50

Dutch
Banking Association

[redacted]

To the members of Article 29 Working Party
Sent via e-mail:
JUST-ARTICLE29WP-SEC@ec.europa.eu
Presidence29@cnil.fr

Date 31 January 2017
Reference BR2589

Subject: Guidelines "Data portability"

To the members of Article 29 Working Party,

The Dutch Banking Association welcomes the guidelines published on the subject "Data portability" and would like to make use of the opportunity the Article 29 WP provides to send observations on this subject matter.

In this letter we expose our concerns and we propose a possible approach to achieve effective data portability in the banking industry. Our association would appreciate if a meeting could be arranged during which the following can be further clarified.

Data portability: a means to achieve free flow of data and strengthen the control of citizens over their own data
We understand that the aim of this right is to strengthen the control of citizens over their own data but it observes too that it also constitutes a step towards the free flow of data in Europe.

The banking sector also appreciates the advantages of this right for consumers: if consumer data is made "portable", consumers will be able to easily switch from service providers (free flow of data), and it will give them the feeling that they are more in control. The industry also sees the opportunities it represents for both the traditional banking sector as for new participants in the market.

The industry observes however that the article 29WP has chosen a broad interpretation of what "portable data" is. This broad interpretation goes beyond the wording used in article 20 of the GDPR. It does 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.

An underestimated risk: the dilution of data security and decrease of consumers' control of their financial data
Inasmuch as the industry sees the advantages of data portability, it sees this right as interpreted in the Guidelines nevertheless as a menace to what the GDPR is aiming at securing and enhancing: the privacy rights of citizens in Europe. In the coming paragraphs we explain why.

This right as further interpreted in the Guidelines will entail that citizens can easily download their sensitive financial data (transaction data, or data regarding their banking products, account information) into their often insufficiently safe devices and the obligation for financial institutions to

transfer it to other parties (other data controllers), which the banking industry considers a risk given the nature of financial data. Below we explain this further.

The sensitive nature of financial data
Financial data is perceived by the European citizens as well as the Dutch Data Protection Authority as very sensitive. These data can be easily misused for different forms of criminal abuse.

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 laying there unprotected, the use and abuse of such data can have far reaching consequences for citizens.

From the moment that it is well known that the industry will facilitate the downloading of sensitive financial data into often unprotected consumer devices (due to for example insufficient firewalls on their devices or as a consequence of developments such as the internet of things) or to unregulated parties who do not observe the same standards of protection, it is likely that criminals will seize this opportunity -without having to use the most advanced techniques- to easily access such computers and get their hands on 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 is likely to lead to a wave of cyberattacks to consumer devices.

Another threat is the use that other parties to which data will be made "portable" will make of such data. 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 malafide parties do not use it in accordance with the GDPR.

In addition, the risk exists that an unequal level playing field is created. Those who are not bound to the strict rules of the industry may use the data in different ways than those that will be considered acceptable in the financial industry.

Strengthening the control of the citizens' own data is also one of the objectives of this right. There seems to be an inexplicable paradox when portability relates to financial data. From the moment that the data can be easily made available to other parties, the control that the data subject can have on his financial data becomes more and more limited. It is likely that the citizen will lose the overview of which parties have his or her financial data.

The industry's existing mechanisms regarding switching payment accounts and the PSD2 obligation to disclose account information and the data portability of the GDPR
The industry understands that one of the aims of data portability under the GDPR is ensuring to promote consumer welfare by preventing so-called "lock-in-effects". "Lock-in" practices 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. In this regard we would like to point out that the banking industry has already dealt with this subject matter and is already bound to sector specific rules that aim at facilitating switching payment accounts. The rules to which the industry is already bound are to be found in the Directive 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (for the purposes of this note, the Switching accounts directive).

Moreover, the banking industry is preparing to abide by the principles of Second Payment Services Directive (PSD2). One of the novelties of this legislation that will apply as of January 2018 is that it introduces the portability of account information relating to payment accounts including transaction

information, to regulated parties. These are certified market participants, which are subject to the industry rules and regulations.

These obligations have similarities with the right to data portability enshrined in the GDPR.

The GDPR's data portability right is however not restricted to having to disclose financial personal data to regulated parties, but to any party addressed by the data subject to receive such information and to the data subject itself.

Parties receiving personal data on account of such specific banking rules will be bound by the strong industry standards, rules and regulations. In particular regarding the PDS2, in the views of the industry and the European legislator, this seems to mitigate the risk of the possible decrease of control of the financial data.

With respect to the PSD2 it should be noted that in its origins it aimed at a broader disclosure of client data in the context of the new services described in the PSD2. However in the end the risks of such broader disclosure made the EU legislator choose limiting the data that had to be disclosed to the providers of such new services to "just" payment account information with the consent of the client. The industry is preparing to ensure that such disclosure based on the consent of the client takes place safely.

Despite the above, the regulator AFM, consumer organisations, media and political parties in the Netherlands are however vividly expressing their concerns, especially regarding the decrease in overview of which parties will hold in the end sensitive client financial information as a result of PSD2.

These concerns will only increase when these parties realise that the portability of financial data under the GDPR ensures even less guarantees of protection. It is therefore only logical that the privacy concerns raised in the context of the PSD2 are also taken into account when considering the risks of the GDPR data portability in the financial sector.

Other practical consequences
No restrictions as to the amount of data that will be portable
This can result in practical problems for the consumer. If the consumer asks for all his transaction data, which could go years back if available, his or her device can collapse while receiving the data. Agreements should be reached as to how far in time a consumer may ask his bank to transfer his data to him or another party. The principle of proportionality should be observed.

Increase of legal claims against banks
Banks are expected to protect the data of clients using the most adequate standards. This follows from the general principle of due care and from sectoral laws. Citizens will expect that the data disclosed under the data portability right is safe also in their own devices and that is also safe in the hands of the third parties to whom the data is transferred. The possible expectation of citizens that banks would only allow transfers or disclosures "because it is safe" widens the expectation of due care that citizens have from the industry. In the meantime, the reality is that banks do not have control –nor should they be expected to have such control-on the third parties to whom data should be transferred when the client requests so.

If clients are hacked or third parties to whom clients requested banks to "transport" the data misuse it, the industry expects a wave of civil claims against the banks. Consumers may feel that it is the responsibility of banks to ensure that the data is at all times safe and secure. Also when the data reaches another party.

These claims will be of course unfounded: a) the banks when disclosing or transporting the data under article 20 GDPR or under the PSD2 are fulfilling a legal obligation and b) the responsibility of the banks ends at the moment that the data is received by the data subject or by the third party.

Nevertheless, responding to such court claims will entail high legal cost and a negative effect on the efforts undertaken to restore the trust of the citizens in the industry.

A proposed practical approach

1. GDPR compliance to data portability for the financial industry = PSD2 portability

Since the banking industry is already bound by the portability obligation set out in the PSD2, the industry proposes including a chapter in the guidelines explaining that due to the specific nature of financial information and the unpredictable consequences if data is misused, the data portability to third parties for the banking sector 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".

2. Agree to a maximum number of years of electronic portable data can be asked by the customers

It should be possible to agree to maximum of years back of available data to be transferred. This will ensure that the proportionality principle is observed, that there is less data available to possible mala fide parties if recipients receive and misuse such data and at least could partially mitigate the risk that the citizen's devices collapse due to the amount of data they request to be downloaded.

Also in this case, this limitation can be based on article 23 of the GDPR.

Legal base
Being able to rely on the exceptions of article 23 of the GDPR is justified on the grounds that the portability of financial data as stated above constitutes a risk for the data subjects. Moreover article 20.4 of the GDPR also states that "the right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others".

The proposed approach in this letter is made from the view point that being able to rely on the exceptions provided in the GDPR is possible: such approach does not entail a limitation of the privacy rights of individuals. On the contrary, the approach proposed here pursues a better protection of such rights.

Please let us know if you require further clarifications or examples.

Sincerely,

[redacted]

[redacted]
Dutch Banking Association