To:

JUST-ARTICLE29WP-SEC@ec.europa.eu

presidenceg29@cnil.fr

Brussels, 15 February 2017

EBF_025448E

EUROPEAN BANKING FEDERATION'S COMMENTS TO THE WORKING PARTY 29 GUIDELINES ON THE RIGHT TO DATA PORTABILITY

Article 20 of the General Data Protection Regulation introduces a new right to data portability which aims at empowering the data subject by giving him/her more control over his/her personal data and encouraging free movement of data within the European Union. Data portability is central in order to provide customers with more choice, avoid data monopolies (competition issue) and allow personal data to be available to other operators (with consumer consent). Within regulated industries, customers already experience and benefit from the possibility to switch from one service provider to another.

The European Banking Federation (EBF) welcomes the possibility given to provide comments on the Guidelines prepared by the Article 29 Data Protection working party (Article 29 WP) on the right to data portability.

In our views, further considerations should be given to the need to:

- Clarify the liabilities in the application of the data subject's right to receive personal data and the right to transmit personal data from one data controller to another data controller;
- Ensure that the scope of the right of data portability is only limited to data actively provided by the data subject to the controller (raw data);

- Ensure that sufficient security is maintained and risks prevented in the context of the transmission of personal data to the data subject;
- Ensure the framework of the right of data portability of the General Data Protection Regulation[1] (GDPR) is aligned with recent legislative initiatives at EU level which already regulate the right to data portability (for example the Payment Accounts Directive (PAD)[2], the new Payment Services Directive (PSD2)[3] etc.);
- Ensure that public consultations of stakeholders will take place prior to the adoption of the guidelines with a reasonable period of response.

1. MAIN ELEMENTS OF DATA PORTABILITY AND LIABILITY ISSUE (PAGE 4-6).

- **The right to receive personal data and right to transmit personal data from one data controller to another data controller (page 4 and 5)**

  - According to the Guidelines *"data portability is a right to receive personal data processed by a data controller, and to store it for further personal use on a private device, without transmitting it to another data controller. In this regard, data portability complements the right of access. One specificity of data portability lies in the fact that it offers an easy way for data subjects to manage and reuse personal data themselves".*

    The data subject can exercise its right of data portability to directly transmit the data from one controller to another. Considering the sensitivity of some data (including some banking data), in the event the customer exercises his/her right of portability to store the data for further personal use on a private device, without transmitting it to another data controller, then, a clarification regarding the liability of the controller and the data subject to ensure the safety of the data is very important. It will notably avoid that the controller is latter on recognised liable for any damages that can affect the customer or third parties due to improper use of data.

  - In addition, we believe it would be necessary to emphasize that the "sending" data controller cannot prevent adverse effects on any third parties involved in the context of the data portability.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[2] Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

[3] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

In this context we very much support the approach adopted by the guidelines which mentions 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*".

We also welcome the approach of the Article 29 WP which recognises the security risks which might occur in the context of the right of data portability in particular that "*by retrieving their personal data from an online service, there is always also the risk that users may store them in a less secured system than the one provided by the service*" and the importance for the data subject to be made aware of this in order to take steps to protect the information they have received (see also our argumentation regarding the security issue).

- **Awareness of the data subject**

We think in this context it is very important that:

- the data subject is fully aware of the lower regulatory requirements that may apply to some receiving data controllers. These may not have the same legal obligations outside of the GDPR (for example confidentiality, data security etc.);
- The right of data portability should not derogate from higher regulatory requirements already in place;
- The data subject is aware that the 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 (as recognised by the guidelines in the paragraph on 'controllership' on page 5).

2. THE SCOPE OF THE RIGHT OF DATA PORTABILITY WHICH SHOULD BE LIMITED TO DATA PROVIDED BY THE DATA SUBJECT TO THE CONTROLLER (PAGE 6-10)

Pursuant to Article 20(1) of the GDPR, to be within the scope of the right to data portability, data must be a) personal data concerning him or her, and b) which he or she has provided to a data controller.

However, the Article 29 WP Guidelines has chosen to adopt a broad interpretation of what "portable data" is. In our views, this interpretation goes beyond the intent of the legislator in article 20 of the GDPR or in the recitals.

We very much welcome the exclusion of "inferred data" and "derived data", which include personal data that are generated by the service provider (e.g. algorithm results as credit score) but believe that, in line with the GDPR, only the data actively provided by the data subject to the data controller should fall in the scope of right to data portability.

Indeed it would not only concern data that has been provided by the data subject himself but also data generated by the use of the service. It also covers data that refers to others than the data subject. There is a need to clarify the term "technically feasible", or to consider that there is technical feasibility by default. If a data controller claims unfeasibility, it would have to prove it. Otherwise, direct portability between controllers may become an exception and there would not be a level playing field between players.

- **Clear distinction between raw data and managed/derived data is needed**

  - We believe, a clear distinction should be made between 'raw data' and 'managed/derived data': 'raw data' are those provided by the customer and 'managed/derived' data are those that have undergone further processing, such as verification, internal processing, cybersecurity checks, analysis, etc. Data that results from the processing of the controller should, by no means be considered as 'raw data' provided by the data subject.

    These should belong to the companies that create an additional level of value based on their know-how.

  - Some companies, notably banks, tend to enhance the quality of the raw data they receive from customers and other sources. In fact, they are often legally required to guarantee a higher quality of data (e.g. for Anti-Money Laundering, credit facilitation etc.). These processes create an additional layer of value on top of the raw data.

    We believe it is important to recognize that there is an added value in the data managed by those companies. When the customer applies for data portability, we believe that this should only include the raw data that he/she has provided - but not the data of enhanced quality that is the result of further verifications and analysis run by the data controller to fulfill his/her legal obligations. It is also important to keep in mind that some activities (notably for banks) are subject to strict supervision which implies going through a specific processing with a strict verifications of the raw data provided by the data subject. In line with the distinction made above between 'raw data' and 'managed/derived data', it would appear contradictory to allow the portability of such data.

  - Only the data actively provided by the data subject to the controller (= data input) should be considered in the scope, meaning that the data subject can request his/her original input (e.g. his identification data or his order data).

- Should portable data include both raw data and managed/derived data, it would mean that the right to portability would permit the free transmission of this added value enhancement. Consequently, both EU competitors and technology giants outside the European Union will unfairly benefit without any reciprocity. This approach cannot effectively contribute to the protection of data subject's rights.
- According to the GDPR, direct portability between data controllers will only take place when 'technically feasible'. It is important to make sure that this term is interpreted and implemented in a homogeneous way across EU Member States and industries, and to foster standardisation and direct portability between data controllers.

  It is important to take into account the difference between 'raw data' and 'managed/derived data' as well as the distinction between personal and non-personal data (which is already included in the GDPR). It should be clear that portable data means raw personal data directly provided by the customer.
- Even for the portability of what we define as raw data, the GDPR will require that all data controllers share sets of personal data provided by the data subjects - should they individually request so - with the data subjects themselves (with a third party only when considered 'technically feasible') and using a 'structured, commonly used, machine-readable and interoperable format'. In the GDPR, there is however no "obligation for the controllers to adopt or maintain processing systems which are technically compatible" (Recital 68 of the GDPR). For example, there should not be obligation to make data from different banking systems technically and semantically compatible.

- **Application of new concepts to data (page 8)**

  We would however appreciate further clarification about the interpretation of new concepts of 'observed data' and 'inferred data' created by the Working Party, particularly, taking into account that the term, according to the article 29 WP, 'provided by the data subject' is interpreted broadly and that 'observed data' are included in the data portability right.

  We would welcome deep analysis of the mentioned concepts based on the principles and requirements established in the GDPR (e.g. meaning of 'personal data', existence of a filing system).

  Also, we consider that for defining the concept of 'observed data', the relevance of processing based on the main activity of the data controller and its relationship with data subjects, should be taken into consideration. As well as the purpose of the legislator, when introducing the data portability right, to enable the switching of providers and avoid lock-in situations.

  Further attention should be also given to the feasibility of the portability when defining the concept of "observed data".

- **Clarification between access and portability**

  We also believe that it would be more appropriate to specify the relationship between 'right of access' to data (incl. the right to get a copy of data processed) and 'portability' considering that they respond to different purposes and they are applicable in different contexts.

  Putting them in connection may induce that it is more effective to exercise the right to portability of personal data for personal use, instead of the right of access. It could give the feeling that a wider range of data is communicated with the 'right to data portability' compared to those obtained by exercising 'the right of access' when to the contrary the right of data portability covers a more limited amount of information.

- **Further consideration should be given to the level playing field among the different actors and fair competition**

  Data portability requirements should foster a level playing field between the different data controllers so that data subjects continue to benefit from better data quality and protection. Otherwise it could lead to competitive disadvantages. The sending data controller may have invested considerably in obtaining the data, whereas the receiving data controller need not.

  There is an opportunity for the regulatory framework to ensure that the relevant European sectors, such as the banking sector, have the right incentives to keep investing in validating the accuracy of data and enhancing data methodologies.

- **Processes to automatically answer portability requests (page 7)**

  As stated in Recital 68 and Article 20 of the GDPR, data portability is applicable where the processing of personal data is based either on consent or on a contract. Based on the above, we do not agree with the "good practice" indicated in the footnote number 9 which proposes to develop processes to automatically answer portability requests, by following the principles governing the right to data portability in case of processing based on the legal ground of necessity for a legitimate interest and for existing voluntary schemes. It is important to recall indeed that in certain countries some processing based on legitimate interests is needed to detect and prevent money laundering and other financial crime. The portability of such data does not contribute to the purpose of data portability itself, which is facilitating the customer to switch from one service provider to another. This recommendation goes beyond what the legislator intended to achieve with the introduction of the data portability right.

Based on the above we recommend deleting the following reference included in footnote number 9: *"However, it is a good practice to develop processes to automatically answer portability requests, by following the principles governing the right to data portability. An example of this would be a government service providing easy downloading of past personal income tax filings. For data portability as a good practice in case of processing based on the legal ground of necessity for a legitimate interest and for existing voluntary schemes, see pages 47 & 48 of WP29 Opinion 6/2014 on legitimate interests (WP217)."*

- **Data covered by intellectual property and trade secrets (page 10)**

The guidelines states that "(…) *a potential business risk cannot serve as the basis for a refusal to answer the portability request*".

We would appreciate further clarification about this matter and a deep analysis regarding the limitations included in this paragraph.
Particularly as regards large datasets, it is a relevant point to clarify to avoid unfair competition and breaches of controller's IP rights. Indeed although controllers might not have IP rights to specific data points, they might have IP rights over the databases, which could be impacted if there are large numbers of portability requests.

Additionally, in those cases in which the controller processes a large quantity of information concerning the data subject, in order to prove its due diligence and as indicated in Recital 63 of the GDPR, this section should include that the controller should be able to request that, before the information is delivered, the data subject shall specify the information or processing activities to which the request relates.

3. APPLICATION OF THE GENERAL RULES GOVERNING THE EXERCICE OF THE DATA SUBJECTS RIGHTS TO DATA PORTABILITY (PAGE 10-15)

- **Prior information provided to data subject (page 10)**

With reference to the information that should be given to the data subject, Articles 13 of the GDPR just makes reference to the existence of right under Article 20. Therefore when the Article 29 WP Guidelines request the data controller to inform the data subject with an ex-ante disclosures of the types of data that can be obtained by exercising the right to portability, it goes beyond the level 1 regulation and introduce a complex and costly requirement. (see also cases in which data portability request should be rejected or a fee charged).

- **Security issue (page 15)**

  Financial data is perceived by the European citizens as well as National Protection Authority as very sensitive. The industry has always been aware of such threats and it has large experience in using high standards of protection. The citizens trust the industry with their data (see Eurobarometer results of 2015). In the wrong hands, or insufficiently protected it can have far reaching consequences for citizens.

  In general, the data controllers should guarantee the "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')" according to Article 5(1)(f) of the GDPR.

  However, in line with what has been described above the transmission of personal data to the data subject may also raise some security issues:

  - As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission). The industry observes that if the recipients of sensitive financial information do not fall under the rules and controls of the regulated financial industry, the risk exists that they will treat that data according to lower protection standards, increasing the risk that malevolent parties do not use it in accordance with the GDPR. The data controller is responsible for taking all the security measures needed to ensure that personal data is securely transmitted (e.g. by use of encryption) and received exactly as it has been sent (integrity) by the right receiver/destination (e.g. by use of additional authentication information). However, under the guidelines, such security measures should not be obstructive in nature and must not prevent users from exercising their rights, e.g by imposing additional costs. It may be very difficult in practice to ensure effective security and controls without creating any costs for data recipients. It would therefore be more appropriate for the guidance to refer to avoiding 'inappropriate' or 'disproportionate' costs.
  - By retrieving their personal data from an online service, there is always an additional risk that users may store them in a less secured system than the one provided by the service. It is then likely that criminals will seize this opportunity -without having to use the most advanced techniques- to easily access such computers and get their hands into the data. These data can be used for identity theft, plundering bank accounts of citizens, and potentiate other forms of fraud. In addition, such criminals will be more able to peek into the life of citizens constituting an attack to their privacy. This may lead to increased incidence of cyberattacks to consumer devices. As set out in the Guidelines, the data subject should be made aware of this in order to take steps to protect the information they have received. The

data controller could also, as a good practice, recommend appropriate format(s) and encryption measures to help the data subject to achieve this goal. It would be appreciated if the Guidelines would emphasise that such recommendations do not imply an increase of the liability exposure for data controllers.

- **Time limit imposed to answer a portability request (page 12)**

  It would be important to clarify whether data controllers which still hold personal data of the data subject are obligated to comply with a request of data portability in case the processing is ceased, or the relationship with the customer is terminated.
  If a customer relationship ends, can a portability request still be made? This can arise where the customer relationship has finished, but the firm must hold records for a certain period (e.g.: 10 years) in order to comply with legal or regulatory obligations in its Member State.

- **Cases in which data portability request should be rejected or a fee charged (page 12)**

  Further clarifications should be provided regarding the cases where data portability request be rejected or a fee charged. Particular reference should be made to data collected in the context of fight against fraud or anti-money laundering. Disclosing such data would amount to a 'tipping off" offence. We would appreciate a deep analysis (and further examples) with regard to the exceptions concerning data portability requests (i.e. unfounded and/or excessive requests) taking into consideration the tools and technical means used to transmit the information. Repetitive or frequent portability requests is given as an example of what can be considered excessive. However, the example is ambiguous. Some principles and examples (but not an exhaustive list) clarifying those elements would be appreciated.

- **The right of data portability should be aligned with existing legislations:**

  When interpreting Article 20 GDPR, it should be kept in mind that the right to data portability was created with major internet companies in mind. The leading idea was to promote consumer welfare by preventing so-called "lock-in-effects".

  "Lock-in" practices mainly refer to the tendencies of major internet companies to create high-level switching costs and to refuse to supply or deal with other competitors in order to build a user base of loyal customers. Lock-in becomes a concern when companies achieve large market dominance or become an essential facility (e.g. Facebook) and then impede competition. The guidelines of the Article 29 WP could be criticized as meaning that data portability will lead to disproportionate compliance cost in markets which do not suffer from customer lock-in.

Moreover, in the case of credit institutions, it should be generally noted that the prevention of lock-in effects has been area-specifically addressed by the Directive 2014/92/EU (Payment Accounts Directive / PAD). The account switching service required by the PAD contains data portability services. Therefore the PAD is *lex specialis*.

Similarly, the Payment Services Directive 2 should be reflected in the guidance, as it addresses many of the same issues, but is targeted at the financial services sector.

- **Overarching point: the need to accommodate industry differences**

Each industry has particular challenges and differences that may impact the appropriate manner in which to implement the right to data portability. Indeed, the guidance recognizes the importance of industry approaches.

As is clear in the sections above, in some sectors they are particular concerns on customer data, including around security, the interaction with other regulatory obligations (e.g. Anti-Money Laundering), and the sensitivity of those individual data. This being the case, the portability of such data must therefore be assessed in the light of existing regulations (such as for the banking sector, the newly adopted Payment Services Directive 2 (PSD 2), which includes specific provisions to ensure that data subjects' interests are protected (particularly through security requirements and licensing of data recipients)).

The guidelines in principle should cover all sectors but does not take into account the existing legislations each sector has to comply with. Moreover, a lot of the information that banks have regarding their customers must be protected for several reasons, for example from risk of fraudulent attacks. The right of portability must be seen in that light and take into account the risk of opening up sensitive data to actors who do not have the same obligations or level of regulatory oversight.

Since the banking industry is already bound by the portability obligation set out in the PSD 2 and the mobility principle included in the Payment Accounts Directive (PAD), the EBF would welcome a consistent approach that takes into consideration those existing requirements, the specific legislation and nature of certain data, in particular the unpredictable negative consequences which could happen if data is misused or treated insecurely. The data portability to other payment services providers will be attained through the mechanisms that the industry is putting in place for PSD2 and the disclosure of account information to regulated third parties.

This restriction of the data portability can be sustained in article 23.1 (J) of the GDPR: article 20 of the GDPR may not apply "when this is necessary for the protection of the data subject or the rights and freedoms of others".

4. THE IMPORTANCE OF PUBLIC CONSULTATIONS AND THE INVOLVEMENT OF STAKEHOLDERS IN THE ELABORATION OF THE GUIDELINES

The deadlines for compliance with the GDPR are very tight and guidance from Data Protection Authorities is needed promptly to enable data controllers to meet their obligations on time.

Adapting to the GDPR is an important task, so it is key that guidance be developed promptly to clarify the requirements in many areas where the text of the GDPR is unclear.

In our views, although speed is important, Article 29 WP Guidelines need to be prepared using effective industry consultation in order to ensure that they are properly designed and do not create unintended outcomes, even because the definition at EU level of some standards that can help controllers to put in place the modalities of implementing the portability or the interoperability of system could be appropriate.

Although events like the FabLab and the fact that Article 29 WP has sought comments on these guidelines are positive, they cannot replace proper public consultation, with a reasonable time period for written responses. Closed events with only restricted attendees and no ability to provide comments in writing, following due consideration, will not give Data Protection Authorities / regulators the same level of insight. We would therefore recommend for the future that the guidelines be published in draft with a reasonable period for response signalled well in advance.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.5 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Noémie Papp

Senior adviser Digital & Retail

n.papp@ebf.eu

+32 2 508 37 69