ETPPA response to EDPB Guidelines 06/2020 on the interplay of PSD2 and GDPR

Brussels, 16-Sep-2020

Introduction and general comments

The interplay of PSD2 and GDPR is a very complex subject, which has caused many concerns by all parties involved and many uncertainties about how to comply with both laws in parallel. Therefore, ETPPA very much welcomes the attempt to provide clarifications around this subject.

As the dedicated industry association representing the interests of TPPs, we would have also welcomed an invitation to the EDPB's stakeholder workshop in February 2019, where the foundations of these draft guidelines were discussed and agreed. TPPs are central stakeholders in this issue and should have been considered as such in this process. Being given just 6 weeks to provide our input now is rather challenging.

For this reason ETPPA would welcome the redrafting of these guidelines, based on the input of a more balanced representation of all relevant stakeholders including a representative TPP organisation. As this topic is crucial to our businesses, the TPP industry remains committed to inform an approach that reflects the realities of the industry, which is very fast pacing. ETPPA would be grateful for a follow-up meeting regarding our response, and going forward we believe it would be essential that the TPP industry is given a seat at the table for these salient discussions on an ongoing basis.

We believe that due to the lacking input of TPPs so far, unfortunately, the current guidelines are based on some incorrect assumptions. This means many of the guidelines, as they stand, are in fact incorrect or not applicable. In response, the TPP industry would like to clarify several of these assumptions to better inform the draft guidelines:

For example, it is a common misunderstanding that PISPs are always providing services to the payer, which is not correct. To the contrary, the PSU of a classic PISP is not the payer, but the payee. These guidelines are also based on this wrong assumption and therefore causing confusion and wrong conclusions. If there is a contractual relationship at all between such a PISP and the payer it would be indirect via their contract with the payee (typically a legal person, i.e. not a data subject) and the payee's contract with the payer, which therefore comes into play as well, albeit only under GDPR obviously. That said, there are also other PISP business models, where the PSU is indeed the payer, which means that both cases have to be considered.

PSD2 defines a payment service user as “a natural or legal person making use of a payment service in the capacity of payer, payee, or both”, and we would recommend to add this under 1.1 Definitions. This differentiation between the roles of "payer", "payee" and "payment service user (PSU)" is not recognised nor considered in several of the proposed guidelines. In this context it should also be noted that a “payment order” is “an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction” according to PSD2 4 (13).

It is very surprising that the focus of these guidelines is on TPPs, rather than all PSPs acting under PSD2. Singling out AISPs and PISPs creates the wrong and very disturbing impression that their processing of personal data causes particular concern, whilst they are normally only processing a subset of the data processed by ASPSPs, which therefore should cause a bigger concern. Similarly, card acquirers are currently much more prominent than PISPs and are processing a much higher volume of data, which therefore should be a bigger concern as well. This narrow view limits competition in financial services, one of the key objectives of PSD2, and is the direct result of TPPs not having been invited as a relevant stakeholder to this group.

Generally speaking it should be understood that applying the proposed guidelines to ASPSPs and their processing of personal data would make banking and payments, as we know it, completely impossible and thereby destroying the basis for providing TPP services at all. Consequently, the initial focus should be on providing guidelines for ASPSPs.

Once reasonable interpretations of PSD2 and GDPR, which allow for a reasonable interplay between the two have been established for the case of ASPSPs, one can then look at TPPs and other PSPs and the additional services they are providing. First and foremost, we must enable ASPSPs to comply with both legislations in parallel when processing personal data in alignment with their users' expectations and data privacy rights.

The principles thereby established for initiating payments and the handling of account information data by ASPSPs themselves could then more easily guide the corresponding services involving TPPs and other PSPs. Let's pick one example, say a payment to a gay club. Do ASPSPs have to know all the legal names of all gay clubs in the world to suspect GDPR-sensitive (special category) data here? Would it make a difference if they knew if their PSU concerned is actually gay or just working there? Or should they better obtain GDPR-explicit consent from the PSU for each credit transfer and direct debit - just in case? Or which other GDPR Art. 9 (2) exception could they use whilst "performance of a contract" is not a valid option for that? And what about corporate PSUs, where personal data does not come into play? Are ASPSPs expected to create completely different setups for consumer and corporate PSUs? Firstly, we must understand how ASPSPs themselves can lawfully process payments potentially involving GDPR-sensitive data at all. Then we can look at the consequences of involving a card acquirer, PISP or AISP into the equation.

These guidelines could easily throw out the baby with the bath water, unless great care is taken. They have to be guided themselves by the reasonable expectations of consumers and thereby squaring the circle of allowing payment services with sufficient convenience, whilst fully complying with both PSD2 and GDPR. We must enable PSUs to consume banking and TPP services in line with their desire and without having to provide GDPR-explicit consent for every single click they make.

The following lists our comments to the specific guidelines we are concerned about:

Re #3

The focus of these guidelines must be on any PSP acting under PSD2. Singling out AISPs and PISPs creates the wrong impression as if their processing of personal data would cause particular concern, whilst they are normally only processing a subset of the data processed by ASPSPs, which therefore should cause a bigger concern.

Re #4

The definition of ‘Payment service provider’ should read "refers to a body".

Re #6

The term "with respect to the user's payment account" should be replaced with "with respect to a payment account". The PSU of a classic PISP is the payee, which means that payments are initiated from "a" payment account (of the ASPSP's user) and received on the PISP's user's payment account.

To clarify the case, we suggest adding another sentence saying: "The PSU of a PISP is usually a legal person, e.g. a merchant.

Re #8

The sentence "Services that entail ... fall under the GDPR." should be deleted, because it is not correct that PSD2 explicitly or implicitly excludes such services from its scope. To the contrary various member states have positively confirmed the opposite.

Re #10

We suggest deleting this part of the sentence as it is obvious and inappropriate to mention, because it suggests non-compliant actions of TPPs.

Re #11

The term "requested by the payment service user" should be replaced with "requested by the payer".

The term "limits the access" should be replaced with "regulates the access", because the whole scope of PSD2 is limited to payment accounts, which means that PSD Art. 67 (2) (d) is a redundant stipulation, and the AISP's access to other accounts is not limited by PSD2. The EBA opinion EBA-Op-2018-04 paragraph 18 also states that “PSD2 is silent on access to other types of information than the information from payment accounts (and associated transactions.”

This conclusion “The latter emphasises … service it provides” goes one step too far. PSD Art 67 (2) (f) allows any AIS service explicitly requested by the PSU. The addition of "in accordance with data protection rules" suggests that AIS services may contain purposes not covered by PSD2, which then must be handled in compliance with GDPR. It is worthwhile noting that this addition was not done in the equivalent article for PISPs, where such other purposes are not expected.

Re #14

The term "are always provided" should be replaced with "are usually provided", because PSD2 does not stipulate such a contract. PSD2 recital 87 establishes that intermediary parties (not regulated under PSD2) are usually involved in payment services and that PSPs should have contracts with these, although PSD2 can only concern contractual obligations between PSU and PSP - if existent.

Re #15

This should be the other way round and read "The establishment of a contract in which parties have access to payment account data of the payment service user is usually a prerequisite for the provision of these services as defined by PSD2". And to clarify an important aspect, the following sentence should be added: "It should be noted, however, that payer and payee are usually two different PSUs, e.g. a shopper and a merchant, and that they may also have a contractual relationship, which comes into play - not under PSD2, but under GDPR."

Re #17

The term "particular aim, purpose, or objective of the service" should read "particular aim(s), purpose(s), or objective(s) of the service" to clarify that a service may well have multiple aims, purposes and objectives.

It would be useful to add the other perspective as well at the end, for example as follows: "On the other hand, some processing can be necessary in this sense, without being obvious to the parties involved. A payment initiation service, for example, will usually provide much more than the actual initiation of a payment and may therefore necessitate more data than necessary for the initiation itself."

Re #22

Again, the conclusion here is going too far. PSD2 is not considered to be lex specialis versus GDPR, i.e. PSD2 in general, nor its articles 66 (3) (g) and 67 (2) (f), could limit a controller's ability to comply with GDPR Art. 6 (4) by processing data for purposes, which are not incompatible with originally agreed ones. PSD Art. 67 (2) (f) even specifically refers to the accordance with data protection rules. Hence, the processing of personal data must be allowed in compliance with GDPR, which includes other lawful grounds than consent as provided under GDPR Art. 6 (1). As explained by yourself in section 3.2, the term “consent” under PSD2 cannot be understood in the same way as defined under GDPR. Also, GDPR recital 50 says “The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required.”

Moreover, it must be noted again that any PSP service, whether offered by an ASPSP, AIS or PIS, can - and usually will - cover multiple purposes from the very outset. It is important not to confuse a simple payment initiation and a simple account information aggregation with a Payment Initiation Service resp. Account Information Service, because the offered "service" is of course much more complex and comprehensive. To pick an example again: a PIS is quite often about not initiating a payment if the risk of non-execution by the ASPSP is deemed too high.

Re #34

It would be important to note and highlight the difference between the stipulation concerning AISPs and that of other PSPs. AISPs do not need PSD2 Art. 94 (2) explicit consent for "accessing, processing and retaining data", but just for their service as a whole as provided in PSD2 Art. 67 (2) (a).

Re #35

The term "in principle" should be replaced with "in many cases".

Re #36

The term "purpose" should be replaced with "purpose(s)" indicating that a service may well cover multiple purposes.

We are not sure what is meant by "explicitly agree to these clauses" or "explicitly accepted by the data subject", but if the PSD2-explicit consent is of a contractual nature and therefore contained in a contract, it would be agreed with the contract as a whole, rather than separately, clause by clause.

Re #37

These interpretations and conclusions are based on previously described misunderstandings. PSD2 Art. 94 (2) applies to ASPSPs and PISPs (not AISPs). Both ASPSPs and PISPs usually obtain the payer's personal data from the payer directly, or from an intermediary, e.g. a merchant, having consent to provide that personal data to the ASPSP or PISP. It is correct, in our opinion, that PISPs should be allowed to access the payer's account to obtain payer-consented data from there, but the EBA is unfortunately of a different opinion, meaning that PISPs have to get the necessary data for initiating a payment, e.g. the payer's IBAN, from the payer directly. Furthermore, classic PISPs usually do not store any payer related data at all, which only leaves the processing of the personal data to be PSD2-explicitly consented.

Consequently, for such PISPs, the "object of the explicit consent under Article 94 (2) PSD" is not "the permission to obtain access to", but just the processing of the personal data. We would agree with the conclusion that "if explicit consent is given by the data subject, the ASPSP is obliged to give access to the indicated personal data", but as stated above the EBA has a different opinion, namely that PISPs do not need access to payment accounts for a PIS, which is probably also based on the misunderstanding that a PIS would just be the simple initiation of a payment.

Re #43

It would be useful to replace the term "payment service provider" here with "payment service provider, who is not an AISPs". AISPs do not need explicit consent for "accessing, processing and retaining data", but just for their service as a whole as provided in PSD2 Art. 67 (2) (a).

Re #47

It would be useful to replace the term "PISPs and AISPs" here with "ASPSPs, PISPs and AISPs" or simply "PSPs", to not create the wrong impression that privacy concerns about silent party data would be specific to TPPs. For example, if there was a concern about displaying silent party data in a consolidated AISP statement, surely the same would apply to the statements of each ASPSP, which the AISP is just consolidating.

Re #49

Once more, we believe that this conclusion is going one step too far. If "the rights and freedoms" of a silent party can be respected by the legitimate interest of the controller with regard to the original purpose, despite "the absence of any relationship with the data subjects that are silent parties", then GDPR Art. 6 (4) (b) can not be given weight to judge the incompatibility of any further purpose either; and the same applies to any other compatibility test element of GDPR Art. 6 (4).

Regarding footnote 28, it should be noted that PISPs often process data of both payer and payee, which means that there is no silent party in such cases.

Re #52

The transaction details of a payment do not allow conclusions about the sensitivity of its data, for which we have already provided some examples. Therefore, we suggest to delete this recommendation, which does not appear to be practical.

Re #55

The processing of data that - under certain circumstances - may qualify as special categories of personal data does indeed mean that PSPs (ASPSPs, AISPs, PISPs and others under PSD2) must ensure that the processing is not prohibited by the provisions of GDPR Art 9 (1).

Although EDPB has identified explicit GDPR consent (Art. 9 (2) (a)) as an alternative, this does not appear to be a feasible basis for a PSP’s processing of GDPR-sensitive data. However, as PSP activities under PSD2 clearly qualify as being of both substantial public interest and systemic importance, the processing of special categories of personal data should meet the criteria of GDPR Art 9 (2) (g). Both PSD2 itself and the national implementations thereof mean that such processing is made on the basis of Union and/or Member State law. Naturally, this applies only if all other criteria of GDPR Art 9 (2) (g) (such as necessity and proportionality) are met as well.

To avoid further uncertainty on this matter we urge the EDPB to elaborate on this as it is critical that all PSPs fully understand exactly what measures are required to achieve GDPR compliance of PSD2 services. A failure to come out clearly on this may result in major disruptions, which in the light of the provisions of GDPR Art 9 (2) (g) cannot be anyone’s objective.

Re #56

We are again puzzled why TPPs are singled out with regard to these obligations? Clearly, all PSPs need such a lawful derogation and the term "TPPs" must be replaced with "PSPs" in this context.

Member States must indeed very carefully look at this issue, because GDPR Art. 9 (2) (a) does not appear to be a feasible basis for an ASPSP's (or any other PSP's) processing of GDPR-sensitive data. Banking, as we know it, can only be sustained if laws fulfilling the criteria of GDPR Art 9 (2) (g) are enacted, unless that is the case already. Any such law must of course ensure that TPPs are not discriminated vis-a-vis ASPSPs or other PSPs, i.e. that they can also use it for the lawful processing of such data.

Re #57

First and foremost, ASPSPs would have to stop their own processing of special categories data in such a case. If GDPR Art. 9 (2) (g) was not an option in a given member state, ASPSPs would have to obtain GDPR-explicit consent for any payment potentially involving GDPR-sensitive data. As explained above, ASPSPs are typically not in a position to affirmatively exclude that potential and therefore would have to get that GDPR-explicit consent for almost any and all transactions.

Since according to the proposed guideline #49 "consent of the silent party is legally not feasible", it appears that this guideline maneuvers us into a complete dead-lock. To repeat once more: this would end banking as we know it. In such a hopefully avoidable scenario, TPPs would also have no other choice, but that is then a rather secondary issue.

“Preventing the processing of certain data points”, as suggested, does not seem to be a feasible solution either. If, for example, a bank would block data related to health care providers' bank accounts, and hence not be able to execute payments to them, they would most likely be in breach of the payment accounts directive.

Re #61

It must be noted here and should be highlighted that the introduction of dedicated interfaces (APIs) for accessing payment accounts has been very counterproductive for data minimisation, because most APIs do not allow granular access to specific data points, as is possible with screen scraping or other direct access methods. Instead most APIs provide lumps of data often containing more than necessary for the specific service of a TPP.

As stated above, we fully agree with your view that “PSD2 requires ASPSPs to share PSU information on request of the PSU, when the PSU wishes to use a payment initiation service”, and would be very grateful if you could convince the EBA of that in order to sustain this claim in here.

Re #62

The more prevalent problem, unfortunately, is that AISPs cannot access all the relevant data, because many APIs do not offer all data available to PSUs directly as they should according to the PSD2/RTS Art. 36 (1) (a) data parity principle. It is understood and agreed that AISPs shall not collect unnecessary data or discard it when delivered by non-granular APIs.

Re #63

Welcome "technical measures that enable or support TPPs" in this sense would be either a) to ban the imposition of non-granular APIs and/or b) allow TPPs direct access via ASPSPs' user interfaces as a generally available alternative. This would allow TPPs to minimise all data handled and collect exactly what is needed for their specific service. As it stands, they are often obliged to obtain PSU consent for data not needed, but unavoidably made available by bad APIs. This by itself is a competitive disadvantage and impediment for the take up of TPP services. Please do not fall for the common misconception that APIs allow more data minimisation than direct access. The opposite is the case.

Furthermore, we strongly recommend avoiding the term and concept of a "filter", because we cannot allow one party filtering the data for another party, which seems to be suggested here. ASPSPs are not in a position to second guess the necessary data for a specific TPP service and then filter out anything else. It is clearly only the TPP who can judge the necessity of any data for their service. The PSD2/RTS Art. 36 (1) (a) data parity principle has been re-enforced by the EBA in their opinion EBA-Op-2018-04 paragraph 18.

Hence, this comes back to the requirement of API granularity, i.e. all data, made available to the PSU directly, must be available via an API, but it should be accessible in a sufficiently granular way so that TPPs can collect exactly what they need and no more. This was actually one of the API Evaluation Group's recommended functionalities (see here RF#4 on page 3), which was strongly supported by TPPs, but not implemented by the API standardisation initiatives due to the resistance of ASPSPs.

Re #64

This guideline is rather misleading. PSD2 obliges the availability of access to payment accounts, but does not prevent the access of other accounts. The purpose of PSD2 is to protect payment accounts more than other accounts, due to their higher fraud risk, rather than less. The access of other accounts does not have these additional restrictions and is governed solely by GDPR and other applicable laws as the case may be. The EBA opinion EBA-Op-2018-04 paragraph 18 also states that "PSD2 is silent on access to other types of information than the information from payment accounts (and associated transactions)."

To avoid the impression that access to other accounts would be illegal the text of this guideline should be replaced with something like "It should also be noted in this regard that the ASPSP's lawful processing ground of PSD2-legal obligation is limited to payment account information. There is no obligation under the PSD2 to provide access with regard to personal data contained in other accounts, such as savings, mortgages or investment accounts. Accordingly, PSPs must ensure that any processing of non-payments personal data is nevertheless done in compliance with GDPR."

Re #77

A PSP's privacy dashboard can obviously only provide information directly accessible to that PSP. An ASPSP could therefore indeed show the "personal data that has been accessed by TPPs", but they can usually not provide an accurate "overview of the TPPs that have obtained the data subject's explicit consent", since that consent would have been given to the TPP, not the ASPSP.

A PSD2-explicit consent must be given to and withdrawn from the same PSP, which is concerned. Giving such consent to a TPP and then trying to withdraw it from an ASPSP would have no legal effect and could not "result in a denial of access".

EBA/OP/2020/10 paragraph 45 suggests that PSUs could request their ASPSP to deny access to one of more particular TPPs. This is different from "withdrawing a specific explicit PSD2 consent" and ASPSPs must still ensure that "any restriction of TPPs' access is done in compliance with the PSD2" and only for "objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account." This means that, apart from fraud cases, such access denial could only be sustained if the PSU has also withdrawn their consent directly from the TPP, because otherwise the TPP's access would still be authorised.

It is therefore misleading to suggest that PSUs could avoid withdrawing their consent from the TPP directly by using an ASPSP provided privacy dashboard. Such dashboards can be useful for reading permissions, but not for revoking permissions. Moreover, it should be noted that they could have unintended consequences leading to major inconveniences for PSUs. For example, an ASPSP dashboard would probably list the legal names of the TPPs accessing their PSU's account, which would rarely be recognised by PSUs normally only knowing brand names. Therefore chances are high that unintended access denials may occur, which would cause big headaches for the PSU until the TPP can regain their consent.

To avoid such laborious efforts it is advisable, as explained above, to refrain from so called read-write dashboards and keep them read-only. Otherwise, PSUs are easily misled, could suffer from complete service outages and would have to spend time and effort to resurrect their service.

This completes our assessment and feedback of the proposed guidelines, and we would like to highlight that we are very grateful for the opportunity to do so!

Please let me repeat our offer for having a follow-up meeting and that we stand ready to advise about TPP concerns and business insights also on an ongoing basis.

Yours sincerely,

Ralf Ohlhausen
Vice-chair
ETPPA - European Third Party Providers Association
Tiensestraat 12, 3320 Hoegaarden, Belgium
www.etppa.org