POLICY BRIEF #29

16 September 2019

PSD2 and other challenges to the protection of personal data in the financial sector

Ine van Zeeland, Jo Pierson

This weekend, on 14 September 2019, the updated Payment Services Directive (PSD2) took effect in the European Union (EU). This will potentially have far-reaching consequences for the European financial sector. This policy brief particularly deals with aspects related to personal data protection, while also considering other current developments in the financial sector that affect the protection of personal data in the EU: law enforcement access to financial data, personalized banking services, and new entrants in the market, including moves by big technology companies. Our analysis is based on desk research and insights learned from conferences and workshops.

In addition, imec-SMIT is setting up a scoping study on the influence of cyber insurance on data protection practices that is of great relevance to the financial sector, as this sector is one of the main targets of hackers and consistently appears in the top 3 of sectors with most data breaches.

1. Data protection and payment services in EU law

Two recent pieces of European legislation have an impact on the use of personal data in the financial sector: The General Data Protection Regulation (GDPR)[1] and the updated Payment Services Directive (PSD2)[2]. Whereas the first regulates the protection of personal data and aims for accountability, the latter regulates payment services and service providers and aims for efficiency. Needless to say, the two sometimes interfere with one another, but both also make a point of consumer protection.

National legislation based on PSD2 should make it easier for European citizens to pay online and use innovative fintech services – if citizens consent to sharing their bank account data. In its implementation, the focus has been on promoting innovation and efficiency over security[3], though legislation differs between EU Member States. Studies have shown that bank clients are more sensitive to convenience than to risk (e.g. Clemes, 2012), prompting serious concerns among privacy and consumer advocates, as well as traditional banks, regarding reliance on client consent.

Payment data betray an astounding amount of people's personal lives: How much do they earn? What do they spend it on? How often do they overspend? Are they a member of a political party or church? How responsive are they to special offers? How often do they see a doctor or visit a sports school? Several of these categories of information are considered as sensitive in the GDPR, subject to stricter protection. While consent needs to be 'informed' to be valid in line with the GDPR, meaning an explanation must have been given about purposes

[1] Regulation (EU) 2016/679
[2] Directive (EU) 2015/2366, 'Open banking'
[3] See e.g. (in Dutch:) https://www.marketingfacts.nl/berichten/privacy-in-het-gedrang-door-psd2

and means of data processing (and several other aspects of the use of those data)[4], it remains to be seen whether an individual can foresee what the long-term consequences are.

Even if a person denies consent for sharing bank account data with a certain third party, that same third party may still have insight in some of this person's payments through the consent of others, such as relatives and friends, restaurants, delivery services, online retail, and so on. For instance, if an online shop collaborates with a payment service and a customer uses the service's payment method for their purchase, the payment service provider will know about it whether the customer has agreed to sharing financial data with that provider or not. Since some payment services are used by many online shops, a particular payment service provider may develop a substantial overview of this customer's buying habits.

Notwithstanding such concerns, traditional banks have also seen opportunities in the advent of PSD2. 'Open banking' does indeed promote innovation and lower costs for clients. Banks have set up their own fintech subsidiaries and are offering APIs and sandboxes for payment service providers to try out new services. By staying ahead of the pack and relying on superior consumer trust in their brands, forward-looking traditional banks are weathering the increased competition. As licenced banks have to commit to stringent oversight and high security standards, this development in traditional banking should be welcomed from a data protection perspective.

2. Law enforcement access to financial data

EU anti-money laundering and terrorism legislation imposes obligations on banks: they must apply measures to prevent money laundering and terrorist financing. These measures entail a type of profiling: certain types of transactions are flagged and used to create profiles of suspect behavior. What is important to note here is that these transactions are perfectly legal but may *potentially* be fraudulent or support terrorism. In addition, the e-Privacy Directive[5] allows Member States to adopt laws that restrict the protection of personal data and provide for the retention of data to safeguard national and public security, as well as for the prevention, investigation, detection and prosecution of criminal offences (among other purposes). Under certain conditions, national law enforcement authorities will request access to personal data that is retained for these purposes.

In GDPR terms, the legal basis for sharing these data with law enforcement authorities is not entirely clear and there are doubts about the proportionality of such 'pre-crime' measures. The question is whether banks are in a position to weigh these considerations, or even whether they should be in that position. The liability of banks for unauthorized sharing of personal data with authorities is also not clear yet, exposing banks to possible litigation. Meanwhile, further steps are taken by EU legislators to advance sharing more financial data for law enforcement and intelligence purposes, such as a fifth iteration of the Anti-Money Laundering Directive[6].

3. Using financial data for personalized services

Over the past years, many banks in the EU have been analyzing client data to find patterns, but they have often been reluctant to move forward into unprompted personalized offers, possibly fearing clients' discomfort with the realization that their transactions have been tracked. In July 2019, the Dutch Data Protection Authority took the initiative to explicitly warn banks against this use of financial data. They pointed out that people have no choice but to open a bank account in today's economy and can reasonably expect no other use of their transactions data than necessary for making payments. The situation is different, of course, when clients have explicitly agreed to personalized services, such as being offered travel

[4] Most conditions for consent can be found in article 7 of the GDPR. 'Consent' under PSD2 does not equate with 'consent' under the GDPR: the contractual consent needed under PSD2 does not suffice as valid consent to the processing of personal data under the GDPR. However, if there is a contract, personal data may be processed when it is necessary for the performance of the contract.
[5] Directive (EU) 2002/58 on privacy and electronic communications; discussion is still ongoing about its replacement by an e-Privacy Regulation, more in line with the GDPR and harmonizing legislation within the EU to a greater extent.
[6] Directive (EU) 2018/843

insurance after having made a transaction to a travel agency. In that case, the conditions for consent that were mentioned above apply.

Third parties who have received payments data under PSD2, however, will probably want to monetize on those data by offering personalized services. Fintech apps generally provide advice on spending or saving, with some even offering discounts on services of other companies. If clients become more used to this type of service, this would change 'reasonable expectations' and the threshold will be lower for traditional banks to personalize as well.

4. New entrants in the financial markets

While fintech companies are still relatively new and come nowhere near the sizable customer bases of traditional banks, the latter do fear other new market entrants: big technology companies. Big tech companies like Amazon, Facebook, Google, and Apple do have large customer bases and powerful brands, as well as advanced tools for analysis of customer data, including extensive behavioural data that banks still lack. Big tech platforms will also be able to cross-subsidize banking services with profits obtained from other services, like e-commerce or advertising.

In China, this transformation has already happened. Payment app Alipay was launched in 2004 by e-commerce site Alibaba/Taobao and spun off in 2011. Renamed Ant Financial in 2014, it has become one of the world's biggest financial companies, offering payments, wealth management, lending, insurance, and credit scoring.

Silicon Valley platforms are now making similar movements, again starting with payments. In March 2019, Apple announced the introduction of a virtual credit card, the Apple Card, to be used in combination with Apple Pay. In June 2019, Amazon introduced Amazon Credit Builder, basically a rewards credit card for people with bad credit.[7] Also in June, Facebook announced Libra, a digital currency project that instantly drew fire from American and European regulators and lawmakers.[8]

Given big tech's business models, that are centred around the monetization of personal data by way of advertising and manipulation, there are reasons for concern. Big platforms may be less interested in offering trustworthy banking services than in obtaining financial data. From a principled data protection point of view, the accumulation of personal data in the hands of a few large entities reduces choice and autonomy for individuals and induces total surveillance.

5. Data breaches and cyber insurance

While some organizations still try to keep data breaches under wraps, there has been more openness about breaches in recent years, partly due to stricter notification requirements under such legislation as the GDPR and the Basel II accord for financial services companies. One of the major reviews of the annual costs of data breaches is the NetDiligence Cyber Claims study[9], which over the years has consistently shown that the financial industry is among the hardest hit by data breaches. Not only are financial services companies among the primary targets for hackers, insider threats are also a major concern.[10]

Even with optimal security for data and infrastructure there will always remain residual risks. This is why cyber insurance is on the rise. As for other insurance products, cyber insurance premiums can vary based on the provider's assessment of the insured party's risk profile and

[7] Amazon has also introduced a lending referral programme in China, as part of its Amazon Lending service.

[8] See e.g. https://edps.europa.eu/sites/edp/files/publication/19-08-05_libra-network-joint-statement_en.pdf

[9] https://netdiligence.com/portfolio/cyber-claims-study/

[10] A recent example that has attracted a lot of media attention was the breach of the American bank Capital One in August 2019. See e.g. https://www.wsj.com/articles/capital-one-cyber-staff-raised-concerns-before-hack-11565906781.

protective measures. For example, some insurance companies have cyber insurance policies that are specifically tailored for financial service organizations, considering the specific risks to data protection that this sector faces. As a consequence, organizations that are interested in taking out cyber insurance will review their practices and may be faced by protection requirements from insurers.

Imec-SMIT is currently setting up a scoping study on the influence of cyber insurance on data protection practices within organizations, reviewing organizations' motivations to choose cyber insurance, contractual obligations, and factors in premium calculations, among other aspects. Any organizations interested in participating in the study can express their interest or ask questions to researcher Ine van Zeeland, ine.vanzeeland@smitresearch.be.

6. Conclusion and recommendations

Though the GDPR does not specifically designate financial data as sensitive data, there is no doubt that financial information can be very revealing of a person's private life, predilections and affiliations. This allows for extensive profiling and possible manipulation. The history of banking shows a keen understanding of these facts on the part of financial institutions. Such awareness may be less of a concern for fintech start-ups. A major challenge post-PSD2 is to impress the possible risks of sharing financial data upon banking clients. Strict consent requirements that include the provision of information on data recipients, processing activities and possible consequences, mean little when enforcement is scarce and dependent on the acuity of individual data subjects.

Relevant supervisory authorities, such as Data Protection Authorities, need to enhance their capacities to be vigilant of financial data sharing. The warning provided by the Dutch Data Protection Authority presents an example that deserves following in other EU Member States.

A special concern for European policy makers should be the lack of clarity on financial institutions' responsibilities and liabilities regarding the sharing of personal data with law enforcement authorities. New legislation in this area should principally provide more clarity.

Amid worldwide calls for stricter regulation of big technology firms and a growing number of investigations into market imbalances and possible effects on competition, it comes as no surprise that lawmakers show suspicion of the major platforms' moves into payments services. The announcement of an examination of Facebook's Libra project by European Commissioner Vestager on 4 September 2019 can therefore only be commended.

Ine van Zeeland is a PhD researcher within the VUB research chair on Data Protection On The Ground.

Jo Pierson is in charge of the research unit 'Data, Privacy & Empowerment' at SMIT and associate professor in the Department of Media and Communication Studies at the Vrije Universiteit Brussel. He holds the VUB research chair on Data Protection On The Ground.

The VUB research chair on Data Protection On The Ground 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 four sectors: smart cities, health, media, and banking. The Chair is coordinated by the research center imec-SMIT in collaboration with the research group LSTS (Law, Science Technology & Society), and supported by BNP Paribas Fortis. For more: www.dataprotectionontheground.be.

Imec-SMIT (Studies in Media, Innovation and Technology) is an imec research group at Vrije Universiteit Brussel. Our research is clustered within two main programmes: Media & Society and Data & Society.

For questions about this policy brief, please contact Ine van Zeeland, ine.vanzeeland@smitresearch.be