Open banking – when will it start?

Marcin Olechowski and Wojciech Iwański of Sołtysiński Kawecki & Szlęzak
dive into the intertemporal conundrum that has created legal uncertainty around the launch date for open banking in Poland

A cornerstone of the open banking revolution is the ability of third party providers (TPPs) to interface with the systems of account servicing payment service providers (ASPSPs) – usually traditional banks – in order to provide customers with certain services based on the accounts that ASPSPs manage.

In the European Union, the interfacing between TTPs and ASPSPs has been ushered in by the Second Payment Services Directive (EU Directive 2015/2366; PSD2). PSD2 requires ASPSPs to grant access to TPPs that operate either as payment initiation service providers (PISPs) or account information service providers (AISPs). The uniform solutions introduced by PSD2 replace a fragmented pre-existing regime where national regulations addressed the issue in a variety of ways.

In Poland, the new PSD2 regime was incorporated into the Payment Services Act (PSA) through the Amending Act of May 10 2018, which entered into force on June 20 2018 and provided for a general transition period until December 20 2018. At the same time, ASPSPs and TPPs are both required by the Regulatory Technical Standards set out in the Commission Delegated Regulation (EU) 2018/389 of November 27 2017 (RTS) to implement a number of security measures by September 14 2019.

This has resulted in some uncertainty as to which of those dates triggers the obligation for Polish ASPSPs to enable direct access for TPPs in accordance with PSD2 principles.

We argue in this article that the correct interpretation is that the obligation to allow TPPs direct access to client accounts will only arise when a given ASPSP is RTS-compliant, which should occur no later than September 14 2019.

Open banking begins with the appropriate security levels

PSD2 provides for two general guidelines that regulate the scheduling

Dr Marcin Olechowski
Partner, Sołtysiński Kawecki & Szlęzak
Warsaw, Poland
T: +48 22 608 70 62
F: +48 22 608 70 70
E: marcin.olechowski@skslegal.pl
W: www.skslegal.pl

About the author

Marcin Olechowski is a partner and the head of the financial regulatory/banking and finance practice. He regulatory advises financial sector clients and service providers on regulatory and client documentation issues concerning the online and mobile provision of financial services, new product development and other fintech-related matters, including Bitcoin. He lectures at the Warsaw University Faculty of Law on banking law, including fintech, and sits on the supervisory board of Mediacap SA, a publicly listed leading Polish marketing and communications group focused on applying big data, video online and machine learning solutions in marketing and

Dr Wojciech Iwański
Senior counsel, Sołtysiński Kawecki & Szlęzak
Warsaw, Poland
T: +48 32 731 50 23
F: +48 32 731 59 90
E: wojciech.iwanski@skslegal.pl
W: www.skslegal.pl

About the author

Wojciech Iwański is a senior counsel and regularly advises financial sector clients and service providers on financial regulatory and client documentation issues related to the online and mobile provision of financial services, new product development and other fintech-relevant matters (including Bitcoin). Wojciech, who also practises in securities and capital markets law, is currently involved in a project aiming to implement distributed ledger technology as a sectoral solution in the Polish banking industry for client documentation. His doctoral thesis concerned the impact of the Payment Services Directive on Polish regulation of e-banking services.

of its implementation into national legal systems. First, PSD2 Article 115(1) defines a deadline by which EU member states must have adopted and published the measures necessary to enforce PSD2. Second, PSD2 Article 115(2) indicates the expected start date for the application of national implementing provisions. In both cases, the date specified is January 13 2018 (the Polish legislator missed both deadlines). However, as discussed below, PSD2 also provides for certain exceptions from these general intertemporal rules.

The first of those exceptions relates to the fact that PSD2 requires TPP activity to be carried out in a secure environment, which presupposes the adoption – both by ASPSPs and by TPPs – of a range of technical measures aimed at ensuring the security of the payment services provided, including, in particular, securing the movement of customer data between ASPSPs and TPPs.

Indeed, both PSD2 and Polish law specifically require ASPSPs to ensure secure communication with TPPs in line with the RTS's requirements regarding joint and secure open communication standards (Articles 66(4)(a) and 67(3)(a) PSD2 and, respectively, Articles 59r(4)(1) and 59s(3)(1) PSA). This is mirrored by an analogous obligation on TPPs (Articles 66(3)(d) and 67(2)(c) PSD2 and, respectively, Articles 59r(3)(4) and 59s(2)(3) PSA).

Secure communication between ASPSPs and TPPs requires payment service providers to develop a range of systemic solutions, including implementing processes that ensure identifiability of all interactions with other payment service providers (Article 29 RTS); the introduction of special access interfaces (so-called APIs) or the adaptation of interfaces of direct access of the users (Article 31 RTS); or the enabling of TPPs to rely on all authenticating procedures made available by the ASPSP to the user of the payment services, including strong user authentication procedures (Article 30(2) RTS).

However, Article 115(4) PSD2, by way of express derogation from the general date of application of PSD2, requires member states to ensure the application of security measures referred to in Articles 66 and 67 PSD2 (which concern, respectively, PISPs and AISPs), from 18 months after the date of entry into force of the RTS (ie, as of September 14 2019).

This means that national provisions implementing PSD2 solutions with regard to the right of users to avail of the services of PISPs and AISPs in accordance with the principle of direct access do not need to enter into force or be applied prior to September 14 2019.

Indeed, since the provision by TPPs of services based on direct access to payment accounts requires the implementation of security measures mandated by the RTS, and since ASPSPs are not obliged to apply those same security measures prior to September 14 2019 (Article 22(1) of the Amending Act), then an ASPSP's obligation to grant TPPs direct access to the payment accounts managed by that ASPSP will not arise as long as this deadline has not lapsed (or a given ASPSP has not implemented the RTS-mandated solutions, if earlier).

Otherwise, both the ASPSP and the TPP would breach the provisions of the PSA which require the observation of specific security standards applicable to mutual communication between ASPSPs and TPPs.

This conclusion is also supported by functional arguments. Prior to PSD2, many EU jurisdictions, including Poland, did not regulate TPP activity at all. As a result, the introduction of these services in those markets, including Poland, requires setting up an entirely new legal and system infrastructure connected with the activity of TPPs, including the adaptation of the IT systems of payment service providers, which in turn need to satisfy the security requirements provided in the RTS. Providers of payment services should thus have an

appropriate time for effecting these technical-implementation tasks.

This concern is reflected by the view of European Banking Authority (EBA) that the 18-month transitional period following the entry into force of the RTS is designed to provide the payment services sector with the necessary time to develop market standards and technological solutions in accordance with the RTS (Final Report, Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), EBA/RTS/2017/02, 23.02.2017, pp. 4 and 42). The alignment by ASPSPs and TPPs of their activities with the RTS rules is of key importance for ensuring security of the newly regulated services. ASPSPs are not, however, obliged to adapt their activity to RTS before the date of commencement of application of same (ie September 14 2019). Indeed, both the EBA and the Polish Financial Supervision Authority (PFSA) have merely postulated and encouraged, rather than required, ASPSPs to adapt their activity to the requirements of RTS before September 14 2019.

A contrary view that required enabling open access prior to the implementation by ASPSPs of the solutions mandated by PSD2 would effectively result in allowing TPPs to access payment accounts outside of any RTS-mandated security standards. This would pervert one of the basic purposes of PSD2, namely to increase security in payment services. This observation applies of course to a situation in which in a given state, such as Poland. No rules were provided for the provision of this type of service prior to the entry into force of PSD2.

No grandfathering of TPP activities under Article 115(5)

These conclusions are not affected by Article 115(5) PSD2, which says that member states shall not forbid legal persons that performed the activities of PISPs and AISPs, within the meaning of PSD2, in their territories before January 12 2016, to continue with those activities during the transitional period referred to in Article 115(2) & (4) PSD2 and in accordance with the currently applicable regulatory framework.

Under Polish law, this provision does not – in our opinion – provide grounds for TPPs to provide services between January 13 2018 and September 14 2019 in accordance with the principle of direct access in a manner other than in accordance with the security measures provided for in the RTS.

Indeed, member states which did not previously regulate or which prohibited TPP activity, are not mandatorily bound to enable TPPs to provide PIS and AIS services in the transitional period.

This is clearly the case in Poland. Until the implementation of PSD2, Polish law did not provide a regulatory framework (statutory provisions, regulatory guidelines, etc.) that permitted the provision of services based on access to a payment account. To the contrary, the Polish Financial Services Authority's Recommendation concerning internet payments of November 2015 expressly considered as impermissible *any disclosure whatsoever* by a customer of its log-in data – which in practice impedes (and even makes impossible) the provision of services by TPPs. In the view of the PFSA, disclosure by a customer of its authenticating data should be deemed an example of failure by the user to fulfil its cautionary obligations related to the use of a payment instrument (Article 42(2) PSA).

The PFSA Recommendations applicable as of January 12 2016 should be considered as the Polish regulatory framework (as per Article 115(5) PSD2), making it impossible for TTPs to provide services in a scheme based on direct access to a payment account and with use of the authenticating data of the user.

Thus, under Polish law, the obligation under Article 115(5) PSD2 to enable TPPs to continue the earlier conducted activity in the transitional period does not arise, because these entities were not previously authorised to provide services based on access to an account.

The same conclusion needs to be reached based on the transposition of Article 115(5) PSD2 into Polish national law by Article 22(3) of the Amending Act, which provides that prior to September 14 2019 payment services providers are obliged to apply "hitherto provisions regarding security of payments".

Although this wording might be viewed as narrower than the formula "currently applicable regulatory framework" used in Article 115(5) PSD2, it is not enough to constitute a permission for TPPs to provide services based on access to payment accounts in a manner other than in accordance with the standards of security set out in the RTS in the transitional period. Indeed, a narrow construction of this formula would lead to the absurd conclusion that even though prior to June 20 2018 (the entry into force of the Amending Act) customers were prohibited from disclosing their individual authenticating data for the purpose of provision by TPPs of services based on access to a payment account. After September 14 2019 TPPs have to comply with rigorous standards of security set out in RTS, the period between June 20 2018 and September 14 2019 would be a regulatory void where the provision of this type of service would not, in principle, be subject to any restrictions whatsoever. This is difficult to reconcile with one of the basic assumptions of PSD2 – the introduction of uniform and safe rules of access by TPPs to payment accounts (which are regulated in detail in the RTS), since it would expose payment services users to increased risks resulting from the lack of application of any regulatory framework whatsoever defining the rules for the provision of payment services by new providers (TPPs).

This is difficult to reconcile with one of the basic assumptions of PSD2 – the introduction of uniform and safe rules

Article 115(6) does not justify direct access prior to September 14 2019

A separate question is whether earlier direct access might not result from Article 115(6) PSD2, which stipulates that member states must ensure that until individual ASPSPs comply with the regulatory technical standards referred to in Article 115(4) PSD2, they will not abuse their non-compliance to block or obstruct the use of payment initiation and account information services for the accounts that they are servicing.

However, the provision is far from clear and its wording leaves much to be desired. In particular, it is unclear to which time period does this prohibition of abuse relates: the

transitional period between implementation of PSD2 into the national legal order and the day of application of RTS (ie September 14 2019) or the period following the lapse of the period of application of RTS (ie after September 14 2019)?

Indeed, when referring to the need for ASPSPs to fulfil their obligations under the RTS, the European legislator did not cross-refer to Article 98 PSD2 but to Article 115(4) PSD2, which points to the need to implement the security measures set out in that provision no later than at the moment of the lapse of 18 months from the date of the entry into force of the RTS (September 14 2019).

In our view, one may cautiously accept that Article 115(6) PSD2 in fact relates to cases of ASPSPs that will have failed to become RTS-compliant by the maximum deadline of September 14 2019 and will attempt to rely on this failure as an obstacle for TPPs.

Cross-border activity of TPPs prior to September 14 2019

A final issue is how member states treat TPPs that were permitted these activities under the home state's regulatory framework and that would like to provide further services in the home state on the basis of the European freedom to provide services.

In our view, in this case a Polish ASPSP will not be obliged to enable a TPP to have access to accounts of users before September 14 2019 (or before the implementation of the RTS solutions by that ASPSP) under rules other than those that meet the standards of security provided in RTS.

Indeed, in accordance with Article 115(5) PSD2, member states cannot ban legal entities that acted as a PISP or AISP in their territory before January 12 2016 from continuing this activity in their territory during the transitional period.

This means that those particular member states that regulated and deemed admissible TPP activity (also as regards the manner in which it was carried out) prior to the entry into force of PSD2 cannot restrict TPP activity in the transitional period.

It does not mean that a TPP may during this period also start to carry out a new activity

However, while PSD2 allows TPPs to continue their activity during the transitional period, it does not mean that a TPP may during this period also start to carry out a new activity of a cross-border nature in other member states where the host member state has to that date directly or indirectly banned TPP activity – as is the case in Poland.

Open banking – September 14 2019

To conclude, open banking in Poland will only fully start 18 months from the entry into force of the RTS, in other words, no later than September 14 2019.