laid down in the GDPR, prevail above the right to data portability, it favors an interpretation that enables data controllers to refuse to provide multiple people records to the requesting data subject when this would adversely affect the rights and freedoms of third parties.
- Secondly, the fact that, in the view of the Article 29 WP, it should be the receiving data controller that should control the received data and refrain from processing third party data for any purpose which would adversely affect the rights and freedoms of the third-parties involved. In Ecommerce Europe's interpretation of the GDPR, the transfer of personal data of third parties from the data controller to the requesting data subject, the storage of these personal data by the requesting data subject, as well as the transfer of these data from the requesting data subject to another data controller, as such is processing of personal data subject to the provisions of the GDPR. According to these rules, for each individual request for data portability, the transferring data controller has to assess whether the rights and freedoms of these third parties are adversely affected by the transfer, and if, he/she should refuse the transfer of this data to the requesting data subject. The same applies for the requesting data subject storing third party personal data or transferring them to another controller. The transferring data controller and the requesting data subject, in each case have to assess whether the protection of the rights and freedoms of third parties prohibits transfer or storage of third party personal data. Contrary to the Article 29 WP, Ecommerce Europe does not see any valid argument why such an assessment should only be carried out by the receiving data controller. As this *ex post* control will frustrate the fundamental rights and freedoms of the involved third parties, only to enable the far less fundamental right of the data subject on data portability, Ecommerce Europe strongly opposes the suggestion of the Article 29 WP to have this data transferred without any check in the initial stage of a request on data portability.

Data portability tools: Direct download opportunity and API
By using the wording "they should offer..." in the guidelines on page 5 on data portability tools, the Article 29 WP seems to suggest that the data controller under Article 20 has a mandatory obligation to offer a direct download opportunity on his site which could be implemented by making an API available.

As it is not mandatory to offer a direct download opportunity, and as such an opportunity is particularly not indicated where personal data of third parties are involved in the request on data portability, it should be perfectly clear that the choice for adequate data portability tools is totally at the discretion of the controller. In that perspective, Ecommerce Europe strongly recommends that the Article 29 WP changes the wording "they should offer..." to "they could offer...".

Interoperability of transferred data
To ensure the interoperability (portability does not aim to produce compatible systems) of the data format provided in the exercise of a data portability request, the Article 29 WP strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability (page 3 and 14). As also expressed in the ICDP paper, Ecommerce Europe believes that the requirement of providing portable data in a structured, commonly used, machine readable, and "interoperable format" should be clarified. In particular, Ecommerce Europe is worried about defining the terms "interoperability" and "machine readability" on the basis of EU secondary law and implementing acts aimed at the public sector[2]. Moreover, the guidance should differentiate between "interoperable data formats" and "interoperable systems". While the former is rooted in the GDPR, the latter is not a requirement nor a goal. Indeed, according to Recital 68 there is no obligation for the controllers to adopt or maintain technically compatible processing systems. It is very important that the GDPR will remain technologically neutral. Online traders should remain free to grant the data subject's right to data portability with the technological solution they consider the most suitable and to use any format which does not inhibit the data subject from using the data should be allowed, including most popular and common standards for structured documents and web data[3].

How to help users in securing the storage of their personal data in their own environment
In the opinion of the Article 29 WP (page 15), the data subject should be made aware of the fact that by retrieving his/her personal data from an online service, there is always a risk that he/she may store this data in a less secured system (mostly his own) than the one provided by the service. However, the Article 29 WP does not clarify who is the addressee of this duty to raise awareness. By advising that the data controller, as a best practice, could recommend appropriate format(s) and encryption measures to help the data subject to achieve his goals on security, the WP seems to suggest that the data controller transferring data to the data subject that requested data portability is the addressee of this duty.

However, Ecommerce Europe is convinced that the protection and storage of (his or her own) personal data that the data subject choses to store in his/her own system or individual environment, completely falls under the responsibility of the data subject itself. It should be very clear from the text of the guideline that this is not a responsibility of the online service provider and that it is up to the discretion of the service provider to provide the data subject that retrieved data in the course of a request for data portability, with recommendations on appropriate formats and encryption measures.

---

[2] "ICDP comments on the Article 29 Working Party's guidance on data portability", February 2016
[3] *Idem*

Authentication, risk of adverse effects on the rights and freedoms of others, and refusal on request

The guidelines should clarify further what sort of authentication processes would be required by controllers exporting or importing personal data in the context of the data portability right and ensuring that these do not disproportionately affect businesses, considering the costs and time required to authenticate a data subject.

Furthermore Ecommerce Europe supports the ICDP paper in asking for guidance on the question when a controller a controller may reasonably refuse to act on a request for data portability because it is unable to reasonably authenticate the data subject, as may be the case in services that do not operate on a log-in basis. Requiring the provision of data portability where a data subject is not identified or authenticated, may carry with it a risk of a data breach that may adversely affect the rights and freedoms of others. The draft guidance should clarify that the right to data portability must not adversely affect the rights and freedoms of others[4], and - where it does - it should be clear that the trader has the right to refuse to transfer the requested data.

Relevant Extracts from the GDPR

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply when the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply when the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. 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. When, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

For any questions, please contact Ecommerce Europe at info@ecommerce-europe.eu.

[4] "ICDP comments on the Article 29 Working Party's guidance on data portability", February 2016