PSD2 Review: Open Banking

Mastercard position paper on Open Banking
in the context of the PSD2 review

The revised Payment Services Directive (PSD2) has been instrumental in fostering competition in financial services and enabling new products and services through the creation of the Open Banking framework in the European Union. It is also a first and necessary step in the process of ultimately creating an open data ecosystem, where regulated and controlled access to a broad range of data can lead to better, more efficient, user friendly and tailor-made services across the economy.

Mastercard welcomes the European Commission's initiative to enrich competition through Open Banking and facilitate the flow and use of data for the ultimate benefit of consumers. We have been actively supporting the entire European ecosystem through our platform and network services that facilitate connectivity, while through some of our subsidiaries we are also active as Third Party Providers (TPPs) in many European markets. This puts Mastercard in a unique position, where we can offer a holistic view on how Open Banking has developed in Europe, what the key challenges and opportunities are, and how future regulation should respond.

In its position paper Mastercard outlines its views on key topics and issues in Open Banking (in the context of PSD2), which in our view need to be addressed by policy and regulation to improve and fine-tune the system in place.

For any questions and comments, please reach out to Boris Martinovic at boris.martinovic@mastercard.com

***

Summary of Mastercard's recommendations

1. **Quality of testing facilities**: The EBA should ensure consistency of application of the rules across jurisdictions, and sandboxes should reflect the production environment in terms of both functionality and specification. Any changes to the production environment should be reflected in the sandbox at least 90 days in advance of the change on the production environment. As an alternative to a fully functional sandbox environment, ASPSPs could offer a test environment through their production APIs using synthetic or test data.
2. **Standardization**: *In general*, the industry and the regulators should learn from current market experiences, and there should be further industry consultation and dialogue on how to best tackle the issue of standards going forward.
   For larger banking groups, clear and aligned API standards should be in place, defined to the right level of granularity, such that ultimately all the APIs should work the same way irrespective of whether different bank sub-groups have different API implementations and/or different end-points. In the interim, providing visibility to which groups use which API implementation, and requiring bank groups to document and highlight differences within the group would help.
   On uniform SCA user experience, the regulator should produce some guidelines, or they should identify the right authority that can create guidelines, mandate and police them. Ideally, the UK example of the OBIE User Experience Guidelines should be replicated.
3. **Fallback interfaces**: Ultimately, fallbacks should not be used. Until then, Mastercard suggests the following approach:
   - Where a fallback exemption has not been obtained by an ASPSP, TPPs and TSPs should be explicitly permitted to develop interoperability with any interface or external access point offered by the ASPSP to their PSUs.
   - Where a fallback exemption has not been obtained, an ASPSP must publish specifications for all external facing access points or interfaces related to payment accounts to enable TSPs and TPPs to develop interoperability.
   - Before PSD2 is expanded to additional account-types or services, additional consideration should be given to how the RTS is governed and enforced.

   The Commission should also adopt a technically neutral approach to alternative access methods (when APIs are not available) that is not limited to screen scraping, thus allowing interoperability with any external access point or interface.
4. **Certificate requirements**: Future regulation should define the relevant processes and procedures with regards to certificates, including their content, revocation, and renewal. Also, the related enforcement actions should be defined and then executed in a harmonized way across the EU.
5. **Change management**: A uniform change management process across ASPSPs should be created, with active communication from the ASPSPs to TPPs. In practice, a central facility (website) should be developed by an independent body where ASPSPs must publish:

- details and specification of their PSD2 APIs;
- advanced notifications of changes to existing APIs;
- details of new APIs;
- details of fallback provisions.

6. **Overseeing the Regulatory Technical Standards (RTSs)**: More and better enforcement should happen at national level, which should also be consistent and coherent across the European Union.
7. **Monetization**: Mastercard supports the principle of free-at-point-of-access banking data for PSUs. However, providers of data should be able to support access provision with further chargeable services or enhancements and regulation should allow space for a complementary value-add ecosystem. A fair distribution of value should be permissible where ASPSPs and others are supporting such an enhanced ecosystem. Also, alignment is needed across the different instruments to ensure consistency within the ecosystem.
8. **Data management**: With regards to *use of data, interplay with GDPR and definitions/terminology*, Mastercard recommends to:
    - Remove restrictions of articles 66, 3 (g), 67, 2 (f) and 94, 2 of the PSD2.
    - Failing to do so, allow TPPs to obtain consent (GDPR) for further processing of the data or use different lawful basis such as legitimate interest, execution of the contract, legal obligation, etc.
    - Clarify that TSPs can process the data for AML/KYC purposes, eventually on behalf of PSPs.
    - Include additional authorized processing activities, such as product/service improvement, etc.
    - Permit the anonymization and aggregation of the data about the transaction, as well as the transaction itself to develop innovative new services and improve existing products/services.
    - Confirm that TPPs and TSPs can further process so-called Silent Party Data based on the legitimate interest of the data controller, as long as the interests or fundamental rights and freedoms of the data subject are not overridden.
    - Avoid repeating language from data specific legislations, such as consent, in non-data legislations by giving it a different meaning.
    - Replace references to "(explicit) consent" in the PSD2 by "agreement", to avoid confusion with the GDPR.
    - Ensure that data usage rights are appropriately scoped.
    - Adopt a consistent set of definitions.
    - Continue to encourage the development of industry-led standards for data sharing and data interoperability, including in the context of European Data Spaces and the work of Gaia-X.

1. Dedicated APIs / interfaces

1.1. Quality of testing facilities

ASPSPs are required[1] to offer sandboxes or test facilities to allow developers to integrate to the dedicated interfaces without relying on production users and data to complete a stable and reliable integration to the ASPSP.

In general, ASPSPs have fulfilled the requirement by making available some functionality that only allows for some primitive testing. For example, in most cases, the sandboxes do not allow the TPPs to develop and test integrations to make them stable and robust, taking into account differences between:

- different customer types,
- what should be identical SCA user journeys including
    - non-happy path SCA user journeys,
    - multiple approvers;
- business logic including
    - payment cut-off times,
    - value limits for payments
    - 'step-up' SCA based on bank risk;
- error messages during downtime,
- etc.

The quality of the sandboxes is essential for developing high quality software and user experience. The RTS and subsequent clarifications from the EBA does not seem to have had a significant impact on the quality of the sandboxes over time.

Hence implementers of PSD2 interfaces such as TSPs or TPPs have resorted to perform significant testing on the production interfaces.

This situation is not sustainable, as it puts increasing operational risk or testing cost on TSPs and TPPs, as Open Banking gets adopted by businesses across the Union. A simple way to solve this would be to force ASPSPs to 'dogfood' their dedicated PSD2 interfaces, that is using them for their own products.

[1] RTS, Article 30 (5)

Mastercard recommendation:

The EBA should ensure consistency of application of the rules across jurisdictions, and sandboxes should reflect the production environment in terms of both functionality and specification. Any changes to the production environment should be reflected in the sandbox at least 90 days in advance of the change on the production environment. As an alternative to a fully functional sandbox environment, ASPSPs could offer a test environment through their production APIs using synthetic or test data.

1.2. Standardization

Industry standards

PSD2 and the level 2 RTS on SCA and CSC are meant to be technologically neutral by not mandating the use of one particular standard/technology. The RTS state that the ASPSP should give access either through:

- a "dedicated interface" (typically an API), plus a fallback in case the dedicated interface doesn't operate as it should – although the ASPSP can be exempted from the fallback requirement; or
- a "modified customer interface" (MCI).

In parallel with legislative work with the PSD2 and RTS, standardization efforts have developed. This includes The Berlin Group NextGenPSD2 XS2A Interoperability Framework, the STET PSD2 API specifications, local API initiatives such as PolishAPI standard, and to some extent the CMA9 OBIE and OBL API specifications. It is especially worth noting the proliferation of local standards (such as CBI Globe, under-pinned by Nexi, in Italy, or the PolishAPI in Poland). It is also worth noting that typically such standards are not really standards in the traditional sense of the term, but rather more similar to guidelines that the local ecosystem adopts with varying degrees of consistency.

While standardization has been welcomed by TSPs and TPPs, the standards have often come out of sync with the rapidly evolving regulatory landscape of interpretations by EBA and local regulators. Even when standards have adjusted to the updated interpretation, ASPSPs have been slow to update to the latest standards.

In addition, ASPSPs have been relying on standards to become compliant with the RTS, however, more often than not, the standards have actively caused the ASPSPs to be incompatible. In particular the 'feature parity'[2] between customer interfaces and the dedicated PSD2 interface, are likely to be unfulfilled, when standards in detail specify the functionality and data that is made available to the TPPs. This has often led to entrenched conversations between ASPSPs and TPPs, where diverging from the standard would be needed

[2] RTS, Article 36 (1)

Today we have a somewhat fragmented API landscape, despite the efforts of the industry to follow standards. In addition, a large cost has been incurred by both ASPSPs and TPPs in trying to make the ASPSPs fulfil their 'feature parity' requirements, in order for TPPs to serve customers in local markets, where 'non-standard' features and data is needed[3].

Under various (draft) EU legislation forcing entities to share data with others (e.g. draft Data Act, DGA, DMA as regards gatekeepers), we already see the European Commission facilitating interoperability by encouraging the development of technical standards, such as access data, data structure and formats; and removing obstacles to data portability when switching between data processing services through standards. From the business side, the Gaia-X project gathers industry representatives with the aim to create a federated open data infrastructure based on European values for data and cloud sovereignty, such as openness, privacy, security, and transparency. As part of this association, companies such as Mastercard gather efforts, knowledge, and expertise to establish the right conditions and highest standards for strong and secure data sharing spaces at scale. Such initiatives need to be considered within the context of the PSD2 review so as to build on existing resources and avoid inconsistency of approach.

Connectivity to large banking groups

In addition, in practice TPPs are also facing a high complexity of connecting into larger banking groups whereby the initial API connections seem similar, however they aren't necessarily uniform, therefore creating either a significant testing overhead (testing for each local banking brand) or pushing TPPs to take a calculated risk (to only test certain banks). This is in-part due to historic formation of these banking groups and their back-end systems, however the individual banking groups could support TPPs with better guidance on which APIs within a banking group are the same and which have a degree of variation. In France, for instance, one institution had 40 different APIs – one for each region.

Uniform user experience of SCA

The RTS requires[4] ASPSPs to make available, through the TPPs, the same SCA methods that they make available to PSUs in their customer facing channels. Based on practical implementation of dedicated interfaces, there is a significantly different user experience between ASPSPs.

In some instances, ASPSPs rely on the exact same authentication system that is also used in the customer-facing channels and in other cases there is a significant variability on what the user experiences during the SCA flow of the PSD2 interface, including:

- embedded consent-like language;
- embedded account selection;

[3] Examples include: local payment options, local remittance information, reconciliation data, ASPSP specific transaction data, etc.
[4] RTS, Article 30 (2)

- poor user experience or poor conversion rates;
- mobile unfriendly user experience;
- broken app-to-app switching;
- dead ends in redirect flows.

In general, TPPs have blind spots when it comes to seeing where consumers are being lost in the process, which should be addressed.

In UK Open Banking, significant alignment was produced between ASPSPs and TPPs due to OBIE publishing User Experience Guidelines. It is clear that EBA is not delegated such wide-reaching powers, and without it we will continue to see large fragmentation between user experience between ASPSPs and PSUs being subjected to unfamiliar user journeys.

Mastercard recommendation:

On standardization in general, Mastercard suggests that the industry and the regulators should learn from the experiences as described above, and there should be further industry consultation and dialogue on how to best tackle the issue of standards going forward.

For larger banking groups, clear and aligned API standards should be in place, defined to the right level of granularity, such that ultimately all the APIs should work the same way irrespective of whether different bank sub-groups have different API implementations and/or different end-points. In the interim, providing visibility to which groups use which API implementation, and requiring bank groups to document and highlight differences within the group would help.

On uniform SCA user experience, the regulator should produce some guidelines, or they should identify the right authority that can create guidelines, mandate and police them. Ideally, the UK example of the OBIE User Experience Guidelines should be replicated.

1.3. Fallback / Contingency interfaces

In the final version of the RTS, the concept of fallback or contingency interfaces was introduced, based on pressure from TPPs. While seen primarily as an implementation safe-guard, now 2.5 years after the production date of the RTS, we still see a significant portion of the ASPSPs not having received a fallback exemption. This means that it is unclear whether ASPSPs will ever seek to make their dedicated interfaces compliant with the RTS and get the 'NCA stamp of approval' by obtaining an exemption from providing the fallback interface.

Even among ASPSPs where fallback interfaces are offered, there is still a large interpretation-based variability among the offering. Some ASPSPs have to some extent created a parallel interface to fulfil eIDAS certificate requirements, documentation requirements and to allow some exemptions to be applied[5]. Some TPPs question whether 'sandboxes' should be available for fallback

[5] Such as RTS, Article 10.

interfaces. And some ASPSPs are simply not providing additional information for TPPs, except for that they point to some website that should be 'screen scraped'. Some clarification on the scope of the fallback exemption is greatly needed, including that it should be clear that TPPs should be able to rely on ANY interface offered by the ASPSPs to its own PSUs.

In any case, the reliance on fallback or contingency interfaces 2.5 years after the production deadline should clearly be seen as a warning that the governance surrounding the RTS is not working adequately, and it should be improved.

PSD2 identifies screen-scraping as the fallback technology for when the regulated APIs fail or are unavailable. Fallback access / screen scraping is just one of the technologies in the market for account access when APIs are not available / functioning, and we think that the Commission should adopt a technically neutral approach to alternative access methods (when APIs are not available) that is not limited to screen scraping allowing interoperability with any external access point or interface. That would require ASPSPs to publish details on those access points.

Mastercard recommendations:

Mastercard's default position is that ultimately fallbacks should not be used. Until then, we suggest the following:

- **Where a fallback exemption has not been obtained by an ASPSP, TPPs and TSPs should be explicitly permitted to develop interoperability with any interface or external access point offered by the ASPSP to their PSUs**
- **Where a fallback exemption has not been obtained, an ASPSP must publish specifications for all external facing access points or interfaces related to payment accounts to enable TSPs and TPPs to develop interoperability**
- **Before PSD2 is expanded to additional account-types or services, additional consideration should be given to how the RTS is governed and enforced**

The Commission should also adopt a technically neutral approach to alternative access methods (when APIs are not available) that is not limited to screen scraping, thus allowing interoperability with any external access point or interface.

1.4. Certificate requirements

While the RTS requires[6] the use of eIDAS QWAC and QSealC certificates for accessing dedicated PSD2 interfaces, no additional processes or procedures have been mandated surrounding the contents of the certificates[7], certificate revocation checking practices or certificate renewal procedures.

[6] RTS, Article 34

[7] An ETSI standard (ETSI 119 495) has been developed, but the author is not aware that it has been adopted as the canonical standard by EBA or the member states

In practice, since certificates have started to expire, we have seen that certificate renewal practices are lacking from the ASPSP side, which have involved costly manual processes for the TPPs and have in some cases resulted in downtime, as ASPSPs have not been able to update the certificates in a timely manner.

We have also seen ASPSPs and NextGenPSD2 framework further constraining the use of certificates, such as putting ASPSPs specific requirements onto certificates that are not required by eIDAS or the ETSI standard - and in some instances requiring TPPs to violate usage certificate policies (such as using a QWAC certificate to sign messages or decrypt messages).

Mastercard recommendation:

Future regulation should define the relevant processes and procedures with regards to certificates, including their content, revocation, and renewal. Also, the related enforcement actions should be defined and then executed in a harmonized way across the EU.

1.5. Communication on change management

ASPSPs are required[8] to make available any changes that are made to the dedicated interface, 3 months before the change affects the production environment. In practice the term "made available" is interpreted wildly differently between ASPSPs. Some ASPSPs inform of changes by email and continuously follow up with the TSPs and TPPs until they have made their changes. But many ASPSPs have opted to simply update a paragraph on a website or in their online documentation.

We have seen instances where minor changes on the ASPSP website have gone unnoticed by TSPs or TPPs, resulting in outages on the production interface. A uniform change management process across ASPSPs is essential, including active communication from the ASPSPs to TPPs.

Mastercard recommendation:

A uniform change management process across ASPSPs should be created, with active communication from the ASPSPs to TPPs. In practice, a central facility (website) should be developed by an independent body where ASPSPs must publish:

- **details and specification of their PSD2 APIs;**
- **advanced notifications of changes to existing APIs;**
- **details of new APIs;**
- **details of fallback provisions.**

[8] RTS, Article 30 (4)

2. Overseeing the RTS

Regulatory moving target for ASPSPs

ASPSPs have experienced a moving target for the requirements of the implementation of the RTS, with key topics being settled after development work has already been completed. This has led to a cycle of continuous rework for ASPSPs to meet the new regulatory target. The 'moving target' is further amplified by some standards that are largely being ASPSP driven, seeking the most conservative approach when there has been room for interpretation.

One such example is the EBA opinion[9] on obstacles imposed towards TPPs, which was only published one year *after* the production deadline of the RTS.

In addition, EBA Q&As continue to substantially change the interpretation of what the dedicated APIs need to offer.

We are approaching a more stable definition of what the regulatory requirements are only 2.5 years after the production deadline of the RTS. Hopefully this will be stable going forward, but it is a valuable learning experience, should we move towards revising PSD2 and the RTS.

Banking secrecy and reporting outcomes

TPPs as well as ASPSPs are required[10] to report issues on the PSD2 interfaces without delay to the NCAs. However, due to local bank secrecy regulations, it is often impossible for TPPs to understand how NCAs are using these reports and how ASPSPs are held accountable. In many ways, reporting is a black box for the TPPs. As reports have gone unanswered by NCAs and as TPPs experience that issues do not tend to get resolved through this mechanism, it is questionable whether TPPs will prioritize such reporting.

Without efficient shared issue tracking between the TPPs, ASPSPs and NCAs, there is a substantial risk of issues not being addressed through proper channels and parties not participating efficiently in the process. In particular, TPPs are required to report identical issues to NCAs, without simply contributing to a shared understanding of the issue. As the issues are often technical in nature, the matter at hand can often be lost in translation. Some TPPs are today coordinating through platforms such as the paid service 33 Report[11].

Mastercard recommendation:

We recommend that more and better enforcement happens at national level, which should also be consistent and coherent across the European Union.

[9] EBA/OP/2020/10
[10] RTS, Article 33 (3)
[11] https://www.33report.eu/

3. Monetization framework

Lack of ability for ASPSPs to monetize access to accounts is a key delaying factor for open banking market take-up in the EU. ASPSPs are forced to incur significant investment in establishing APIs. At present, ASPSPs cannot recoup this investment by charging TPPs, and there are significant question marks over the ability of ASPSPs to do so by charging PSUs. As Open Banking is extended to Open Finance, these challenges will become even more significant.

In addition, while PSD2 requires ASPSPs to share payment account data with AISPs free of charge, other (draft) EU legislation provide for the possibility to charge a fee – e.g. the draft Data Act provides that the data holder can charge a "reasonable compensation" to the data recipient (Art. 9(1) draft Data Act), etc. *Alignment is needed across the different instruments to ensure consistency within the ecosystem*

Mastercard recommendation:

Mastercard supports the principle of free-at-point-of-access banking data for PSUs. However, providers of data should be able to support access provision with further chargeable services or enhancements and regulation should allow space for a complementary value-add ecosystem. A fair distribution of value should be permissible where ASPSPs and others are supporting such an enhanced ecosystem. Also, alignment is needed across the different instruments to ensure consistency within the ecosystem.

4. Privacy and Data matters

In light of the ongoing discussions regarding existing Open Banking Implementation efforts and broadening horizons implicating Open Finance, Mastercard recognizes that data protection and better data management lie at the core of these discussions. These issues should be examined within both the context of PSD2 and applicable provisions of GDPR while keeping an eye on the need for more definitive industry standardization. . A principle-based approach remains an effective way for regulators to spur necessary sparks of innovation within the marketplace and Mastercard looks forward to engaging in these initiatives, as well as participating in any related industry and policy discussions.

Mastercard appreciates the efforts made by the European Data Protection Board (EDPB) and others to provide helpful clarification to existing legislation. For example, Guideline 06/2020 on the interplay of the PSD2 and the GDPR provides important guidance that payment services lawfully process personal information in that such services are always provided on a contractual basis between the payment services user and the payment services provider pursuant to GDPR Art. 6(1)(b). The Guidelines further clarify that ASPSPs lawfully process personal data requested by a PISP or AISP in order to perform their payment service to the payment service user through GDPR Art. 6(1)(c) which allows for the processing of such data "necessary for compliance with a legal obligation". These

clarifications are precisely the kind of assistance that the marketplace appreciates and stands ready to incorporate into their existing practices.

In that spirit, we set for the following thoughts and observations for broader discussion and contemplation.

4.1. Use of data (PSD2 context)

Art. 67 PSD2 limits what an AISP can do with the data: "The [AISP] shall … not use, access or store any data for purposes other than for performing the [AIS] explicitly requested by the [PSU], in accordance with data protection rules" (Art. 67(2)(f) PSD2). The EBA has confirmed in Q&A 2018_4098 that "Articles 4(16) and 67(1),(2) PSD2 do not require that the [AISP] provides the consolidated information to the [PSU] in order for the service to constitute an [AIS] according to PSD2. The AISP may therefore transmit the consolidated information to a third party with the PSU's explicit agreement. Regarding the use made by any third party of the consolidated information transmitted, other provisions of EU law may apply, for instance the [GDPR]". In addition, the EDPB in its GDPR/PSD2 interplay guidance has indicated that for example, an AISP can actually do more with the data that what is stated in Art. 67(2)(f) PSD2 provided it obtains the GDPR consent from the consumer as to what else will be done with its data.

Still, at present, PSD2 terms are considered restrictive around what a TSP or TPP can do with the data they see flowing through, or the data being used in the provision of, the service. There are a few areas where this is restrictive and potentially not in the best interest of the PSU:

- There is no exception for counter-fraud or AML purposes. As a TSP, we are reliant on other legislation to carry out this activity. PSD2/PSD3 should be explicit in the appropriateness of this
- PSD2 has a limiting effect on both what the account holder can give agreement to and what the other actors in the eco-system can request / do with the data. There is no recognition of customer consent to further processing of their data. This is implied by GDPR but interpretations vary.
- There is no recognition of the need to conduct reporting on both PSU and / or ASPSP activity. For example, an ASPSP may wish to understand their activity in the context of the wider market and understand where their performance (eg.: API response time) does not meet market benchmarks. There should be provision for TSPs / TPPs to use anonymized and aggregated data to provide reporting services back to both PSUs and ASPSPs.
- For a lending relationship like a mortgage where it can go up to 30 years, in the U.S. the consent language provides the TPP (and their servicer) access to the data for *as long as* the loan is active. The lender does not have to go back to the consumer and have them re-authorize the consent every x number of months. The consent is part of the contract such that, as long as the mortgage is active, the lender is allowed to pull the OB data and confirm the status/credit worthiness of the consumer on an ongoing basis. It would be good if the review of PSD2 and the upcoming PSD3 addressed this.

- In general, PSD2 does not align with other data legislation that permits or foresees the benefit of anonymization and aggregation of data to develop innovative new services. This includes both the data about the transaction as well as the transaction itself.
- Any enhancement or evolution of PSD2 should ensure that data usage rights are appropriately scoped. For example, to settle disputes or to report activity across multiple parties, participants may need access to or rights to use 'source of truth' transaction data. This would also support upholding the overall ecosystem quality standards by enabling great oversight or challenge. Constraints around what kind of data, usage purposes, and data retention policies will surely be needed, but they should not be so strong that fundamental value-added services become impossible to execute.

4.2. Open questions for regulators and the industry to consider

Reciprocity

Under PSD2 ASPSPs are required to share customer data with AISPs. An ASPSP can also act as an AISP and, in that role, receive customer data from other ASPSPs. But some institutions are only AISPs, meaning that they only receive customer data but are not forced to share customer data with anyone.

It might be argued that the access to customer data for some institutions excludes other institutions from accessing such data and therefore it is not creating a "level playing field for existing and new entrants". This is the case of pure AISPs (typically fintechs) as well as some of the GAFAs. A question for regulators and the industry to answer would be if *going forward "pure AISPs" (i.e. financial institutions that are not ASPSPs) should also be forced to share customer data with others to the extent that they are permitted to do so under data protection rules*?

Of course, pure AISPs are subject to Art. 20 GDPR (right to data portability) – but that right is not fit for purpose because Art. 20 of the GDPR only requires a data controller to share customer data with another data controller (not a data processor), upon the PSU's request, "where technically feasible". Some of those "pure AISPs" may be subject to future legislation other than PSD3 that may, perhaps, force them to share customer data (e.g. DMA if designated as gatekeeper or the recently agreed Data Governance Act) – but shouldn't PSD3 also require those "pure AISPs" (e.g. fintechs and GAFAs) to share customer data with others subject to data protection rules and clear security safeguards? In addition, under Art. 20 of the GDPR, providing the information in a "machine readable format" can in itself present challenges between institutions where there is no standardised approach to doing this. *We suggest developing an infrastructure that standardises both machine readable access and machine to machine communication to enable data interoperability*.

Agreement

PSD2 requires ASPSPs to share payment account data with AISPs without the need for an agreement between the ASPSP and the AISP. But other (draft) EU legislation does foresee the need for an agreement – e.g. the draft Data Act provides that an agreement based on FRAND terms

should be entered into between the data holder and the data receiver (Art. 8(1) and 8(2) of draft Data Act) and that the EC will develop non-binding model contractual terms (Art. 34 draft Data Act).

It could be argued that *regulators should ensure alignment, for example by PSD3 requiring ASPSPs/data holders and AISPs/TPPs to enter into an agreement on FRAND terms*. This agreement could either be a bilateral agreement, or it could be based on a network of bilateral agreements / a multi stakeholder arrangement / multi stakeholder terms.

Duration of PSU contractual consent given to a TPP

At the moment, under PSD2 the contractual "explicit consent" given by a PSU (in particular an AISP) to access its payment account is in principle not limited in time (unless something else has been agreed between the PSU and the TPP).

It should be considered if under the new regulation the consent given by the PSU to a TPP to access their data should continue to be unlimited in time, or if it should be limited in time to a maximum of X days/weeks/months and therefore require regular renewals of consent. Mastercard is of the view that in principle consents should be limited in time, however, a one-size-fits-all approach would be flawed, instead case-by-case approach should be adopted.

4.3. Interplay with GDPR

The many different permutations of "controller to controller transactions", as data moves from context to context, contributes to a misalignment between intent of the RTS and market outcomes, plus a lack of transparency. A user needs to be presented with clear information about data use. This includes for example:

- being clear about when data is being transferred versus being processed;
- when they are agreeing to something versus providing consent;
- who is responsible for documenting the transfer of data once agreement or consent is given;

There is a strong reliance here on the user experience and interface to clearly inform the user and empower them to make decisions.

The blurring of different basis for processing and transferring data also leads to a conflict over who documents the information transfer. Should this be the responsibility of the account provider or the third party requesting the data, or both. Then when data is onward processed or transferred, who has visibility and takes responsibility.

This results in relying on a blend of different regulations and legal basis for the processing of account holder data, which creates opacity and friction, contrary to the desire to be transparent and straightforward. For example, data may frequently be collected using PSD2 consent, transferred to a 3rd party using GDPR consent, and then further processed on the basis of legitimate interest. All for fulfilling one request by an account holder to a third party.

4.4. Terminology / definitions

There are several terms within PSD2 that take on different meaning to GDPR or other regulations and clarity is needed.

The most important of these conflicting definitions is "consent". GDPR considers consent to be a freely given, specific, informed, and unambiguous permission for the processing of personal data. In PSD2, "explicit consent" means an agreement – a contract between the account holder and account provider to transfer data for a specific purpose, which differs from the "GDPR explicit consent". (OBIE view "consent" to mean something closer to permission based on a specific set of terms. In the U.S., simple disclosure or notification is considered as "consent", and there more: "contractual consent", "credential consent" for screen scraping, etc.)

In effect, PSD2 is a non-data-related law using a data term in a different context. Payment legislation also confuses the terminology, with effectively a card transaction triggering a consent for payment and agreement for a transfer of data for SCA.

The relevant regulations should adopt a consistent set of definitions that could include terms such as:

- Consent
- Informed consent
- Explicit consent (PSD2 vs. GDPR)
- Notification
- Agreement
- Permission
- Disclosure

4.5. Going beyond payment accounts

The European Commission's public consultation on Open Finance highlights three sets of data types that are at the center of the Open Finance framework:

- the use of confidential customer data for the purpose of providing financial services;
- data held by financial institutions and other firms provided that it is used for the purposes of providing financial services; and
- access to and reuse of raw data only, as opposed to enriched data.

"Data" referred to in the second bullet point above not only refers to payments but also savings, investments, securities, mortgages, insurance products, pension products as well as data relevant to the risk and sustainability profile of those products. This suggests that the Commission's intention is to create a framework where financial institutions (other than ASPSPs) would give access to non-payment account data.

Today we know for a fact that, much like pre-PSD2, some TPPs already access non-payments account data in contravention with data protection rules via non-regulated channels/technologies (e.g. screen scraping, reverse engineering). The intention therefore would be to move such practices into a "regulated space". From a consumer perspective, we would argue that this may overall enhance the consumer experience, but the consumer might want to see the tangible benefits e.g. compensation for sharing such data (with their consent). That said, there are risks from a privacy perspective, namely, how secure is the consumer's data, does the consumer still have control over their data, and how long will their data be used for with potential third parties. The lawfulness of processing i.e. Art. 6(1)(a) GDPR obtaining consent (and Art.9(2)(a) GDPR explicit consent with respect to certain sensitive personal information) or Article 6(1)(b) GDPR relying on the performance of a contract, not to mention the other data protection principles (purpose limitation, data minimization, accuracy of the data, and indeed the integrity and confidentiality of data) may well present obstacles to the proposed "seamless" Open Finance infrastructure, and should be considered carefully when designing the new framework.

For additional comments we refer to Mastercard's position paper on Open Finance.

Mastercard recommendations:

- **Remove restrictions of articles 66, 3 (g), 67, 2 (f) and 94, 2 of the PSD2;**
- **Failing to do so, allow TPPs to obtain consent (GDPR) for further processing of the data or use different lawful basis such as legitimate interest, execution of the contract, legal obligation, etc.**
- **Clarify that TSPs can process the data for AML/KYC purposes. Eventually on behalf of PSPs;**
- **Include additional authorized processing activities, such as product/service improvement, etc.**
- **Permit the anonymization and aggregation of the data about the transaction, as well as the transaction itself to develop innovative new services and improve existing products/services.**
- **Confirm that TPPs and TSPs can further process so-called Silent Party Data based on the legitimate interest of the data controller, as long as the interests or fundamental rights and freedoms of the data subject are not overridden.**
- **Avoid repeating language from data specific legislations, such as consent, in non-data legislations by giving it a different meaning.**
- **Replace references to "(explicit) consent" in the PSD2 by "agreement", to avoid confusion with the GDPR.**
- **Ensure that data usage rights are appropriately scoped.**
- **Adopt a consistent set of definitions.**
- **Continue to encourage the development of industry-led standards for data sharing and data interoperability, including in the context of European Data Spaces and the work of Gaia-X.**