Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Banking Regulation 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Austria: Trends & Developments

Jasna Zwitter-Tehovnik and Anže Molan
DLA Piper

practiceguides.chambers.com

Trends and Developments

Contributed by:
Jasna Zwitter-Tehovnik and Anže Molan
DLA Piper **see p.8**

Current Developments in Open Banking From the EU and Austrian Law Perspective

Introduction

In the last couple of years, the bank-centric financial market has been increasingly faced with challenges related to the spectrum of choices that can be provided to customers as well as the development of new financial products and services based on the technologies which are gaining in popularity. One of the most important (and often described as revolutionary) trends is "open banking", a banking practice that enables third-party financial services providers access to several types of data kept by banks and other financial institutions, thereby transforming the existing bank-centric financial system and, most importantly, introducing innovation and competition into the financial services sector.

Simultaneously, the (supra)national legislators and regulators have been – considering several developments that have taken place on the market – presented with new legal issues that needed to be addressed. In the context of the open banking phenomenon, these issues include, among others, defining the appropriate and sufficient regulatory response as well as concerns related to regulation of data being shared in this respect. This paper will focus on the latter aspect, namely the question of how to regulate increased data sharing while maintaining high standards of privacy and data protection as well as ensuring a level playing field between different financial services providers (including banks and fintech providers).

The key EU measure in this respect was the introduction of the Directive (EU) 2015/2366 of the European Parliament and of the Council 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 (PSD 2) which entered into force on 12 January 2016 and started to apply on 13 January 2018. EU member states, including Austria, have transposed the PSD 2 into national legislation to establish a functioning legal framework for payment services providers as well as general rules applicable to the financial services sector as a whole.

Despite the successful implementation of the PSD 2 and its provisions, the new legal challenges combined with the new technologies that have emerged require amendment of the current legal rules. In particular, one of the main issues is the interaction of financial services rules on open banking (including PSD 2) with personal data protection and privacy law which will be discussed below.

What is open banking?

Open banking is an emerging banking practice with the purpose of providing third-party financial services providers "open access" to various types of data on consumers as well as other financial data kept by either banks or other financial institutions. In principle, the open access to such data is provided using the so-called application programming interfaces (APIs).

Open banking therefore breaks the concentration of information in traditional banks and increases networking of multiple accounts as well as data across the financial services sector merged between old and new service providers (see, for instance, F. Ferretti, *Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR*, 1 European Review of Private Law 2022, 30, pages 73–102). As will be discussed in more detail below, this enables new products and services to enter the fintech market, which leads to a better overall customer experience.

Under the PSD 2 regime there are, broadly speaking, two different types of entity that are regulated and considered as third-party providers in the above sense, namely:

- account information service providers (AISP), and
- payment initiation service providers (PISP).

The aim of the AISP and their respective services is to provide a payment services user with an overall view of its financial situation immediately at any given moment (see, for instance, Recital 28 of PSD 2). Payment initiation services, on the other hand, enable the PISP to provide comfort to a payee that the payment has been initiated to provide an incentive to the payee to release the goods or to deliver the service without undue delay (ie, a low-cost solution for both merchants and consumers that provide the latter with a possibility to shop online even without possessing payment cards – see, for instance, Recital 29 of PSD 2). It should be noted that both types of third-party providers described above must be licensed and need to comply with the legal requirements laid down in PSD 2.

Legal framework – status quo

The key legal act on the EU level is PSD 2 which forms the cornerstone of EU legislation on open banking. As a successor of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, which was largely limited to the regulation of payment services and information requirements for payment services providers, PSD 2 tackles broader issues. This includes, among other things, opening up payment markets to new entrants as well as furthering the level playing field for payment services providers, leading to more (fair) competition, greater choice and better prices for consumers. In this context, PSD 2 pertains to companies offering consumer-oriented or business-oriented payment services which are based on access to the payment account and differentiates between account information services on the one hand (provided by AISP) and payment initiation services on the other (provided by PISP) – ie, both licensable payment services, pursuant to Nos 7 and 8 of Annex 1 to PSD 2.

In Austria, PSD 2 has been transposed, among other acts, into the Austrian Payment Services Act (ZaDiG 2018).

Key provisions of PSD 2/ZaDiG 2018 relating to open banking aspects relevant to this paper are

- Article 66 of PSD 2 (which has been transposed into Section 60 of ZaDiG 2018 with, in principle, no notable derogations) in relation to payment initiation services (*Zahlungsauslösedienste*); and
- Article 67 of PSD 2 (which has been transposed into Section 61 of ZaDiG also with, in principle, no notable derogations) in relation

to account information services (*Kontoinformationsdienste*).

Apart from the regulation pertaining to payment services as such, open banking is subject to several other regulatory realms including EU electronic verification rules, cybersecurity legislation, the most recently adopted EU digital finance package, and, finally, privacy and personal data protection legislation.

Amending proposals for the existing legal framework

Following the European Commission's Call for Advice on the review of the PSD 2 in 2021, the European Banking Authority (EBA) published, on 23 June 2022, an Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) (the "EBA Opinion"). In the comprehensive EBA Opinion, the EBA's amending proposals touch upon several aspects with the aim of contributing to the development of a single EU retail payments market as well as ensuring a harmonised and consistent application of the legal requirements across the EU. As a side note it is worth mentioning that even though discussions are currently taking place on the EU level, the amendment of the PSD 2 regime will result in amendments of the EU member states' national payment services regimes (including ZaDiG 2018 in Austria).

One of the EBA's proposals aims at protecting consumers' data, more particularly, access to and use of payment accounts data in relation to account information services and payment initiation services (ie, also a special section of the European Commission's Call for Advice). On several occasions, the EBA Opinion mentions the problem of interplay between PSD2 and Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (GDPR). According to the EBA, legal uncertainty of interplay between PSD 2 and the GDPR pertains especially to the following aspects (as outlined on pages 113 et seq of the EBA Opinion).

- The implementation of the data minimisation requirements under the GDPR into the design of the interfaces that account servicing payment services provider are required to provide under PSD2.
- The processing of special categories of personal data, and in particular whether the processing of payment transaction data is subject to the requirements in Article 9 of the GDPR (whereby it shall be borne in mind that such an interpretation could have far-reaching effects on the processing of all payment transactions and on the financial system).
- The legal ground for processing of the so-called "silent party" (defined by the European Data Protection Board (EDPB)) as personal data pertaining to a data subject who is not the user of a specific payment services provider, but whose personal data is being processed by that specific payment services provider for the performance of a contract between the provider and the payment services user; see EDPB: Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR as of 15 December 2020 (the "EDPB Guidelines").
- The compatibility of the GDPR principle of data minimisation with "screen scraping" techniques.
- The possibility for third-party providers to share with account servicing payment services providers data such as the payment

services user's location, IP-address, and other device data.

Further to the above aspects, additional problems of interplay between PSD 2 and other legal acts regulating the processing of personal data may arise also in light of the specific requirements stemming from national legal regimes. In Austria, the most important national law in this area is the strict banking secrecy legislation which may affect the data protection regime under PSD 2.

Lawfulness of processing of the customer's data by third-party providers

One of the main issues deriving from the interplay between PSD 2 and the GDPR is the nature of the legal bases for processing customers' data. Although the EDPB Guide has provided a certain level of clarity in this respect, both the EBA and EDPB recognised that explicit consent under Article 94 (2) of PSD2 shall be differentiated from (explicit) consent under the GDPR leaving several aspects of the issue at hand unclear to a certain extent.

Consent under the GDPR

Under the GDPR, controllers that wish to process personal data must have a legal basis. Article 6(1) of the GDPR represents an exhaustive and restrictive list of legal bases for processing of personal data under the GDPR regime which includes, among others, consent (Article 6(1)(a), GDPR).

Consent of the data subject under the GDPR regime (as defined in Article 4(11), GDPR which reflects Recital 32 thereof) shall be understood as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Apart from other safeguards stemming from, for instance, Articles 7 and 9 of the GDPR, it shall also be mentioned that consent can under no circumstances be inferred from potentially ambiguous statements or actions. In addition, consent cannot be obtained through, for example, agreeing to a contract or accepting general terms and conditions (see page 13 of the EDPB Guidelines).

Despite national legal rules pertaining to consent in the context of processing of personal data (in particular, the Austrian Data Protection Act (*Datenschutzgesetz* – DSG)), the GDPR regime constitutes a comprehensive regulation of consent which means that the DSG provisions are in this respect, generally speaking, of no relevance.

Explicit consent under PSD 2/ZaDiG 2018

According to Article 94 (2) of PSD 2, payment services providers shall only access, process, and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment services user.

Although similar in nature, explicit consent under PSD 2 shall be differentiated from (explicit) consent under the GDPR regime, according to the EDPB Guidelines. Namely, the EDPB explicitly rejected the notion that Article 94 (2) of PSD 2 shall be regarded as an additional legal basis for processing of personal data. Accordingly, the explicit consent requirement defined in Article 94(2) of PSD2 shall be regarded as an additional requirement of a contractual nature in relation to the access to, and subsequent processing/storage of, personal data in the context of provision of payment services (see page 14 of the EDPB Guidelines). Due to the fact that the explicit con-

sent under Article 94 (2) of PSD 2 is a contractual consent, the following aspects are implied, according to the EDPB Guidelines.

- When entering into a contract with a payment services provider in line with PSD 2, data subjects must be made fully aware of the specific categories of personal data that will be processed.
- Data subjects shall be made aware of the specific (payment service) purpose for which their personal data will be processed and shall agree to these clauses in an explicit fashion.
- The relevant clauses should be clearly distinguishable from the other clauses within the contract and should be required to be accepted by the data subject in an explicit fashion.

In conclusion, consent under Article 94 (2) of PSD 2 does not represent a legal ground for the processing of personal data; however, it ensures a degree of control and transparency for the user of payment service.

In Austria, Article 94 (2) of PSD 2 has been transposed in Section 90 (4) of ZaDiG 2018 without, generally speaking, any notable differences. Nonetheless, Section 90 (4) of ZaDiG 2018 goes a step further than 94 (2) of PSD 2 by stipulating that payment services providers shall inform payment services users about the processing of personal data in accordance with Article 13 (Information to be provided where personal data are collected from the data subject) and Article 14 (Information to be provided where personal data have not been obtained from the data subject) of the GDPR.

Austrian banking secrecy regulation as an additional set of requirements pertaining to processing of customer's data by third-party providers

Apart from requirements pertaining to (explicit) consent under the GDPR and PSD 2 regime, there is one additional aspect that needs to be considered when assessing the role of customer's consent in the context of open banking regulation, namely consent to allow access to a customer's banking data as per banking secrecy provisions. See The Role of Consumer Consent in Open Banking: Financial Inclusion Support Framework. Technical Note; Washington, DC © World Bank (the "Technical Note").

Banking secrecy (*Bankgeheimnis*), a general obligation of banks not to pass on information to third parties which they obtained because of a business relationship, is traditionally excluded from the scope of the EU harmonisation project. This means that the banking secrecy legislation is almost entirely based on national rules. In Austria, the banking secrecy rule in enacted in Section 38 of the Austrian Banking Act (*Bankwesengesetz*, BWG).

Section 38 (1) of the BWG sets out that credit institutions (eg, banks), their shareholders, members of governing bodies, employees, and other staff employed by the credit institutions shall not disclose or exploit secrets entrusted to them or made accessible to them exclusively based on business relations with customers. This means that the entities/persons subject to banking secrecy rules must ensure their customer's interest in confidentiality in the form of a duty of confidentiality on the part of the obliged entities/persons (see Kammel in Laurer/M. Schütz/Kammel/Ratka, BWG Section 38 No 1-7 (Status 1.1.2019, rdb.at)).

Despite the strict nature of the banking secrecy provision, Section 38 (2) of the BWG lays down several scenarios which release the obliged entities/persons from banking secrecy requirements. These include, inter alia, the customer's express and written consent to the disclosure of the secret, pursuant to Section 38 (2) No 5 of the BWG (whereby it shall be noted that the BWG also foresees certain exemptions from the requirement that such consent shall be provided in a written form, in particular in cases where means of distance communication with customer authentication are used). Austrian legal scholars have described express and written consent as a "non-genuine exception" to banking secrecy regulation and simultaneously emphasised its function as a protective measure to ensure that the customer does not grant premature or misleading consent (due to the requirement of written form and an express nature) (see Kammel in Laurer/M. Schütz/Kammel/Ratka, BWG Section 38 No 20 (Status 1.1.2019, rdb.at)).

In light of the above, Austrian law imposes – in addition to explicit consent-related requirements under the GDPR and PSD 2 – explicit and written consent requirements under the Austrian banking secrecy legislation, under the assumption that the entity/person in question is subject to the respective rules. This means that the relevant entities shall also observe this aspect when considering participating in open banking arrangements, in particular due to the possible consequences/sanctions that may apply in the case of a breach of the banking secrecy legal framework which range from civil and criminal to administrative sanctions.

Conclusion

Considering the ever-growing popularity and presence of open banking on the financial services market, it may be expected that such arrangements will become more and more important as well as increasingly used by different market participants. Although this will bring benefits to customers and the financial services market as such, it will simultaneously create challenges for legislators and regulators to ensure a safe and stable market.

Despite the issue of consent for processing data in the course of existing open banking arrangements in the EU being, for the most part, clarified, the authors believe that there are still several uncertainties which may – especially in the case of larger amounts of data and other types of data being processed – cause problems. In order to avoid any issues in the future, the amendment of PSD 2 (as well as any other legal acts) should also clarify in detail the interplay of PSD 2 and the GDPR as well as – although not important for the EU as a whole – potential conflicts with the national banking secrecy regimes.

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa, and Asia Pacific. It is the leading mid-market M&A and private equity firm in Europe and has more than 70 corporate partners across Europe specialising in PE. The management advisory team has acted on over 30 mandates over the last three years with a combined value of over EUR36 billion. The team at DLA Piper has specific expertise in fundraising, buyouts and secondaries, buy and builds, sponsorship and management, corporate ventures and venture capital and exit planning and execution (M&A/IPO/refinancing/return of cash).

Authors

Jasna Zwitter-Tehovnik specialises in finance and projects and M&A, and is qualified in Austria, England and Wales, New York, and Slovenia. Her practice covers the entire financial services and infrastructure sector as well as a broad range of additional industrial sectors. She advises commercial and investment banks, fintechs, mezzanine financiers and private equity providers, and corporates on a wide range of financing and M&A transactions as well as debt restructurings. Other key areas of Jasna's practice include infrastructure and energy projects, including private partnership transactions, and privatisations, often in a cross-border context. She is ISDA counsel for Austria and advises on a broad range of regulatory aspects.

Anže Molan advises clients on regulatory aspects across a wide range of industries and sectors with a special focus on banking regulatory law, regulation of other financial services, fintech services as well as post-Brexit financial regulation, most notably in the CEE and SEE regions. He is also experienced in project financing transactions and M&A transactions, often with a cross-border component. In the past few months, he has advised on several projects taking place in Austria, Croatia and Slovenia. An important pillar of his practice is providing advice on corporate matters such as corporate transactions as well as advising clients in respect of other kinds of regulatory matters such as data protection.

Contributed by: Jasna Zwitter-Tehovnik and Anže Molan, **DLA Piper**

DLA Piper Weiss-Tessbach Rechtsanwälte GmbH

Schottenring 14
1010 Vienna
Austria

Tel: +43 1 53178 1042
Fax: +43 1 53178 52 52
Email: jasna.zwitter-tehovnik@dlapiper.com
Web: www.dlapiper.com/en/austria/locations/vienna/

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com