CHAIR
DATA PROTECTION
ON THE GROUND

in partnership with BNP PARIBAS FORTIS

Personal data protection in the financial sector

Round table report

November 2019

www.dataprotectionontheground.be

ABOUT THE CHAIR ON DATA PROTECTION ON THE GROUND

The VUB Chair "Data Protection On the Ground" (DPOG) promotes the investigation into actual practices of data privacy in organizations and the dissemination of best practices.

The focus of its research is on developments in smart cities, and the health, media, and financial sectors. To this end, the Chair compares practices in public sector organizations with those in the private sector, and organizations experienced in personal data protection with organizations that are making their first steps. In lectures, workshops, roundtables and other events, the Chair brings experts and practitioners together to stimulate the discussion of best practices.

The Chair is coordinated by the research center imec-SMIT (Studies on Media, Innovation & Technology) in collaboration with the research group LSTS (Law, Science Technology & Society), and supported by BNP Paribas Fortis. For more information, please visit the Chair's website at www.dataprotectionontheground.be.

ABOUT THIS REPORT

This report describes the results of a roundtable session in September 2019, that brought 13 representatives from different stakeholder groups together to discuss challenges and solutions for (personal) data protection in the financial sector. Participants had been provided beforehand with a policy brief, containing recommendations for policy makers. Under the Chatham House Rule, participants were free to bring in any topics related to personal data protection that they saw fit.

The analysis for this report was conducted by Ana Pop Stefanija and Ine van Zeeland, with support from Jonas Breuer, Laura Temmerman, Cora Van Leeuwen and Chantal Wauters; researchers at imec-SMIT, Vrije Universiteit Brussel.

REPRODUCTION

AUTHORS

Ine van Zeeland
Ana Pop Stefanija
Jo Pierson

For questions about this report, please contact Ine van Zeeland, ine.van.zeeland@vub.be.
For questions about the DPOG Chair, please contact dataprotectionontheground@vub.be.

Contents

1. Introduction

When the renewed Payment Services Directive (PSD2) came into law in the European Union in September 2019, questions of personal data protection in the financial sector came to the forefront of public debate once again. The roundtable organized by the VUB Chair on Data Protection On The Ground took place only four days after the implementation of PSD2, and it therefore came as no surprise that these issues were on every participant's lips. Early on in the roundtable discussion, a participant asked the question that struck at the heart of the issue: "Have the legislators for PSD2 and the GDPR talked to each other?"

Sharing more data with third parties, as is stimulated by PSD2, seems to run counter to the stringent data protection measures proposed by the GDPR. PSD2 relies heavily on explicit consent from the person whose payment data will be shared with third parties[1], but it is unclear whether 'explicit consent' means the same thing under PSD2 as it does under the GDPR, which has very strict provisions for the validity of consent. What is more, a major challenge in practice lies in assuring that individuals, but also banks, truly understand what exactly is consented to and what the consequences might be. As big data initiatives continue to be developed at a fast pace, it becomes difficult for all involved to foresee where data will end up and what may be done with it in the near future, particularly when it comes to profiling and scoring potential customers.

"How is this going to work in terms of confidentiality or trade secrets, even for the bank?"

Participant quotes

Participants also warned against further steps to remove access barriers to financial data, as recently suggested by the European Commission. The impression is that banks are not benefiting from 'open data' as much as other parties, while they do have to give up valuable assets. Participants also remarked that new entrants on the payment services market will seek to monetize the data they receive – otherwise, what would be their business model? And what if these new competitors can do a lot more with personal data than banks can, as they are not regulated in the same way? How can we make people more aware of the risks of improper use of their payments data?

This report will go into these main themes discussed during the roundtable:

- transparency and explainability of data processing practices,
- competitive pressures and regulatory imbalances,
- credit checks and rating.

The roundtable discussion also yielded insights that promise avenues for solutions to data protection challenges. Those avenues will be sketched at the end of this report.

2. Transparency and explainability

An issue that occupies the minds of a number of participants in the roundtable discussion is the 'transparency paradox', explained by one participant as "What is the level of transparency and consent that the client can really handle? What does the consumer want and when do you start to annoy them?" This issue is closely related to what is known as 'consent fatigue', the phenomenon that people click for agreement to any and all privacy-related requests without further consideration, because they

[1] Article 94(2) PSD2.

feel overwhelmed by the number of requests.[2] The GDPR principle of purpose specification – which entails that customers must be informed in detail of what their data will be used for – can lead to a consent fatigue effect when all possible purposes are presented to the customer for consent.

"We are supposed to provide transparent information, but not in 100 pages because that leads to transparency fatigue. What is the appropriate information? What is too much or not enough?"

Consent fatigue and related phenomena may lead some to believe that people just don't care about privacy, but it is at least also a matter of cognitive overload: people can impossibly read all the privacy notices and policies they are presented with. For that reason, consent requests and explanations will have to be concise. The practical question for the data controller is: What level of granularity do we have to reach in transparency?

One suggestion during the roundtable was that consent from the customer is not always needed; for instance, legitimate interests of a financial institution can also be a legal basis for processing personal data. However, this legal basis cannot be used for sharing payments data under PSD2, nor for situations in which decisions with significant effects on individuals are made in an automated manner – in both instances, consent from the individual will be needed. And even when consent is not needed, individuals will always have to be provided with information about the processing of their personal data. It is therefore important to separate the issue of providing sufficient information from the issue of obtaining valid consent[3] even if these issues often coincide.

Obtaining consent in a valid and proper manner is important to financial institutions for other reasons as well. Consumers are more sensitive about financial information than other types of personal data. One participant remarked that people tend to read information about their financial data three times. Trust is very important to banks, so 'softening' consent requirements to make it easier to process data will not work for banks in the long run.

"It is a question of ethics in the end. We have to have the trust of the clients, for the bank it is an asset."

Most people today cannot assess how their personal data are used by organizations or what the consequences of those uses are. When machine learning for artificial intelligence and automated decision-making becomes more common, explaining what happens with personal data will be all the more challenging, as even those in charge of processing the data will not understand exactly how the data are used.

Perhaps it will not be necessary to explain the intricate details of what happens with the data; we should consider what kind of information is useful. For example, potential clients for a loan will mostly want to know which factors are taken into account for the decision to grant or deny them that loan. Another consideration is the question of who needs to be able to understand the information provided: anyone, or independent experts (such as specialized advocacy groups) who verify algorithms

[2] Another related phenomenon has been labelled 'digital resignation', described by Draper & Turow in their 2019 article 'The Corporate Cultivation of Digital Resignation' as: "the condition produced when people desire to control the information digital entities have about them but feel unable to do so."
[3] For consent to be valid, the consenting individual needs to be 'informed'.

on behalf of the population? Information about data processing can also be layered, with an instant short explanation that offers click-throughs for more extensive explanations.

"If your algorithm decides to exclude someone from an insurance, how are you going to explain it?"

Transparency requirements can be a tool to inspire ethical behavior: if an organization has to be transparent about characteristics of people used in profiling, it will think twice about the relevance of certain characteristics. On the other hand, decision-making procedures and the data they are based on are the core business of the financial sector: in this market, having the right data and analyzing it in the right way are what gives financial organizations a competitive edge. Giving away too much about it can be detrimental. In addition, transparency cannot be provided in some specific instances, for example when it comes to fraud detection.

3. Competitive pressures and regulatory imbalances

While analyzing behavioral data for personalized offerings has become standard practice in online services, the financial sector is strictly regulated on this point. Some roundtable participants wondered how banks are to compete with a business such as Amazon, which also offers credit. Silicon Valley companies already have large and rich stores of personal data, yet if these players enter the financial market they may not have to comply with the same prohibitions. Clearly, when it comes to competition in the financial market, it makes little sense to regard the financial sector in isolation.

"You cannot talk about the financial services in isolation.
They feel the competition coming from other sides."

The trust issue mentioned in the previous section is also relevant in the context of competitive pressures. Had the GDPR not existed, banks would still have taken special care of their customers' data, because it is important to them to signal respect to their clients. New players in the financial market may not recognize the same imperative. People are familiar with such household names as Google and Microsoft, which they have already entrusted with a lot of their data, and they choose convenience over concerns about additional risks when sharing financial data as well. Several roundtable participants insisted that banks will cease to exist if they can or will not exploit their customers' data the way new competitors are doing.

Banks are regulated by a variety of legislation on a national and transnational level. As a consequence, there are strict lines of control ('four levels'), audits are a regular part of the banking business, and banks stand to lose their license if they do not comply with the laws. Banking representatives feel there is not a level playing field when competitors from other sectors enter their market, especially since enforcement seems to be lax for legislation that is not specific for the financial sector, like the GDPR.

Another complaint is that all the different regulations that affect the financial sector can be in conflict. As was mentioned in the introduction, data protection authorities may wish banks to restrict personal data sharing while competition authorities push for the opposite. It is often unclear to financial institutions which regulation has precedence. On top of that, interpretations of the same legislation may differ between authorities and the concept of 'privacy' is treated in different ways between

different regulations.[4] It was also noted that consumer protection authorities are more active and effective than data protection authorities. Roundtable participants therefore suggest more collaboration (or even merging) between supervisory authorities and integrated guidance for the financial sector.

"It is not safe to store an ID card, but you have to show that you are compliant to other regulations, and this is the proof."

Banks that operate across borders are also confronted with other regulatory requirements in different jurisdictions. For example, US regulations may be in conflict with EU regulations, and as fines in the former jurisdiction are higher, those requirements are often followed over the European legislation.

4. Credit checks and rating

One type of legislation that affects personal data processing in the financial sector are regulations for the detection of fraud and terrorist financing. These involve profiling. Profiling is not uncommon in the financial sector of course, as credit rating is mandatory and standard practice. The more data is available and the more accurate that data, the better profiling and credit rating will work. Legally, certain characteristics are not allowed as factors in those systems, such as gender and ethnicity, but there have been several cases published recently around profiling systems based on 'big data' machine learning in which other factors turned out to be proxies for those prohibited characteristics.[5] In April 2019, the Finnish Data Protection Ombudsman ordered financial credit company Svea Ekonomi to correct its creditworthiness assessment practices, stating that an upper age limit is not acceptable as a factor, since age does not describe solvency or willingness to pay.

"Targeting on the wrong criteria or targeting that ends up in a segment of one or two is really dangerous."

Profiling is a sensitive topic with respect to insurance. Consumer organizations warn against insurance exclusion of certain social groups. As insurance companies have more access to personal data of potential clients, they will be able to more accurately determine risk profiles. They may not be willing to offer insurance to cancer survivors or ask higher fees. In particular, legislation should prevent that insurance companies profile consumers on their willingness to pay higher fees or the likeliness that they will switch insurance providers. From a GDPR perspective, the problem is that profiles – inferences – may not be considered personal data, as they cannot be traced back to an individual, and so GDPR protections against automated decision-making with significant effects may not apply.

5. Other data protection challenges

Other challenges related to personal data protection that were briefly discussed during the roundtable were legacy IT systems, unexpected data sharing or re-use, and the lack of GDPR enforcement. Legacy IT systems were described as a problem, because it turned out to be impossible to completely retrofit

[4] For example, 'anonymous data' in financial regulations would not be considered anonymous under the GDPR.
[5] For example, postal codes and surnames can be strong indications of ethnicity.

systems with the introduction of the GDPR. Because various systems are linked, it is difficult to predict what may happen elsewhere when adaptations are made to one system. That this is not good IT design is readily acknowledged but it is already in place and it now leads to headaches.

Unexpected data sharing and re-use are concerns for customers. People fear what is unknown; if there is no intelligible information about what happens with their personal data, they assume the worst. One thing that is unclear is whether banks sell personal data to other parties; some banks apparently do. On the other hand, online retailers and social media services do this too, which may lead to changes in customer expectations. The flip side of the transparency coin is also that many consumers have low data literacy and are unaware of any risks when sharing personal data with an organization.

"I don't have a Facebook account, but I have a bank account."

Several roundtable participants showed disappointment over the scarcity of GDPR enforcement. Enforcements actions like fines offer a clear demarcation of acceptable practices, so even if no company wants to be the first one to be sanctioned, regulatory interventions are welcome as a general principle. There was a clear call for more data protection oversight of big technology companies.

"Enforcement is an important thing. I'm sure people are taking the GDPR less serious by the day. We need strong enforcement."

---

6. Possible solutions

Several solutions have already been discussed:

- Layer information and limit transparency to the information that makes practical sense to the target group.
- Rely on independent experts to verify algorithmic decision-making on behalf of the population rather than explaining everything to everyone.
- Raise awareness of data-related risks and promote data literacy among consumers.
- Collaborate between supervisory authorities and provide integrated guidance to the financial sector.
- Provide (legal) clarity on restrictions of characteristics that can be used in profiling and credit assessment.
- Enforce the GDPR with impressive sanctions.

Other solutions that were suggested during the roundtable were mostly centered on transparency. One suggestion was to identify financial customer journeys (e.g. buying a house, getting life insurance, etcetera) and the moments in these journeys where algorithms intervene, to explain which parameters are taken into account at those moments. Another suggestion was to develop templates for information provision on how data are used in different kinds of financial services. A third solution pointed to privacy by design: transparency should be built into assessment technologies.

Another topic that was much discussed during the roundtable was 'data ownership' for individuals. Legal scholars are cautious about the subject, as currently the law does not provide for data ownership and if we interpret data ownership along the traditional conceptualization of ownership, selling your personal data would entail that this personal data would no longer be yours. Proponents of data

ownership argue that it would empower consumers in their relationships with companies; at least they can receive something in return for the use of their data and they may be able to negotiate. This would, however, again require a marked improvement in people's data literacy. A second matter will be who has ownership over profiles, which are based on aggregated characteristics and a result of analytic treatment, rather than sourced directly from people.

7. Conclusion and recommendations

The solutions proposed in the roundtable are addressed at different stakeholders in the financial sector. Grouping them by addressee we can list the following recommendations:

Financial institutions

- As a sector, design specific, standardized templates for layered information about algorithmic decision-making with the aim to raise awareness of risks and improve data literacy.
- Focus on privacy by design and consider how much transparency can be built into new systems.
- Collaborate with advocacy groups on algorithmic auditing and information on data processing.

Lawmakers and policy makers

- Provide (legal) clarity on restrictions of characteristics that can be used in profiling and credit assessment.
- Consider merging supervisory authorities or facilitate closer collaboration between supervisors.
- Carefully consider data ownership.

Regulators

- Collaborate closely with supervisory authorities in other fields and provide integrated, sector-specific guidance.
- Facilitate the development of standardized templates for transparency.
- Enforce the GDPR with clear sanctions.

Advocacy groups

- Develop expertise in algorithmic auditing in collaboration with the financial sector.
- Provide input for (layered) data processing information and templates for transparency.
- Raise awareness of risks to personal data protection and promote data literacy.

Subsequent research

Based on the challenges and solutions highlighted in the roundtable discussion, subsequent research will be focused on developing 'financial information leaflets' for financial services that process personal data. These research efforts will be conducted within the framework of the research chair Data Protection On The Ground. The VUB Chair on Data Protection On The Ground will also gladly support stakeholder discussions for the development of templates for the sector.