12.

DIGITALEUROPE

DIGITALEUROPE's views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242)

Brussels, 1 February 2017

EXECUTIVE SUMMARY

DIGITALEUROPE as the voice of the digital technology industry in Europe welcomes the opportunity to comment on the Article 29 Working Party's ("WP29") draft guidelines on the right to data portability (WP 242). DIGITALEUROPE believes that the effective implementation of the General Data Protection Regulation ("GDPR") will require a joint effort between all stakeholders **built on mutual trust**. We therefore welcome the decision of the WP29 to deviate from previous protocol and treat all guidance documents, including WP242, as a draft guidance document while encouraging feedback from the data protection community.

DIGITALEUROPE believes that the main objective of WP 242 should be to achieve **legal certainty** so that data controllers of all sizes across the EU clearly understand how the right to data portability should be implemented and will be enforced. While we welcome some of the clarifications presented in the draft document, we believe many questions remain. We are particularly concerned with the broad interpretation of the WP29 in some instances, which we believe could be difficult for companies (both large and small) to implement. DIGITALEUROPE has structured its comments in the following manner, aimed at summarising our key views:

DIGITALEUROPE
Rue de la Science 14 - 1040 Brussels - Belgium
T. +32 (0) 2 609 53 10 | F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register number for the Commission: 64270747023-20

OVERALL VIEWS

DIGITALEUROPE welcomes the fact that the WP29 has recognised the extensive technical and engineering work that will be required by data controllers to comply with the right to data portability by providing guidance on this issue. We welcome, in particular, the clarification the WP29 has provided on the format for the production of personal data, and the need for authentication and strong protections for the portability process.

However, the draft guidelines do not seem to take into account the variety and diversity of sectors to which the right to data portability will apply. While the right to data portability will likely have a strong impact on online service providers including social networks, search engines and online retailers, DIGITALEUROPE is concerned that the **draft guidelines seem to have been written with only these sectors in mind**.

The insurance, banking, telecommunications, healthcare, transport, and retail industries will all face different challenges of how the specific rules pertaining to right to data portability will apply to their sectors. As such, we urge the WP29 to **fully consider the complexity that the right to data portability places on all sectors of the economy** beyond online service providers. It is recommended to start from concrete reasonable expectations of data subjects in those sectors where data portability could have a clear added value for the data subject rather than applying to all sectors/applications/services. This is especially relevant for those sectors where different portability rights are already implemented, as is the case for the telecoms sector.

SPECIFIC CONCERNS

1. Objective of the right

The objectives of the right to data portability as described in the draft guidelines are not sufficiently clear, particularly as an important aspect of the right seems to be already covered by Article 15. DIGITALEUROPE fully understands that the objective of Article 20 is to go beyond Article 15 so that data subjects may transfer personal data to other data controllers and avoid potential 'lock-in'. However, given the extensive interpretations by the WP29, the question arises whether the broad interpretation by the WP29 of Article 20 is the correct solution to the perceived 'lock-in' problem, as the problem varies across industry sectors. A clear answer to the question of 'which problems will this interpretation solve' is not provided.

2. Controllership

The draft guidelines specify that *'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'*. DIGITALEUROPE believes that this does **not sufficiently address the issue of the relationship between a data controller and a data processor** when the right to data portability is exercised by a data subject.

When it comes to the **receiving data controller**, we suggest the following amended wording to the draft guidelines:

> *'...the new data controller ~~does~~ <u>may</u> not need to retain all the details of the transactions once they have been labelled.'*

3. Legal basis

DIGITALEUROPE recognises that each organisation will be required to differentiate the legal basis for processing between personal data of the same individual given that the right to data portability can only be exercised when two of the legal bases set out under Article 6(1)(a) and Article 9(2)(a) or Article 6(1)(b) are used. While all legal bases will now need to be documented by organisations, we call for a reasonable standard on how organisations should respond to portability requests, particularly when considering examples such as a healthcare provider or financial institutions, which have collected data across different databases throughout several years of a relationship with the data subject(s). **We believe the draft guidelines do not properly acknowledge and provide adequate guidance on the complexity of such an exercise**. Furthermore, we could foresee that difficulties may arise for data controllers given that the guidelines specify that pseudonymous and encrypted data are in the scope of the right. When such technological solutions, particularly encryption, are used it can be difficult for data controllers to 'tie-back' that data to individual data subjects on demand.

4. Scope

DIGITALEUROPE welcomes the position that data inferred, or derived by the provider is not within the scope of the right, and that the right to data portability applies to data knowingly and actively provided by the user. This includes the examples of observed data provided by the WP29, such as search history, location data, or health information collected by fitness tracking devices (i.e., personal data that services are designed to enable users to track). These examples provide a helpful illustration of the appropriate scope of the right to portability, ensuring both that users benefit from a full portability right, and that such a right is not overly extensive, which would defeat its utility to individuals.

However, questions remain, particularly regarding the application of Article 20(1). The draft guidelines **adopt a wide interpretation** of data *'provided by virtue of the use of the service'* or *'generated by and collected from the activities of users such as raw data generated by a smart meter*. This is particularly concerning when considering **employees' personal data**. We firmly believe that data collected in an employee relationship should not be subject to Article 20 as this would in many instances violate current employer's confidentiality interests.

In addition, in instances when a data controller is responding to a data portability request pursuant to Article 20(2), we wish to express our concern that the WP29 has essentially **put the burden on the receiving data controller to protect third party personal data and determine which data is relevant for the new processing as well as the appropriate legal basis to be used**. The requirement to assess incoming data for relevance suggests some sort of manual process, which is not realistic for the vast majority of companies. Further, the requirement not just to assess but also to delete what information isn't strictly necessary would create a significant additional workload for companies. At the same time both the receiving and sending data controllers are still required to make investments to *'...implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data.'*

DIGITALEUROPE encourages **the WP29 to adopt an approach that offers adequate protection for other data subjects**. We believe that it would be more effective to restrict the right to data portability to data that does not include other data subjects' data.

We therefore would welcome the final guidelines to **include additional considerations for the exercise of the right** to data portability when other data subject's data are included such as:

- **Proportionality** – the amount of other data subjects' data in relation to the data that is requested to be ported
- The **purpose** for which the right is exercised
- The **feasibility** or complexity of separating other data subject's data
- The **usability** of the data ported after other data subject's data have been excluded
- The actual **legal basis** on which the personal data of third parties can be transferred to another data controller without their consent – Without this clarity, transferring data controllers carry a potential legal liability.

These criteria could be applied to broad categories of data to ensure consistent and effective deployment. We believe that such additional criteria would be of assistance for receiving data controllers to, as best practice, *'provide data subjects with complete information about the nature of personal data which are relevant for the performance of their services.'* Once again, **such a requirement poses a burden for the receiving data controller, including by requiring processing of third party data**. Receiving data controllers would need to process the data before they can provide such information, establish a legal basis or delete the data. We believe such requirements to be impracticable without the inclusion of the criteria suggested above. The WP29 should especially take into account the resources of SMEs in responding to portability requests.

We urge the WP29 to recognise how far-reaching the exercise of the right to data portability can be and how complex it is for data controllers across all sectors to prepare in order to ensure they are able to satisfy this right. **A wide interpretation significantly beyond what is set out in the GDPR risks jeopardising the goal sought by all stakeholders, which is a reasonable balance between the data subject's request and the data controller's obligation**s. All requests must be 'clearly and reasonably defined' and 'proportionate' to the objectives pursued by the exercise of the right.

Moreover, we note the suggestion that data controllers create a means to allow for the transmission of data to personal data stores or trusted third parties. It would be **important for the guidance to clarify the legal basis for this requirement.**

We believe that the guidance **fails to understand that complex data sets cannot be simply ingested into systems and then simply used**. While the goal to specify common formats is understood it must equally be understood that **complex data systems are not capable and never will be capable of allowing a "plug and play" type scenario for ingested data**. The necessary engineering work is impossible to quantify. Instead, the ingesting of data is a matter for each receiving data controller in terms of the relative benefit that they perceive from allowing the easy porting of users from one service to another. In summary, while there may in fact be an incentive on receiving data controllers to be able to ingest and use data received under the data portability right, **there is no legal basis requiring that they do.**

5. Cost to data controller

DIGITALEUROPE agrees with the WP29 that the *'overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request.'* However, we believe the **draft guidelines take an unbalanced stance when further developing the principle**. The WP29 suggests that *'as a result, the overall system implementation costs should neither be charged to the data subjects, nor be used to*

justify a refusal to answer portability requests.' While Article 12 focuses on the requests made by one data subject and not on the total number of requests received by a data controller, the right to data portability can undoubtedly give ground to excessive requests. Therefore, we believe that **in order for data controllers to be able to satisfy adequately reasonable requests, there should be more criteria provided** on what constitutes an excessive or indeed repetitive request that can be refused with legal certainty.

Furthermore, the draft guidelines stipulate that '*for information society or similar online services that specialise in automated processing of personal data, it is very unlikely that the answering of multiple data portability requests should generally be considered to impose an excessive burden.*' We believe **such an assumption is unrealistic and pre-mature** given the complexity described above particularly until the exercise of this right is observed in practice. In fact, the statement **demonstrates a lack of understanding of the complex and detailed technical and engineering work that will be necessary to comply with this right.**

6. Inferred and derived data

It is our observation that data portability rights would be better understood and implemented by the stakeholders in the ecosystem if they were expressed using **well-defined and well-understood concepts and terminology**. The clarification offered uses nuance descriptions of various types of data and how the data portability rights should be handled based on them. To that end, DIGITALEUROPE would recommend that the data portability clarifications be expressed using **standardised terminology and concepts**, for example as described in the upcoming ISO/IEC 19944. This standard clearly defines customer data, derived data as well as service provider data and their sub-types. It is our belief that expressing data portability rights based on standardised types of data, and the degree to which the data is de-identified, would make the implementation of data portability rights more concise and clear.

As previously mentioned under section 4, DIGITALEUROPE welcomes the clarification that data that is '*exclusively generated by the data controller*' (i.e. inferred and derived data) are not within the scope of the right to data portability. The guidelines acknowledge that inferred and derived data are created or enriched by the data controller on the basis of the data initially '*provided by the data subject*'. The guidelines further acknowledge that 'provided by' includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but not subsequent analysis of that behaviour.

DIGITALEUROPE believes that **this distinction is not practical**. The very questions or data fields asked by the data controller may be where the data controller applies innovation and trade secrets, particularly when these questions/data fields are responded to by a large number of data subjects. Moreover, where the data is not actively provided by a data subject, but rather collected from the data subject's *use* of a service, this data is usually processed and analysed immediately and then stored in a way that provides value to the data subject and the data controller alike. This value is created by the data controller's analysis and processing of the data, similar to inferred data. Therefore, "observed data"— data collected from devices and the use of services-- should be considered **out of scope**, for the same reasons that inferred and derived data are.

The draft guidelines describe search history and location data as examples of observed data. DIGITALEUROPE believes these are prime examples of how value is created by subsequent analysis of "raw" user data. For example, a data controller may create a map to help users visualise their observed location data or may create a dashboard to help users navigate and sort through their search history on the site. The effort undertaken by the data controller to organise and derive meaning out of this data means this data is enriched and therefore

proprietary to the data controller. As such, it should be **out of scope of the right to data portability**. We also believe that **metadata** should be out of scope of the right to data portability, since they are generated by the data controller and not by the individual. Lastly, we also welcome the clarification that inferred and derived data, including algorithmic results generated by the service provider and data controller are not within the scope of the right to data portability.

7. Personal data containing the data subject

DIGITALEUROPE welcomes the clarity regarding information provision further to Articles 13(20)(b) and 14(2)(c). However, the **suggested requirement that all customers be informed at the time of account closure of the right to data portability is not grounded in Article 20**. Data controllers have many processes in place for ensuring customers can delete and/or close their accounts. Adding a requirement to further inform users about data portability rights at this points would create unnecessary complexity to the process.

8. What prior information should be provided to the data subject

DIGITALEUROPE is concerned about the views of the WP29 that *'...pseudonymous data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier, cf. Article 11 (2)) is well within scope'* and that where online information is linked to pseudonyms and unique identifiers, data controllers "can" implement appropriate procedures enabling an individual to exercise the data portability right. Indeed, the guidance gives no indication of the sorts of procedures which the WP29 has in mind, nor does the guidance recognise the difficulties in authenticating such requests.

The implications of this interpretation on data controllers, particularly those which have undertaken steps to comply with the separate obligations contained in Article 25 of the GDPR in relation to data protection by design and by default, would be severe. Where a data controller does not possess an identifier and has specifically engineered their product or service so that the data is not personally identifiable in their holding, then **Article 11(2) does not create a basis for a user to provide an identifier that a data controller does not otherwise have and for such data to then become arguably identifiable**. This would be a retrograde step for privacy and would by implication create a disincentive for data controllers to hold data in a format in which the data is rendered not identifiable in their possession. Any guidance should therefore re-iterate that Article 11(2) holds for data portability along with all other data subjects.

9. Expected data format & large/complex datasets

DIGITALEUROPE welcomes the clarifications provided by the draft guidelines on the expected data format when porting data as well as the recommendations on how data controllers should deal with large or complex personal data collection. However, we would once more like to point out the complexity of this right given this right applies to all sectors of the economy. It should also be noted that Article 20 specifically does not seek to differentiate between services where a data controller is offering a broad range of services. **There is no obligation on a data controller to offer a suite of choices as suggested in the guidance.**

10. Intellectual property and trade secrets

With respect to data covered by intellectual property and trade secrets, DIGITALEUROPE welcomes the clarifications provided by the draft guidelines. We believe that the wording of the final guidelines should allow for the determination of a case-by-case basis and as such suggest the following amended wording to the draft guidelines.

> *'...the result of those considerations should normally not result in ~~be~~ a refusal to provide all information to the data subject.'*
>
> *'A potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request and data controllers ~~can~~ should generally be able to transfer the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.'*

It would be helpful to have a stronger acknowledgment from the WP29 of the right of the controller to protect its intellectual property - as this is addressed only briefly in the guidance. For example, by having to provide the data in an interoperable format (and not merely providing access), companies may have to share with their competitors their method of collecting, structuring, and using this data.

Additionally, further clarification would be welcome that 'affected rights' can be confidential rights as well as set out under Recital 63. This should not be limited to intellectual property. The respective rights of the data controller must be considered against a data portability request when asserted.

11. Interoperability and use of download tools

Concerning the encouragement to ensure the interoperability of the data format provided in the exercise of a data portability request, we re-iterate the fact that this right applies to multiple sectors and note the **difficulty of being able to pre-define interoperability needs.** When it comes to the use of download tools and Application Programming Interfaces ("API"), we urge the WP29 to recognise in the final guidelines that this **may not be a desirable or feasible option in all sectors of the economy.** As a minimum, to ensure that the precise legal requirement is accurately reflected, the guidance needs to recognise that Article 20(3) contains a specific recognition that the obligation to transmit from one data controller to another is **only applicable where it is feasible to do so.**

12. Technical feasibility

Further to the above, while DIGITALEUROPE welcomes the flexibility set out in Article 20(2) when a data subject requests for personal data to be transmitted from one data controller to another, **further guidance on the limitations of technically feasible would be welcomed**. We would particularly welcome more guidance on when it can be considered that it *not* technically feasible, specifically whether there are criteria that companies can consider other than the lack of interoperability.

CONCLUSION

DIGITALEUROPE once again wishes to thank the WP29 for providing the European digital technology industry with the opportunity to submit comments on the draft guidelines on the right to data portability. As previously mentioned, it is of paramount importance that data controllers receive legal certainty so that all industry sectors clearly understand how the right to data portability should be implemented and enforced. We trust that the WP29 will make an objective judgement of the feedback it has received from all stakeholders so that the final guidelines reflect the not only the original intentions of the legislators, but also the technical and engineering reality facing data controllers when seeking to comply with the right to data portability.

--

For more information please contact:

[redacted]

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK