Nederlandse Vereniging van Banken

Datum 28 juli 2016
Referentie OD15800

NVB response to the European Banking Authority

Consultation form

Discussion Paper on innovative uses of consumer data by financial institutions

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions detailed below.

1. In what capacity (i.e. consumer, financial institution, technology providers, etc.) have you had experience with innovative uses of consumer data?

The Dutch Banking Association (Nederlandse Vereniging van Banken, in short NVB) represents the common interests of the Dutch banking sector. We would like to thank you for the opportunity to comment on this discussion paper, as published by EBA in May 2016. These comments should be seen as an addition to the comments made by the European Banking Federation (EBF), which we fully support. As stated by the EBF, the banking sector supports a competitive and innovative EU Digital Single Market which safeguards existing consumer protection, trust and security. To do so, the right competitive environment should be set and allow for an open and fair competition among the market players. Given this, it is important that the same rights and the same obligations apply to the same type of services across EU Member States.

All banks use consumer data, for example: to conclude contracts and agreements, develop products and services, for relationship management, to safeguard the security and integrity of the financial sector, and to comply with legal and regulatory requirements. Most banks rely on data which they acquire directly from their clients. Sometimes banks use external data – within the strict remits of the law - for example of credit agencies, information trade bureaus or publicly available sources such as the internet.

The NVB is of the opinion that the privacy rules and regulations (current and upcoming) already address the risks as described in the discussion paper and constitute a sufficient safeguard of the privacy rights of banking clients. We would like to elaborate on our position and indicate (outlined under question 8) how these risks are already mitigated by current and upcoming rules and regulations.
Dutch research MOB[1]*, shows that customers generally accept the use by banks of (payment) data as it is used to fulfill requirements by law and adherence to security issues (acceptance rate 80%), improvement of customer care and services (68%) and following trends (47%).

[1] November 2015 link: http://goo.gl/K55TK5 –in Dutch. This research was conducted by an independent research institute and was commissioned by the Dutch National Forum on the Payment System, which is chaired by Dutch Central Bank DNB.

Acceptance decreases if the use of data is further removed from these types of use and informed consent (opt-in) becomes more relevant to customers. 64 to 90% does not approve of use of (payment) data for commercial purposes by the bank or a third party without consent. The acceptance rate increases when customers can give their informed consent to this use to 55-76%.

In conclusion, if third parties get access to (payment) data, transparent and uniform information to customers and a level playing field are essential.

2. Based on your knowledge, what types of consumer data do financial institutions use most?

NVB adheres to the EBF position

3. Based on your knowledge, what sources of consumer data do financial institutions rely on most?

NVB adheres to the EBF position

4. Based on your knowledge, for what purposes do financial institutions use consumer data most?

NVB adheres to the EBF position

5. How do you picture the evolution of the use of consumer data by financial institutions in the upcoming years? How do you think this will affect the market?

NVB adheres to the EBF position

6. Do you consider the potential benefits described in this chapter to be complete and accurate? If not, what other benefits do you consider should be included?

NVB adheres to the EBF position

7**. Are you aware of any barriers that prevent financial institutions from using consumer data in a beneficial way? If so, what are these barriers?**

NVB adheres to EBF the position

8. Do you consider the potential risks described in this chapter to be complete and accurate? If not, what other risks do you consider should be included?

R1 Consumers experience detriment if they are unaware of the way financial institutions make use of their personal data

The processing of personal data is already subject to strict rules. Article 5.1 (a) GDPR mentions that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 6 of the GDPR states that the processing should be lawfully and provides the controller (banks) with 6 conditions (legal grounds) on which processing is allowed. For example in case the processing is necessary for compliance with a legal obligation. Without a legal ground as mentioned in article 6 GDPR, it is not allowed to process personal data. If a bank wants to reuse the

data for another purpose as collected, this new purpose has to be compatible with the purpose for which the personal data are initially collected.[2]

These are existing rules; they are also part of present regulation: Directive 95/46EU. Therefore the risk mentioned is mitigated by existing legal obligations and national privacy law.

Banks in the Netherlands have undertaken major steps to ensure all available information to their clients is available in clear and plain language as concluded by the Netherlands Authorities for the National Markets (AFM [3] The GDPR requires the information to be presented in clear and plain language[4]. The duty on transparency is further elaborated in the General Data Protection Regulation (GDPR),[5]; transparency (and modalities) are part of a chapter on the rights of data subjects.

R2 Consumers are "locked-in" by their current provider because their data is not assessable to other financial institutions

The banks in the Netherlands provide the possibility to their clients (both consumers and businesses) to use a jointly developed Bank Switch Service ("Overstapservice")[6] to migrate their payment traffic to a payment account held at another bank. The "Overstapservice" aims to facilitate account holders who want to move their payments relationship from one bank to another, thus increasing customer mobility. We would like to mention that Directive 2014/92/EU (Payment Account Directive) obliges Member States to implement a national payment account switching service as per 18 September 2016. Besides this, Article 20 of the GDPR introduces the 'Right to data portability'. Clients will have the right to receive the personal data provided to a controller and have the right to transmit those data to another controller without hindrance from the controller.

R3: Consumers experience detriment if financial institutions misuse their personal data

If a bank wants to reuse the data for another purpose as collected, this new purpose has to be compatible with the purpose for which the personal data are initially collected.[7] Article 5. 1 (a) GDPR mentions that Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 6 of the GDPR states that the processing should be lawfully and provides the controller (banks) with 6 conditions (legal grounds) on which processing is allowed. For example in case the processing is necessary for compliance with a legal obligation. Without a legal ground as mentioned in article 6 GDPR, it is not allowed to process personal data.

Banks are also bound by the Directive on privacy and electronic communications[8] which, among other things, provides for rules concerning the protection on data on the internet (cookies), the use of unsolicited communications for direct marketing purposes (especially on e-mails and SMS messages) and processing of location data giving the geographical location. In the Netherlands these obligations have been transposed in the Telecommunications Act. This means that financial

[2] Article 6 (4) GDPR
[3] AFM see https://www.afm.nl/nl-nl/nieuws/2014/mei/taal-klant
[4] Article 12 (1) GDPR
[5] Regulation EU 2016/679 articles 12-14
[6] With the "Overstapservice" all payments destined for the old personal current account are automatically re-routed to the new account during a period of 13 months.
[7] Article 6 (4) GDPR
[8] 2002/58/EC amended by 2009/136 EC

institutions are already under the obligation to abide these rules. The sanctions that can be imposed by the Authority for Consumers & Markets (ACM) are significant.

Under the current legislation and the GDPR, processing of client data for marketing purposes is allowed provided that this occurs within legal boundaries. For example, article 21 (2) GDPR gives data subjects the right to object in case their data is used for direct marketing purposes.

Financial institutions misusing data (for example by using client data for marketing purposes in a way that goes beyond the legal boundaries) undermine their reputation and potentially breach the law, which is and shall remain very strict on this point, including the possibility of a fine. The fact that at least two regulators in the Netherlands oversee the compliance of the use of data for commercial purposes constitutes a sufficient guarantee for clients to trust that banks shall not misuse their data for these purposes.

R4: Consumers experience detriment as a result of wrong decisions by financial institutions on the basis of wrong information

Clients of financial institutions have the right not to be subject to a decision relating to him or her which is based solely on automated processing and which produces legal effects or similarly affects, such as automated refusal of an online credit application[9]. Besides the data a financial institution processes has to be accurate and kept up to date.[10] The risk of wrong decisions on the basis of wrong information is mitigated by these principles.

Processing of health data or other special categories of personal data is also addressed in the GDPR. Processing of this data is prohibited except in strictly formulated cases. In case of automated decision making, including profiling, the GDPR states that the data subject shall not be subject to a decision solely based on automated processing including profiling. Especially it is not allowed to base a decision on special categories of data (e.g. health data) unless suitable measures to safeguard the data subject's right and freedoms and legitimate interests are in place[11].

R5: Consumers have restricted or no access to financial products or services because they do not allow for their information to be used by financial institutions

Practically and lawfully a bank is in need of access to certain information to be able to provide a product or service. Personal data that is being processed by banks needs to be processed because it is necessary to fulfill a contractual obligation or to abide the law. As mentioned before, banks have the obligation to process lawfully, fairly and in a transparent manner. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimalisation). [12] Banks will therefore only process the data necessary for the purposes as mentioned in the Introduction. In case a data subject doesn't want a bank to use his data commercially, it has the possibility to use his right to object to processing for direct marketing purposes. [13] That does not preclude a financial institution from processing for a legitimate purpose and still give access to financial products and services.

[9] Preamble 76 GDPR
[10] Article 5.1 (d)
[11] Article 22 (4) GDPR
[12] Article 5 GDPR
[13] Article 21 (3) GDPR

R6 Consumers suffer detriment if consumer data stored by financial institutions is obtained fraudulently by third parties

Financial institutions have the obligation to implement appropriate technical and organizational measures[14]. In case of a data breach, a financial institution will be obligated to notify the breach to the supervisory authority and the data subject.[15] Besides these obligations, banks in the Netherlands have specialized departments to prevent fraud and to comply to 3:17 Wft (Dutch Act on Financial Supervision) which amongst others stipulates that: 'A clearing institution, entity for risk acceptance, credit institution or insurer having its registered office in the Netherlands shall organize its operations in s*uch a way as to safeguard controlled and sound business operations*.'

R7: Financial institutions are exposed to reputational risk if they make questionable use of consumer data

As enumerated, banks are of the opinion that it is not allowed by law to use data in a questionable way. Since banks are bound by the GDPR and the Directive, we do not anticipate a reputational risks from this perspective in the Netherlands. However, if third parties would have access to payment data we could envisage potential reputational risks. As stated before, Dutch research shows that an explicit op- in/consent for use of (payment) data for commercial purposes is valued by consumers. Dutch banks are strongly in favor of creating broader support for the use of (payment) data, which can be achieved if authorities communicate to consumers in a transparent and uniform way regarding the rules that financial institutions (including third parties) have to abide to.

R8: Financial institutions that are not in a position to process consumer data cannot compete with new entrants in the market that specialize in using consumer data

New entrants to the markets may only process data if they take the GDPR into consideration. Financial Institutions do see a risk in the interpretation of new entrants in for example the re-use of data (further processing) and combining data that new entrants already possess/have access to in another role.

As long as financial institutions act in line with the GDPR and the Directive, it is allowed to use consumer data for commercial purposes. Preamble 47 of the GDPR states that 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.' The assumption – as stated in the discussion paper – that financial institutions may not use consumer data for commercial purposes seems to be a too strict interpretation of the applicable laws and regulations. Of course the consumer data may only be used commercially within the boundaries of the GDPR and the Directive.

Another risk regarding new entrants is Directive 2015/2366, Payment Service Directive II. New entrants and other institutions (so called 'Third Party Providers') can get access to the consumer (payment account-related) data held by account servicing PSP's (banks). Although they have to agree, data subjects may not always be aware of the fact that other institutions could process the data provided by banks. Although these other institutions also have to fulfill the obligations of the GDPR, the risk of non-compliance as well as uncertainty for the clients might increase.

[14] Article 24 and 25 GDPR
[15] Articles 33-34 GDPR

R9: Financial institutions are exposed to legal risks if their IT systems are compromised

As mentioned under R6 financial institutions have the obligation to take appropriate technical and organisational measures which are designed to implement data-protection principles, such as data minimalisation. Since financial institutions process sensitive and financial data, they already have sufficient measures in place to protect the data of their clients. New entrants might not always be aware of the existing rules and therefore they might not have these measures in place. So instead of new lawmaking more publicity should be given to the rules and regulations that are already in place.

Conclusion

According to the banking sector the risks as mentioned in the discussion paper of EBA are all addressed in the Directive and the GDPR. If a financial institution does not comply with the GDPR, fines can be imposed up to 4% of the worldwide annual turnover[16] of a financial institution. The GDPR also provides clients with the possibility to lodge a complaint to the supervisor and of course to the financial institution itself. Transparent and uniform communication to customers is deemed necessary, as well as a level playing field (same services, same risks) between all parties allowed access to (payment) data.

9. Have you observed any of these risks materialising? If so, please provide examples.

NVB adheres to the EBF position

[16] 83 GDPR