The minefield of TPP regulatory checking for PSD2 open banking

27/11/2018

Konsentus: In January 2018 the European Union Payment Services Directive 2 (PSD2) came into force across Europe, delivering a consistent vision for open banking across all member states. Payment Service Users (PSUs), e.g. consumers and SMEs, will have a legal right to share their personal transactional account data from their Financial Institutions (FIs) with regulated third parties to enable increased competition and better consumer choice.

FIs must provide regulated third parties access to end user transactional account data. Key critical dates that FIs must work to, as directed by the European Banking Authority (EBA) and local National Competent Authorities (NCAs) are:

- March 2019 – F's must have platforms available for external market testing
- Sept. 2019 – FIs must go live or face the risk of fines from regulators

FIs must comply with this regulation and can only provide data to regulated/authorised Third Party Providers (TPPs).

Although as Brendan Jones, Chief Commercial Officer of Kosentus notes "To date there are still a number of countries that have not transposed PSD2 requirements into national law including Romania, Spain and Ireland. Also, there are a number of NCAs who have not yet announced how they will register or approve TPPs, how they will hold the data and how they will communicate revocation. The timings are thus quite challenging."

Who is Covered by PSD2 open banking?

The general term used by the industry is PSD2 open banking, but this is very misleading as it implies that the Regulatory Technical Standards (RTS) published by the EBA only cover banks; they do not. They cover all Account Servicing Payment Service Providers (ASPSPs) or what we would term as FIs.

Under the original Payment Services Directive, it qualifies a 'payment account' as

"an account held in the name of one or more payment service users which is used for the execution of payment transactions."

There is no definition or exclusion on how the party holding the account is regulated. As Brendan clarified, "Whilst it may seem unfair, the regulations cover all banks no matter how large or small, E-money regulated accounts e.g. e-wallets that are used to pay multiple merchants, Payment Institution regulated accounts, credit cards, credit unions and all reloadable prepaid cards. The regulations are very broad on who is encompassed by the requirement."

There are some 9,000 plus FIs in Europe that need to be ready for open market testing under mandatory PSD2 timescales. Brendan went on to add "we are still finding many organisations are unaware of the timings and the requirements".

The EBA recently stated: "Ignorance of them can of course not be used to justify non-compliance. And added, non-compliance amounts to a breach of law, with the resultant consequences for the legal entity."

How to Provide the Data

FIs are required to put in place a dedicated interface and most organisations are doing this through the form of an API for TPPs to access. They do though still have to put in place a 'fall-back mechanism' in the event of the failure of their PSD2 API. This means online access via functionality such as screen scraping unless the FI gains an 'exemption certificate' from their NCA in consultation with the EBA. TPPs must be able to access an FIs fall-back mechanism if their API is unavailable for more than 30 seconds.

Brendan noted though that "many FIs are unaware of both the requirement to put in place a fall-back mechanism and also the ability to gain an exemption certificate. There has been a lot written about the need for APIs but less has been communicated about fall-back and exemption certificates, although the FCA recently did highlight they were concerned they could be faced with a rush of applications." The FCA stated "We would encourage ASPSPs seeking exemption not to wait until this (sic March 14 2019) date to make these available. Stress testing will also need to be carried out by the ASPSP." They then added "The RTS does not allow us to grant a partial exemption. We will provide opportunities for ASPSPs to engage with us before submission of the exemption request. We also encourage timely requests for exemption as we will need time to make an exemption assessment."

If the FI chooses not to offer an API solution then they can offer just a "dedicated interface", what some are calling screen scraping version two. If they do this the FI must be able to ensure:

1. TPPs using the dedicated interface can be identified and checked for their regulatory status
2. The TPP can only access, store or process data the consumer has consented to
3. The data the TPP accesses is logged and, if requested, made available to the relevant NCA
4. They can, upon request, justify to the NCA the use of the interface rather than an API

The Challenge on Checking Who You Provide Data To

The regulations are clear that it is the job of the FI to validate the identity of the TPP and check their regulatory status, this is crucial to establishing the trust factor as part of PSD2 open banking. This means that all FIs need to ensure that they only ever supply PSU data to approved/regulated TPPs. If they supply data to a TPP who is not, then they are in breach of PSD2 and GDPR.

When an FI is approached to provide data for the first time by a TPP they need to:

1. Validate the TPP eIDAS Certificate via the Qualified Trust Service Provider (QTSP) to confirm the identity of TPP and associated NCA
2. Check with the correct NCA that the TPP is regulated/approved
3. Issue the Access Token to the TPP as appropriate (PSD2 schema)

Then each time the TPP accesses the FIs API the FI needs to:

1. Validate the TPP eIDAS Certificate via the correct QTSP to confirm identity of TPP and associated NCA

2. Check with the correct NCA that the TPP is regulated/approved
3. Validate the Access Token checking that end user has not revoked consent

In theory this all seems very simple for an FI, but this is where the minefield exists as Brendan explained: "If there was one EBA single machine readable, real-time database covering both QTSPs and NCA regulated TPPs it would be easy but:

- The EBA Register is not a machine readable, real-time, online accessible database
- In addition, the EBA Register is only updated twice a day for downloading and updated in many cases only once a day with NCA updates
- NCA databases are not machine readable, real-time, online accessible databases and there are 31 of them
- There are 70+ QTSPs who issue eIDAS Certificates and a TPP can choose to use whichever it choses
- NCAs are not legally obliged to inform QTSPs if there has been a change in the regulatory status of a TPP. Indeed, the NCA does not keep information on which QTSPs have issued certificates for TPPs.

And this is where Kosentus has stepped in to create this single registry database. Uniquely though it is being delivered as a SaaS service using RESTful APIs enabling the FI to interrogate the information. And in the world of payments there will always be disputes, and Konsentus operates an immutable audit to ensure that there is an indisputable record of all transactions and activity.

With over 100 databases that an FI must integrate or reference to ensure they are accessing source data with almost none being real-time or machine readable this can be a challenge for FIs. As Brendan went on to say; "With Konsentus providing the only real time, online, machine readable database currently for the market covering both TPP regulatory status and eIDAS identity checking, we believe the biggest threat to PSD2 open banking is

ensuring the NCA databases are ready and that FIs understand the importance of checking on the TPPs regulatory status."

Why is TPP Regulatory and Identity Checking Important

As highlighted, if an FI provides data to a non-regulated TPP they are potentially in breach of both PSD2 and GDPR. But it could be argued there are even greater wider market implications. After all, recent research by Accenture found that 85% of those asked said the fear of fraud would put them off sharing data, and 69% said they would not share financial data with businesses that were not banks.

Brendan concluded "as an industry we have an obligation to ensure the success of PSD2 open banking, as it will create huge opportunities for improving innovation and choice for consumers. The risk is that if TPP identity and regulatory checking is not thoroughly carried out, fraudsters could have some early successes and put the industry back years in terms of consumer perceptions of security."