54.

GSMA Comments on the Article 29 Working Party "Guidelines on the right to data portability"

31 January 2017

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com
Follow the GSMA on Twitter: @GSMA

Policy Contacts

[redacted]GSMA

We welcome the Article 29 Working Party's ('Article 29WP') draft Guidelines on the right to data portability' ('Guidelines'), developed with the aim of providing guidance to organisations for interpretation and implementation of the EU General Data Protection Regulation ('GDPR'). We are encouraged that the Article 29WP has reaffirmed the commitment to technology neutrality reflected in the GDPR. We also appreciate the Article 29WP's clarification that some data created by controllers on the basis of data provided by data subjects would fall outside the scope of the right to data portability. This guidance will facilitate the practical implementation of this right and help provide more protection for the trade secrets and intellectual property of data controllers, with the goal of supporting innovation.

However, the Guidelines also contain highly problematic interpretations that may be inconsistent with the aim of Article 20 and with the intention of the legislators, given the changes in the text adopted during the legislative process. This would ultimately lead to more legal uncertainty for companies and data subjects alike.

Our concerns and questions regarding these Guidelines fall into seven areas: 1) data 'provided by' the data subject; 2) personal data of third parties; 3) interaction with data retention legislation; 4) interaction with other existing obligations; 5) authentication challenges and associated risks; 6) security; and 7) costs.

1. **Data 'provided by' the data subject**

The GDPR purposefully narrowed the scope of the personal data affected by the right to data portability to data 'provided by' the data subject. This wording was chosen deliberately over 'processed' personal data, in order to avoid conflicts with regard to the different rights of data controllers, data subjects and third parties, while creating an easy-to-execute right for the data subject. A broader interpretation of the scope would contradict this limitation.

Furthermore, a broad interpretation that the meaning of 'provided' should include 'the use of the service or the device' would lead to conflict of laws and several privacy issues as further outlined in comments below. In addition, it would also lead to insolvable problems for the data controller. As an example, from a technical point of view, most service providers do not have a separate database containing only the raw data that can easily be separated from the algorithms to create profiles for customer analytics. Transferring this data to another service provider would in almost all cases reveal detailed background information about the technical setup of the original controller and the algorithms used. Therefore, the very base of the controller's business would be revealed, leading to impacts on the commercial interests, intellectual property and trade secrets of the transferring controller. To mitigate these issues, most controllers should only provide data that is not affected by these concerns, linking back to the initial wording of Article 20 of the GDPR (data provided by the data subject, not data by virtue of usage).

2. Personal Data of Third Parties

The right to data portability creates a myriad of legal uncertainties which can be detrimental to the data subject, especially for electronic communication data with legal deletion obligations. In the case of traffic and location data, it is unclear what the implications for the data subject and the new data controller are, given the obligation to delete respective data according to the ePrivacy Directive (and the proposed Regulation on Privacy and Electronic Communications ('ePrivacy Regulation')). In addition, the porting of traffic data always impacts the rights of third parties and this may be considered by some as having an adverse effect on the third parties. This would be a violation of section 4 of Article 20.

Further, the Guidelines note that when the personal data of third parties is included in a data set, another ground for lawfulness of processing must be identified, such as legitimate interest. The ePrivacy Directive provides limited legal bases for processing, and as a result Mobile Network Operators will be unable to rely on another grounds for lawfulness of processing. As a result, the grounds for lawful processing that Mobile Network Operators should utilise to process personal data of third parties included in call logs and traffic data must be clarified.

We also seek confirmation that any 'directory' information including the personal data of third parties may only be used by the requesting user in the context of 'purely personal or household needs' and that the subsequent controller may not use the data for their own purposes. For example, if a data subject requests copies of call detail records from a Mobile Network Operator, and those call detail records include the personal data of third parties, then those call detail records may only be used by the requesting data subject for 'purely personal or household needs.' However, whether or not the data subject uses the data for 'purely personal or household needs' - or the subsequent controller uses the data for its own purposes - these circumstances are beyond the original controller's control.

The Internet of Things will also impact the personal data of third parties. For example, in the case of a home device that generates raw data from the observation of the household, portability will lead to a transfer of personal data relating to data subjects that could have been in the household for a certain period of time but were previously not the focus of the processing activity. This could inadvertently lead to the identification of those individuals which cannot have been the intention behind the right.

3. Interaction with Data Retention Legislation

Additionally, where the reference to 'telephone records' includes call and internet data, and such data is retained under data retention laws which are currently in force in certain jurisdictions (such as the Irish Communications (Retention of Data) Act 2011, as may be updated in due course) would this data be considered data processed with either the data

subject's consent or for the performance of a contract and therefore subject to the right of portability? The Irish Communications Act outlines that its purpose is to, inter alia, "provide for the retention of and access to certain data for the purposes of the prevention of serious offences, the safeguarding of the security of the State and the saving of human life...".

Further, if operators are required to transmit call and internet data to another controller on request, how can the retention of such records be addressed by the 'new' controller where Member States have national law requiring retention of those records for specified periods? Where national laws exist requiring retention for a specified time for State purposes, should the 'ported' records be retained for the balance of such periods only, or is the clock deemed to be 'reset' requiring the operator to retain the data for the entire period from the date of receipt of the 'ported' records? Would the retention period also be impacted if the data is moved from one Member State to a provider in another Member State subject to different legislation?

4. Interaction with Other Existing Obligations

Clarification is needed on how the release of incoming call data to a data subject on the basis of a portability request interacts with other existing obligations including:

a. The right of a calling end user to restrict calling and connected line identification in the ePrivacy Directive. We note that the new EC proposal for a ePrivacy Regulation maintains this right for the calling end user and states that "it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made (...)" (Recital 27, proposed ePrivacy Regulation). Identifying an incoming calling party who has exercised this right for the purposes of responding to a data portability request would thus be inconsistent.

b. Article 7 and 8 of the Charter of Fundamental Rights of the European Union in particular with respect for the private life and the protection of personal data in connection with the provision and use of electronic communications services.

c. Limitation on the possibility, for the data subject, to obtain data referring to incoming phone calls, in force in certain jurisdictions. For instance, according to art. 8.2(f) of the Italian Personal Data Protection Code (legislative decree no. 196/2003), if the data concern incoming phone calls, a data subject may not access his/her personal data, by simply making a request to the controller or processor. Such records can only be disclosed by order of the prosecutor in the context of criminal proceedings.

5. Authentication Challenges and Associated risks

There are other data portability issues specific to Mobile Network Operators, including authentication challenges. Significantly, in many cases, the authenticated account holder is not the user of the service, and we should seek to avoid situations potentially jeopardizing the user, e.g. where a call has been made to a domestic violence or child sexual abuse helpline (or similar) and the information about that call is provided to the abuser. This is particularly important in the case of children and other vulnerable populations who do not understand the potential impact on their privacy and security, and where it is possible that the account holder is actually the perpetrator of the abuse. While the GDPR addresses many facets of privacy, there are other aspects to consider, including confidentiality of communications and protection of the vulnerable/abused for which we have other protections in place, now potentially being jeopardized by over-interpretation of the GDPR portability requirement.

6. Security

In addition to issues relating to authentication of the person making the request, any requirement to give data subjects the right to access and retrieve the data processed by network elements used to provide public communication networks and services, would give rise to significant concerns about the confidentiality of communications and the networks over which they are transmitted, and would potentially increase the points of vulnerability which would be attractive to hostile third parties to exploit. In many cases, this would concern the security of national critical infrastructure.

7. Costs

By way of comparison, the cost of introducing the technology and processes to enable number portability have been very substantial; operating costs alone incur up to millions of Euros per operator on an annual basis. It is noteworthy that number portability concerns one, highly standardized and static data attribute. A call detail record can consist of more than 42 data fields, constantly being created by the network, raising the prospect of massive costs. If unstructured data sets are in scope, the complexity of implementation may increase substantially.