



PSD 2, open banking and the value of personal data

June 28, 2018

Author
Heike Mai
+49 69 910-31444
heike.mai@db.com

Editor
Jan Schildbach

Deutsche Bank AG
Deutsche Bank Research
Frankfurt am Main
Germany
E-mail: marketing.dbr@db.com
Fax: +49 69 910-31877

www.dbresearch.com

DB Research Management
Stefan Schneider

- With the new Payment Services Directive ("PSD 2") of the EU, which entered into force on 13 January 2018, payment services in Europe have become the frontrunner of "open banking". Account holders can request, free of charge, that banks transmit their financial data in digital form to third parties. Furthermore, they can authorise third-party providers to initiate payments from their bank account.
- Personal data are owned by the data subject – this principle also forms the basis of the new General Data Protection Regulation (GDPR). Under the latter, however, there is no obligation to provide a technical solution through which customers can transmit their personal data to third-party providers in a convenient manner. In contrast to the PSD 2, the GDPR is therefore unlikely to stimulate innovation and competition in payments.
- In the financial sector, competition will thus be distorted. Banks must grant competitors access to customer data and their payment infrastructure, whereas internet platforms, for instance, de facto retain sovereignty over the personal data of their customers as well as access to their platforms.

PSD 2 grants third-party providers access to accounts

By breaking up the entity of customer account, account information and payment initiation, the regulation aims to bring more competition and innovation into the payment services market. In this context, three new provisions are of essence:

- Upon request of the customer, an account servicing institution (i.e. banks, as a rule) must grant a third-party provider access to the respective account to retrieve account information or initiate payments. This holds only for accounts that a customer has enabled for online banking.
- The account servicing institutions must put in place open technical interfaces to provide entitled third-party providers with easy-to-use digital access to accounts.
- Access to the customer's account, the account data and the internal payment infrastructure of the servicing institution must be granted free-of-charge.



PSD 2, open banking and the value of personal data

Moreover, the revised Directive¹ aims to further enhance the high security standards in payment transactions, balancing security and consumer protection against innovation and user friendliness. The key requirements are as follows:

- Strong customer authentication²:
 - i. Every time a customer logs into his account, he has to provide at least two of three independent factors to prove his identity.³ These are factors that only he knows (e.g. password), something that only he possesses (e.g. mobile phone) or that he is (e.g. fingerprint).
 - ii. When the customer initiates an electronic payment, dynamic linking to attributes of the transaction is mandatory. For instance, the account servicing institution could send the customer a TAN by text message to verify the amount and the beneficiary of the payment. By entering that TAN, the payment is authorised.
- The reduction of potential risks for account holders using third-party providers:
 - i. Technical: Only third-party providers who are licensed by the financial supervisory authority will be granted access to the account, after having provided an electronic certificate for identification to the bank, and only upon order by the customer. Such assignment is considered issued when the customer logs into the third-party provider by means of the strong customer authentication and, in case of a payment, when he authorises the transaction in the above manner.
 - ii. Legal: The account servicing institution shall be liable for losses relating to defective execution or fraud against customers, even if the respective customer has operated his account via a third-party provider. If the latter has caused the fault, the bank can demand compensation from that provider for the losses incurred.

Bank customers can hence use non-bank services with a direct technical link to their account in a convenient and secure manner. For now, the PSD 2 exclusively demands and regulates account access for so-called payment initiation services (PIS) and account information services (AIS). But as the Directive opens up personal account data, a flurry of further innovative services will likely be brought to market, including areas such as real estate and consumer loans, investment advice or securities services. In cases where the use of account data goes beyond the scope of the PSD 2, the processing of personal data is controlled by the General Data Protection Regulation (GDPR)⁴, which went live on 25 May 2018.

¹ "Payment Services Directive 2 (PSD 2)": Directive (EU) 2015/2366 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. Of the comprehensive payment services provisions outlined in the PSD 2, this article discusses only the introduction of third-party providers' access to customer accounts.

² For an introduction to the PSD 2 provisions on strong customer authentication as well as possible exemptions, see for instance Deutsche Bundesbank, Monthly Report April 2018, p. 53 ff.

³ Authentication is the process of proving one's identity online by means of a password (or the like) to a provider, who then verifies the identity of the user on the basis of the password (or the like) and internal procedures. In short, it is verified whether the user really is who he claims to be.

⁴ "General Data Protection Regulation (GDPR)": Regulation (EU) 2016/679 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.



Final hurdles to PSD 2 implementation

What is a ...

1

Payment initiation service (PIS)

Examples:

- A payment service which is integrated into the website of an online merchant, providing the customer with the option to initiate a transfer from his bank account without being redirected to the online banking interface of his bank. The merchant benefits, firstly because the purchasing process becomes more convenient for the customer and secondly because a confirmation is sent to him immediately after payment. In Germany, the most popular provider so far is Sofort GmbH ("Sofortüberweisung"), an affiliate of Swedish Klarna Bank.
- A retailer which has obtained a payment initiation service license, in order to enable clients to initiate the payments for their purchases directly from their bank accounts without an intermediary service provider.

Account information service (AIS)

- An app which provides an aggregated overview of the accounts a customer holds at different banks.

Source: Deutsche Bank Research

Currently, several stumbling blocks still stand in the way of PSD 2 implementation. Although provision of technical access to accounts becomes mandatory and fundamental technical requirements for this access have been defined by the legislators, the concrete design of an operable interface is in the hands of the individual account servicing institutions. Ideally, a single interface standard would be established throughout the market, allowing third-party providers to connect to accounts at all banks with the least possible effort. Several interoperable interfaces would be another, albeit suboptimal, option. Indeed, several groups of banks or different market participants have been established in Europe with the objective of defining standards which can be used on a voluntary basis.⁵ Whilst a patchwork of interfaces is unlikely to emerge, it remains to be seen whether technical standardisation across different institutions and national markets will de facto be achieved. Political pressure to introduce interoperable standards, at minimum, is high, though. Should voluntary implementation fall behind the expectations of the EU legislators, preventing more competition and more innovation through market fragmentation, standardisation by regulation cannot be ruled out.

From a legal perspective, there are also a number of questions, primarily with respect to the delay of national transposition. The PSD 2 will not become effective unless it is transposed into national law by the member states. To date, however, only 17 EU countries, including Germany, France, Italy and the UK, have done so.⁶ Moreover, several accompanying guidelines and regulatory technical standards, which need to be specified by the European Banking Authority (EBA) and approved by the EU, have not yet been adopted in a legally binding form.⁷ Against this backdrop, it seems highly unlikely that the PSD 2, including all acts that were delegated to the EBA, will become fully effective throughout Europe before year-end 2019. Furthermore, national supervisory authorities are entitled to refuse compliance with some aspects of the EBA's provisions, or to modify them. Major efforts will hence be required to ensure that providers and customers throughout Europe can take advantage of the PSD 2 and use it as a catalyst towards open banking for financial services beyond payments.

Open banking

The PSD 2 paves the way for "open banking", a banking market in which the customer is granted the right to transmit his data in digital form and can easily use the online services of different (non-bank) providers that can access the data they need through open interfaces put in place by the banks. Via these interfaces – which are known under the term API (application programming interfaces) – companies allow third parties to connect their own services. APIs are a core element of every digital platform which embeds third-party providers to set up an internet ecosystem.

As a consequence, open banking is also referred to as API banking. It is noteworthy that under the PSD 2 account servicing banks have no say in whether, and to whom, they provide interfaces to their infrastructure. Provided

⁵ E.g. Berlin Group (participants from many European countries, including Germany, France, Italy, Spain, Poland), STET (France), PolishAPI (Poland), Open Banking (UK).

⁶ For a list of countries which have fully transposed the PSD 2 into national law, see https://ec.europa.eu/info/publications/payment-services-directive-transposition-status_en

⁷ For a list of accompanying guidelines and regulatory technical standards, see <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/-/activity-list/MgjX6aveT17v/more>



PSD 2, open banking and the value of personal data

the third-party provider is licensed by the supervisory authority and authorised by the customer, the bank has to grant access.

How will the PSD 2 affect the supply side? Of course, the beneficiaries will be the new financial service providers such as FinTechs or other software suppliers, who can now seamlessly attach their innovative services to the existing (banking) infrastructure. For BigTechs and retailers with a large customer base, the free-of-charge technical interfaces also open up new opportunities with respect to payment services, retail financing or other tailored products. But – somewhat surprisingly, perhaps – individual banks can also benefit. They, too, can act as third-party providers vis-à-vis other account servicing banks and offer an array of new or extended services to their customers, which will intensify competition among all providers.

At the same time, banks can more easily cooperate with FinTechs, courtesy of the PSD 2. If third-party providers are supervised by the authorities, banks will have to clear fewer regulatory hurdles when cooperating with FinTechs.

Only effective data portability creates customer value

The starting point for the repositioning of traditional and new financial service providers is the customer's right to access the personal data stored by a company and transmit them to third parties. Although the PSD 2 and the GDPR both breathe this spirit, there is an essential difference between the two acts. The PSD 2 aims at the portability of data to strengthen competition. To this end, the account servicing institution is obliged to take appropriate technical measures to ensure its customers can exercise their legal right of data sovereignty. As personal data from the bank account can hence be transmitted easily by the data subject, they become an economic value. The GDPR, on the other hand, focuses on protecting the personal data of a data subject.⁸ Here, the right to transmit personal data to third parties has to be seen as a mere extension of the right to obtain information from a data controller as to whether personal data concerning oneself are being stored and processed.

Whilst the GDPR also acknowledges and endorses that data portability will foster competition, as a desired "side effect" so to speak⁹, provisions with respect to the implementation of data portability are lacking. Providing only recommendations, the GDPR, unlike the PSD 2, does not oblige data controllers to achieve technical operationalisation of the right to direct transmission of personal data to third parties. Thus, data shall be transmitted directly from one company to another upon request of the customer only where it is "technically feasible". The development of interoperable formats is only recommended, an obligation to adopt or maintain processing systems which are technically compatible is explicitly ruled out. Going forward, customers will therefore continue to have practically no opportunity to transmit their personal data from one company to another, possibly competing one in a convenient, digital and smooth manner. The data subject will de facto reap no economic value of the legally granted right to control his personal data.¹⁰

⁸ Under the GDPR, personal data are defined as "any information relating to an identified or identifiable natural person (...); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

⁹ European Commission, Article 29 Data Protection Working Party, Guidelines on the right to data portability (WP 242 rev.01), revised and adopted on 5 April 2017.

¹⁰ See also Körner, Kevin (2018). GDPR – boosting or choking Europe's data economy? Talking Point. Deutsche Bank Research.



PSD 2 and GDPR will distort competition

As a consequence, the lock-in effect for customers of companies with a data-driven business model will not be broken up. The customers will only be put in control of their personal data at banks, to use them to their own advantage. They neither benefit from more competition between internet platforms nor from comprehensive competition in open banking. Data silos in the non-bank sector will not be broken up.

Competition will hence be distorted. With the entry into force of all accompanying guidelines and the regulatory technical standards, banks will be subject to the operationalised PSD 2, obliging them to provide customer data to all licensed competitors, in digital form and free-of-charge. BigTechs, on the other hand, have to observe the GDPR only and will de facto retain economic sovereignty over the personal data of their customers.

A level playing field for all potential providers is lacking not only in the area of data portability, though. Whilst account servicing institutions have to provide free-of-charge digital access to the banking payment system, non-bank providers retain ownership of their technical interfaces for third parties: It is up to them to decide who may use their interfaces and, as a consequence, their platform, and how. As a result, a platform operator can, for instance, prevent competition between third-party providers and an in-house payment service. Without open access to the infrastructure à la PSD 2, the only tedious alternative left is competition law. Ensuring a level playing field for all providers, however, is essential to exploit the full potential of open banking for competition, innovation and customer value. The GDPR, which is aimed at data protection, is no suitable tool in this respect; further efforts need to be made. A recent proposal of the EU Commission to promote fairness and transparency for business users of online platforms is a move in the right direction¹¹, though it is not aimed at open banking.

Data economy opens up new horizons

The question as to who owns what data cannot be answered once and for all: Although some headway has been made, the use of digital data for the development of new technologies, business models and markets is still at an infant stage.

Today, many internet-based companies provide their services free-of-charge and in exchange commercialise the data they collect on their users. In future, however, the data subjects might become increasingly aware of the value of their personal data, and use them accordingly. In fact, a monetary price could emerge for the personal digital dataset, provided it becomes generally transferable and tradable. Similar to a custodian bank, new providers could securely store the datasets for the data subjects and, upon request, transmit them to third-parties against payment.

The evolution of artificial intelligence will intensify controversy about how digital data should be handled, as these budding processes rely on access to large datasets. If data controllers – companies, authorities, research institutions, etc. – face restrictions when using personal data, the development of AI-based products can be hampered, putting the economy at a disadvantage vis-à-vis its competitors. But – as consumers become increasingly privacy-sensitive – it

¹¹ European Commission (2018). Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, Brussels.



PSD 2, open banking and the value of personal data

could also prove to be a competitive advantage, provided strong models for the protection of personal data are developed.

Alongside the economic value of personal data, the public position with respect to privacy protection is of particular interest. The view on data protection can change: Whilst a population census in the 1980s still sparked a heated debate about the protection of data in Germany, personal data are shared generously and often without hesitation in the internet era. It is likely, though far from certain, that this will continue. Not only economic incentives (e.g. use of data against payment) could leave their mark on the behavior of consumers. Also, it will matter if there is popular confidence that data-collecting companies and governments will comply with the rule of law and democratic principles. After all, people are citizens, clients and data subjects at the same time.

Heike Mai (+49 69 910-31444, heike.mai@db.com)

© Copyright 2018. Deutsche Bank AG, Deutsche Bank Research, 60262 Frankfurt am Main, Germany. All rights reserved. When quoting please cite "Deutsche Bank Research".

The above information does not constitute the provision of investment, legal or tax advice. Any views expressed reflect the current views of the author, which do not necessarily correspond to the opinions of Deutsche Bank AG or its affiliates. Opinions expressed may change without notice. Opinions expressed may differ from views set out in other documents, including research, published by Deutsche Bank. The above information is provided for informational purposes only and without any obligation, whether contractual or otherwise. No warranty or representation is made as to the correctness, completeness and accuracy of the information given or the assessments made.

In Germany this information is approved and/or communicated by Deutsche Bank AG Frankfurt, licensed to carry on banking business and to provide financial services under the supervision of the European Central Bank (ECB) and the German Federal Financial Supervisory Authority (BaFin). In the United Kingdom this information is approved and/or communicated by Deutsche Bank AG, London Branch, a member of the London Stock Exchange, authorized by UK's Prudential Regulation Authority (PRA) and subject to limited regulation by the UK's Financial Conduct Authority (FCA) (under number 150018) and by the PRA. This information is distributed in Hong Kong by Deutsche Bank AG, Hong Kong Branch, in Korea by Deutsche Securities Korea Co. and in Singapore by Deutsche Bank AG, Singapore Branch. In Japan this information is approved and/or distributed by Deutsche Securities Inc. In Australia, retail clients should obtain a copy of a Product Disclosure Statement (PDS) relating to any financial product referred to in this report and consider the PDS before making any decision about whether to acquire the product.

ISSN (Online): 1612-0280