POSITION PAPER

ESBG Response to the EDPB consultation on the Guidelines 06/2020 on the interplay between PSD2 and GDPR

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

EU Transparency Register ID 8765978796-80

September 2020

ESBG Response to the EDPB consultation on the Guidelines 06/2020 on the interplay between PSD2 and GDPR

The European Savings and Retail Banking Group (ESBG) welcomes the opportunity that the EDPB is providing by collecting feedback on the Guidelines 06/2020 on the interplay between PSD2 and GDPR.

The comments are provided from a Member Banks' point of view. Only the parts that ESBG could comment to as an association of savings and retail are contained in this Position Paper. These comments have been submitted online to the European Data Protection Board.

As a general remark, first, ESBG would like to stress the importance of harmonising the data protection requirements of the two pieces of legislation, as well as with the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication, in order to create more legal certainty for all parties involved, i.e. ASPSPs, TPPs - both PISPs and AISPs -, PSUs, and the competent authorities in each Member State. In addition, ESBG believes that a clearer distinction is needed concerning the differences in consent management and concerning the type of data are in scope. At the same time, however, we strongly believe that retail payment transactions within the Single Market (i.e. the execution of credit transfers and direct debits) should remain easy to perform.

In our view, second, it is also very important to clearly distinguish the respective data protection responsibilities of the various types of payment service providers - ASPSPs, PISPs and AISPs - according to the roles described in PSD2. Pursuant to Article 4(7) GDPR, the controller is obliged to comply with the requirements of the GDPR with regard to the legal basis of data processing (see Article 6 GDPR), the information obligations (Article 12, 13, 14, 21 GDPR, etc.) and the technical-organisational measures for data protection for his own sphere.

Third, we would also like to highlight that PSD2 only regulates access to PSD2-relevant payment account data. Further access to payment accounts or access to non-payment accounts (such as savings, credit, and securities accounts) is not covered by the PSD2 and must therefore be measured exclusively against the relevant regulations (data protection law, copyright, etc.).

Finally, and most importantly, ESBG would like to raise serious concerns about the paragraphs regarding the envisaged data filtering. The current wording of the Guidelines seems to suggest that banks, under PSD2, should apply data filtering with the aim of removing special categories of personal data *before* sharing payment account data with TPPs. Implementation of such filters would have a major impact on the market. Indeed, banks would be charged with unnecessary burdens, both in terms of costs and responsibility. Not only are such *ex ante* filters not technically feasible, but they would also create discrepancies between what PSUs see when using the customer interface compared to when using an AISP. In other words, mandating banks to implement such filters may undermine the full implementation of PSD2, as it would put additional burdens on banks that have already heavily invested to implement dedicated interfaces, thus discouraging the adoption and further development of APIs and frustrating the objectives of PSD2.

The ESBG comments are provided, per relevant paragraph as per the EDPB Guidelines, in the remainder of this document.

I. Introduction

1. The second Payment Services Directive (hereinafter "PSD2") has introduced a number of novelties in the payment services field. While it creates new opportunities for consumers and enhances transparency in such field, the application of the PSD2 raises certain questions and concerns in respect of the need that the data subjects remain in full control of their personal data. The General Data Protection Regulation (hereinafter "GDPR") applies to the processing of personal data including processing activities carried out in the context of payment services as defined by the PSD2. Thus, controllers acting in the field covered by the PSD2 must always ensure compliance with the requirements of the GDPR, including the principles of data protection set out in Article 5 of the GDPR, as well as the relevant provisions of the ePrivacy Directive. While the PSD2 and the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (hereinafter "RTS"8) contain certain provisions relating to data protection and security, uncertainty has arisen about the interpretation of these provisions as well as the interplay between the general data protection framework and the PSD2.

ESBG Comments:

As a general remark, we would like to highlight that the final Guidelines should ensure coherence with existing legislation, including the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication (RTS on SCA & CSC), especially in respect of any new technical requirements.

PSD2 and the GDPR have the same weight under European law and neither of them can be considered *lex specialis*. However, we believe that Article 6(1)(c) GDPR provides a good enough justification for the access and processing of data under PSD2. As a consequence, if personal data is processed when providing payment services, each controller involved must comply with the GDPR on the one hand and the PSD2 and the respective National law on the other:

- Insofar as Articles 66 and 67 PSD2 and the National law transposing PSD2 specifically grant access to payments account data by PISP and AISP, from the point of view of the ASPSP the applicable legal ground is Article 6(1)(c) GDPR. This classification is accurately reflected in the Guidelines (see Chapter 2.4, paragraphs 25 following).
- If a third-party service accesses customer data, it must itself comply with the rules of the PSD2 and the GDPR, while the ASPSP is not required (and actually has no means) to ascertain whether the PSU has given an explicit consent to the TPP.
- PSD2 only regulates certain aspects of data provision by ASPSPs and access to data by TPPs. Apart from that, GDPR fully applies, and each controller must comply with these two pieces of legislation individually. Therefore, we would like to highlight that ASPSPs cannot be held responsible for processes that are solely within the sphere of the third-party service.

3. These guidelines aim to provide further guidance on data protection aspects in the context of the PSD2, in particular on the relationship between relevant provisions on the GDPR and the PSD2. The main focus of these guidelines is on the processing of personal data by AISPs and PISPs. As such, this document addresses conditions for granting access to payment account information by ASPSPs and for the processing of personal data by PISPs and AISPs, including the requirements and safeguards in relation to the processing of personal data by PISPs and AISPs for purposes other than the initial purposes for which the data have been collected, especially when they have been collected in the context of the provision of account

information service. This document also addresses different notions of explicit consent under the PSD2 and the GDPR, the processing of 'silent party data', the processing of special categories of personal data by PISPs and AISPs, the application of the main data protection principles set forth by the GDPR, including data minimisation, transparency, accountability and security measures. The PSD2 involves cross functional responsibilities in the fields of, inter alia, consumer protection and competition law. Considerations regarding these fields of law are beyond the scope of these guidelines.

ESBG Comments:

We would like to clarify that it is not the ASPSP's decision to grant access to the account. Under PSD2, ASPSPs are 'only' mandated to provide an adequate channel for secure communication and authentication functionalities, as well as to execute the payment orders or service requests coming from those channels without discrimination. Instead, it is always the PSU to give their consent to the TTP to access their payment account. ASPSPs' obligations, therefore, do not include any activity which could be considered "granting". Accordingly, we suggest the EDPB amends other sections in the text where the same terminology "granting access to" appears, for instance in paragraphs 25, 26 and 27.

1.1 Definitions

'*Account Information Service Provider*' ('AISP')' refers to the provider of an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;
'*Account Servicing Payment Service Provider*' ('ASPSP') refers to a payment service provider providing and maintaining a payment account for a payer;
'*Data minimisation*' is a principle of data protection, according to which personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
'*Payer*' refers to a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;
'*Payee*' refers to a natural or legal person who is the intended recipient of funds, which have been the subject of a payment transaction;
'*Payment account*' means an account held in the name of one or more payment service users, which is used for the execution of payment transactions;
'*Payment Initiation Service Provider*' ('PISP') refers to the provider of a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;
'*Payment service provider*' refers to a means a body referred to in Article 1(1) of the PSD2 or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of the PSD2;
'*Data protection by design*' refers to technical and organizational measures embedded into a product or service, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects;
'*Data protection by default*' refers to appropriate technical and organisational measures implemented in a product or service which ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed;

'*RTS*' refers to the Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication;
'*Third Party Providers*' ('TPP') refers to both PISPs and AISPs.

ESBG Comments:

The definitions used in the Guidelines depend on the definitions set forth in PSD2. We have noticed that the Guidelines often use the generic term "Payment Service Provider", which addresses different service providers: not only ASPSPs, PISPs and AISPs, but also Card-Based Payment Instrument Issuers that, however, are never mentioned in the Guidelines. In order to increase the comprehensibility and accuracy of the Guidelines, we suggest the EDPB duly identifies the addressee(s) of each chapter/paragraph. Failure to do so could lead to misunderstandings of the respective roles. This is especially true when it comes to Account Servicing Payment Service Providers (ASPSPs). For instance, paragraphs 20 ff seem to primarily target Third-Party Providers; while it is not clear whether paragraphs 36 and 37 relate to ASPSPs or TPPs, or whether some provisions are only addressed to the latter.

1.2 Services under the PSD2

7. AISPs provide online services for consolidated information on one or more payment accounts held by the payment service user either with another payment service provider or with more than one payment service provider. According to recital 28 PSD2, the payment service user is able to have an overall view of its financial situation immediately at any given moment.

ESBG Comments:

On the one hand, we would like to highlight that although Recitals can help to understand and interpret the law, they do not set legal requirements as such. On the other hand, we would like to point out that when the PSU accesses their payment account via a TPP, the customer is not able to "*have an overall view of their financial situation*", as PSD2 only grants access to payment accounts (i.e. savings and mortgages are not in the scope of PSD2).

8. When it comes to account information services, there could be several different types of services offered, with the emphasis on different features and purposes. For example, some providers may offer users services such as budget planning and monitoring spending. The processing of personal data in the context of these services is covered by the PSD2. Services that entail creditworthiness assessments of the PSU or audit services performed on the basis of the collection of information via an account information service fall outside of the scope of the PSD2 and therefore fall under the GDPR. However, accounts other than payment accounts (e.g. savings, investments) are not covered by the PSD2.

ESBG Comments:

We welcome the clarification that data accessed through a PSD2 channel for the purpose of performing a payments service cannot be used for different purposes, unless the PSUs provides an additional consent. However, while mentioning that PSD2 does not apply to accounts other than payment accounts is understandable, this sentence may lead to misunderstanding, as it does not mention GDPR, unlike the preceding sentence.

2 Lawful grounds and further processing under the PSD2

2.3 Lawful grounds for processing

20. Article 6(4) of the GDPR determines the conditions for the processing of personal data for a purpose other than that for which the personal data have been collected. More specifically, such further processing may take place, where it is based on a Union or Member State law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), where the data subject has given their consent or where the processing for a purpose other than that for which the personal data were collected is compatible with the initial purpose.

ESBG Comments:

In our understanding, the explanations in paragraphs 20-24 are directed at TPPs (both AISP and PISP). We suggest the EDPB makes this clear at the beginning of section 2.3, e.g. by adding "Further Processing *(AISP and PISP)*" to the heading of the section.

24. As mentioned in paragraph 20, Article 6 (4) of the GDPR indicates that the processing for a purpose other than that for which the personal data have been collected could be based on the data subject's consent, if all the conditions for consent under the GDPR are met. As set out above, the controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42 of the GDPR).

ESBG Comments:

Similar to our previous comment to paragraph 20, we would recommend the EDPB clarifies that these obligations are imposed on AISPs (and PISPs) only, thus not affecting ASPSPs. Indeed, ASPSPs are not aware of the extent neither of the contract between PSU and TPP nor of the consent expressed by the PSU.

2.4 Lawful ground for granting access to the Account (ASPSPs)

26. The processing of personal data by the ASPSP consisting of granting access to the personal data requested by the PISP and AISP in order to perform their payment service to the payment service user is based on a legal obligation. In order to achieve the objectives of the PSD2, ASPSPs must provide the personal data for the PISPs´ and AISPs´ services, which is a necessary condition for PISPs and AISPs to provide their services and thus ensure the rights provided for in Articles 66(1) and 67(1) of the PSD2. Therefore, the applicable legal ground in this case is Article 6 (1) (c) of the GDPR.

ESBG Comments:

We welcome the clarification in paragraph 26 and 27 that insofar as Articles 66 and 67 of the PSD2 and the national legislation based on these articles specifically permit access to account data by payment initiation services and account information services, then, from the perspective of the account servicing payment service provider, these articles are permissive rules within the meaning of Article 6(1) sentence 1c of the GDPR. This also clearly delineates the scope of obligations between ASPSPs on the one hand and TPPs on the other. While the ASPSPs draw their justification from the law, TPPs can only access the payment account data of the payment service user with the latter's explicit consent.

3 Explicit Consent

3.1 Consent under the PSD2

3.2.1 Explicit consent under Article 94 (2) PSD2

35. As mentioned above, the list of lawful bases for processing under the GDPR is exhaustive. As mentioned in paragraph 14, the legal basis for the processing of personal data for the provision of payment services is, in principle, Article 6(1)(b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. From that, it follows that Article 94 (2) of the PSD2 cannot be regarded as an additional legal basis for processing of personal data. The EDPB considers that, in view of the foregoing, this paragraph should be interpreted, on the one hand, in coherence with the applicable data protection legal framework and, on the other hand, in a way that preserves its useful effect. Explicit consent under Article 94(2) PSD2 should therefore be regarded as an additional requirement of a contractual nature23 in relation to the access to and subsequently processing and storage of personal data for the purpose of providing payment services and is therefore not the same as (explicit) consent under the GDPR.

ESBG Comments:

We welcome this explanation, as it provides an appropriate assessment of the interaction between GDPR and PSD2. The Guidelines correctly conclude that "explicit consent" in the sense of PSD2 must be distinguished from "explicit consent" in the sense of GDPR. From ASPSPs' perspective, it means that, for instance, banks can execute credit transfers and direct debits without the need to obtain explicit consent, as laid down in Article 7 GDPR in addition to the explicit contractual instruction of the payment service user. We believe that a different conclusion would have led to incomprehensible formalisms without any real added value, even from the perspective of the data subject.

36. "Explicit consent" referred to in Article 94 (2) PSD2 is a contractual consent. This implies that Article 94 (2) PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under the PSD2, data subjects must be made fully aware of the specific categories of personal data that will be processed. Further, they have to be made aware of the specific (payment service) purpose for which their personal data will be processed and have to explicitly agree to these clauses. Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject.

ESBG Comments:

Paragraphs 36 and 38 seem to impose on PSPs a duty to collect a separate and specific explicit consent that appears in contradiction with the recognition that the performance of a contract (Article 6(1)(b) GDPR) is the lawful basis for processing in the context of payment services.

Furthermore, paragraph 36 creates the impression that the contractual sphere between the PSP and the customer (data subject) is mixed up with the legal obligations of the PSP to inform the data subject. While the contractual terms and conditions apply in a relationship between (at least) two parties, by being agreed upon, the data protection information is considered to be the fulfilment of a legal obligation by the controller according to Article 12 ff GDPR unilaterally towards the data subject – i.e. without the data subject having to "accept" the information.

In the case of processing in accordance with Article 6(1)(b) GDPR, consent under GDPR can only be required if sensitive data are processed in accordance with Article 9(1) GDPR and no other justification can be considered. In payment transactions, however, Article 9(2)(g) GDPR also comes into consideration.

41. When considered in the context of the additional requirement of explicit consent pursuant to Article 94(2) of the PSD2, this entails that controllers must provide data subjects with specific and explicit information about the specific purposes identified by the controller for which their personal data are accessed, processed and retained. In line with Article 94(2) of the PSD2, the data subjects must explicitly accept these specific purposes.

ESBG Comments:

We believe that information on the specific purposes for processing and retention is already included in the contractual documentation of the payment service and therefore the is no need to add special/specific clauses in the contract.

4 The processing of silent party data

4.2 The legitimate interest of the controller

45. Article 5 (1) (b) GDPR requires that personal data are only collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. In addition, the GDPR requires that that any processing of personal data must be both necessary as well as proportional and in line with the other data protection principles, such as those of purpose limitation and data minimisation.

ESBG Comments:

From our point of view, it is crucial to distinguish between the responsibilities of ASPSPs on the one hand, and those of TPPs on the other. Indeed, from an ASPSP's perspective, all the data the PSU provides, including that of silent parties, is not only necessary to the provision of the payment services, but also mandatory under the payment law (see Regulation (EU) No 260/2012). In this respect, every party of the payment chain needs to process silent party data, otherwise payment orders would not be processable anymore. From a PISP's perspective, the processing of silent party data is also necessary for the provision of its services for the abovementioned reasons. And the same is true for AISPs that need access to all payment account data for the provision of their account aggregation services. Otherwise, AISPs would not be able to offer a proper evaluation of the data for their customers.

On the other hand, we understand the EDPB is concerned that silent party data could be processed for other purposes than payment initiation services and account information services. According to the role model outlined above, however, we would like to point out that ASPSPs have no means to be aware of the contract between the PSU and the TPP, meaning that banks cannot know the purpose for which the TPP asks to access the PSU payment account. As a consequence, banks do not have any obligation to examine and intervene with regard to the legality of a possible secondary exploitation by the AISP in relation to the processing of silent party data, since the responsibility for this data processing lies solely with the AISP.

47. A lawful basis for the processing of silent party data by PISPs and AISPs - in the context of the provision of payment services under the PSD2 - could thus be the legitimate interest of a controller or a third party to perform the contract with the payment service user. The necessity to process personal data of the silent party is limited and determined by the reasonable expectations of these data subjects. In the context of providing payment services that are covered by the PSD2, effective and appropriate measures have to be established by all parties involved to safeguard that the interests or fundamental rights and freedoms of the silent parties are not overridden, and to ensure that the reasonable expectations of these data subjects regarding the processing of their personal data are respected. In this respect, the controller has to establish the necessary safeguards for the processing in order to protect the rights of data subjects. This includes technical measures to ensure that silent party data are not processed for a purpose other than the purpose for which the personal data were originally collected by PISPs and AISPs. If feasible, also encryption or other techniques must be applied to achieve an appropriate level of security and data minimisation.

ESBG Comments:

First of all, we would like to highlight that it is the responsibility of the TPP (as a controller) processing the data on the legitimate interest ground to establish the necessary safeguards mentioned in this paragraph to ensure compliance with GDPR. It is not the responsibility of "*all parties involved*", otherwise it could be argued that also the PSU has a role in safeguarding the interests/fundamental rights of silent parties. Additionally, this paragraph is clear in putting this obligation on the controller, which cannot be other than the TPP once it has obtained access to the PSU's payment account data. As a consequence, it is not the responsibility of *all parties involved*, but that of TPPs only, namely AISPs and PISPs. Moreover, it should also be noted that the provision of account information/payment initiation services does not depend on the existence of a contractual relationship between the PISP/AIPS and the ASPSP (see Articles 66 and 67 PSD2). This excludes the possibility for ASPSPs to exert any control on PISPs and AISPs, who are data controllers in their own right and have their own obligations under PSD2 and GDPR.

Finally, we would also highlight that ASPSPs have to comply with the obligations laid down in PSD2 to provide access to the PSU's payment account data to PISPs and AISPs. In doing so, ASPSPs have also to comply with the RTS on SCA & CSC, which, inter alia, mandate the ASPSP to provide AISPs with an access that would allow them to provide the PSU with the same data they would see by directly accessing their payment account via the ASPSP (see Article 36 RTS SCA & SCS).

4.3 Further processing of personal data of the silent party

49. With regard to further processing of silent party data on the basis of legitimate interest, the EDPB is of the opinion that these data cannot be used for a purpose other than that for which the personal data have been collected, other on the basis of EU or Member State law. Consent of the silent party is legally not feasible, because in order to obtain consent, personal data of the silent party would have to be collected or processed, for which no legal ground can be found under Article 6 GDPR. The compatibility test of Article 6.4 of the GDPR cannot offer a ground for the processing for other purposes (e.g. direct marketing activities) either. The rights and freedoms of these silent party data subjects will not be respected if the new data controller uses the personal data for other purposes, taking into account the context in which the personal data have been collected, especially the absence of any relationship with the data subjects that are silent parties; the absence of any connection between any other purpose and the purpose for which the personal data were initially collected (i.e. the fact that PSPs only need the silent party data in order to perform a contract with the other contracting party); the nature of the personal data involved, the circumstance that data subjects are not in a position to reasonably expect any further processing or to even be aware which controller may be processing their personal data and given the legal restrictions on processing set out in Article 66 (3) (g) and Article 67 (2) (f) of PSD2.

ESBG Comments:

We believe the interpretation offered by the EDPB on the further processing of silent party data is too restrictive, especially considering that the GDPR does not prohibit collecting personal data from another person than the data subject. As a result, the Guidelines should not imply that there is no legal ground, under any given circumstance, for further processing and that the compatibility test under Article 6(4) GDPR cannot offer grounds for further processing. Hence, we think it would suffice if the final Guidelines referred to the accountability principle laid down in Article 24 GDPR.

That would allow the controller, under their sole responsibility, to assess on a case by case basis whether it is possible to further process the data or not.

5 The processing of special categories of personal data under PSD2

5.1 Special categories of personal data

51. It should be emphasised that in some Member States, electronic payments are already ubiquitous, and are favoured by many people over cash in their day to day transactions. At the same time, financial transactions can reveal sensitive information about individual data subject, including those related to special categories of personal data. For example, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes. Trade union membership may be revealed by the deduction of an annual membership fee from a person's bank account. Personal data concerning health may be gathered from analysing medical bills paid by a data subject. Finally, information on certain purchases may reveal information concerning a person's sex life or sexual orientation. As shown by these examples even single transactions can contain special categories of personal data. Moreover, through the sum of financial transactions, different kinds of behavioural patterns could be revealed, including special categories of personal data and additional services that are facilitated by account information services might rely on profiling as defined by article 4 (4) of the GDPR. Therefore, the chances are considerable that a service provider processing information on financial transactions of data subjects also processes special categories of personal data.

ESBG Comments:

As a general remark, we do not agree on the assumption that "*financial transactions can reveal sensitive information about individual data subject*". Actually, financial transactions per se rarely reveal sensitive information about individual data subjects: health information cannot be gathered by analysing financial transactions, as the medical bill containing details of the service provided is not part of the transaction and nothing can inferred by knowing amount and beneficiary; the same is true for purchases that may reveal information concerning a person's sex life or sexual orientation, as the receipt of the order is not part of the transaction (without considering that the purchase itself could be a gift); in the same way, doing charity to an organisation, church or parish does not necessarily imply the data subject shares their particular religious belief. Additionally, in many instances, individuals make payments (even repeating payments) on behalf of family members or other people. As such, it is not possible to reliably determine the individual to which the payment is relevant, as this will not necessarily be the payor. This is even more true with regards to joint payment accounts.

It follows that to extrapolate information about any of the above-mentioned category of personal data from the financial transaction data of a PSU, an appropriate processing has to be intentionally undertaken by the controller. If this is the case, controllers have to apply Article 9 GDPR. Otherwise, if financial transaction data are not processed in order to infer SCPD, Article 9(1) GDPR should not apply. As a consequence, <u>we would welcome a revision of the Guidelines that acknowledges that financial transactions per se do not reveal sensitive information about the individual data subject.</u>

52. With regard to the term 'sensitive payment data', the EDPB notes the following. The definition of sensitive payment data in the PSD2 differs considerably from the way the term 'sensitive personal data' is commonly used within the context of the GDPR and data

protection (law). Where the PSD2 defines 'sensitive payment data' as 'data, including personalized security credentials which can be used to carry out fraud', the GDPR emphasises the need for specific protection of special categories of personal data which under Article 9 of the GDPR are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, such as special categories of personal data. In this regard, it is recommended to at least map out and categorize precisely what kind of personal data will be processed. Most probably, a Data Protection Impact Assessment (DPIA) will be required in accordance with article 35 GDPR, which will help in this mapping exercise.

ESBG Comments:

As specified above, we do not agree on the fact that financial transaction can reveal special categories of personal data per se. As a result, there is no need for a DPIA as laid down in Article 35(3)(b) GDPR.

5.3 Substantial public interest

55. Payments services may process special categories personal data for reasons of substantial public interest, but only when all the conditions of Article 9 (2) (g) of the GDPR are met. This means that the processing of the special categories of personal data has to be addressed in a specific derogation to article 9 (1) GDPR in Union or Member State law. This provision will have to address the proportionality in relation to the pursued aim of the processing and contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Furthermore, this provision under Union or Member State law will have to respect the essence of the right to data protection. Finally, the processing of the special categories of data must also be demonstrated to be necessary for the reason of the substantial public interest, including interests of systemic importance. Only when all of these conditions are fully met, this derogation could be made applicable to designated types of payment services.

ESBG Comments:

We believe PSD2 and the respective National implementation laws constitute a legitimate ground that justifies the processing of data, including special categories of data. Not only does it set up a framework for the provision of electronic payments to the benefit of EU residents and citizens, thus fulfilling the requirement of the substantial public interest, but it also is proportionate, as it provides for suitable and specific measures to safeguard the fundamental rights and interest of the data subject by ensuring transparency and prohibiting any processing of data that is not necessary for the provision of the payment services. All of this notwithstanding, we also would like to point out that the provision of payment services serves in itself interests of systemic importance.

It follows from the above that a suitable derogation exists. Therefore, the processing of special categories of data is absolutely compliant with GDPR.

5.5 No suitable derogation

57. As noted above, where the service provider cannot show that one of the derogations is met, the prohibition of Article 9 (1) is applicable. In this case, technical measures have to be put in place to prevent the processing of special categories of personal data, for instance by preventing the processing of certain data points. In this respect, payment service providers

may explore the technical possibilities to exclude special categories of personal data and allow a selected access, which would prevent the processing of special categories of personal data related to silent parties by TPPs.

ESBG Comments:

Our comment to paragraph 55 notwithstanding, we believe the final Guidelines should clarify that the call for the implementation of technical measures to prevent the processing of special categories of personal data according to Art. 9 GDPR is addressed not to all "Payment Service Providers", but exclusively to AISPs and PISPs, which should be considered the only controllers (in the meaning of GDPR) in this case. In our understanding, the required technical filtering of payment information would be equivalent to a data protection "upload filter". Real-time payments would be excluded in these circumstances and "ordinary" payments would also be at risk. Filtering sensitive data envisaged in the draft Guidelines would undermine payment services law and the functioning of payment transactions if this requirement were aimed at ASPSP. Additionally, the payee could no longer correctly allocate incoming payments. Due to payment services legislative framework, all the data pertaining the customer's payment order, including the specific categories, must be processed in the course of execution of the payment and must be forwarded to the payment service providers engaged for execution.

Pursuant to PSD2, ASPSPs are obliged to provide AISPs with the <u>same</u> information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information (see Article 36(1)(a) RTS). The consequence would be that PSUs would see different information depending on whether they are accessing their payment account via an ASPSP or a TPP. The filtering of the relevant information would be contrary to ASPSPs' obligation and would require banks to hide some data *before* complying with their PSD2 obligation to share all the data with the TPPs. On this matter, we would also welcome further clarification of the meaning of the expression "*certain data points*".

Additionally, it must be emphasised that in concrete it is not always so easy to understand whether a piece of information falls within the list of special categories of data. For instance, a single payment to a trade union may not necessarily show any affiliation/political belief. It can then be argued that it is not feasible for banks to sort out ex ante whether the requested information is sensitive enough to justify the exclusion from the data shared with the TPP, especially considering it mostly depends on how the TPP itself wants to use the data. However, as the EDPB pointed out, the bank is not in a position to know the content of the contract between the PSU and the TPP, so that banks have no means to determine *ex ante* whether certain data should be hidden or not. It is also not clear what would happen if the TPP were to disagree with the analysis carried out by the bank. This would result in excessive burdens for banks, both in terms of economic investment and legal responsibility.

Indeed, pursuant to PSD2, banks have neither an obligation to examine each contract between PSUs and TPPs beforehand, nor a right to intervene for any given reason in the relationship between the PSU and the TPP. The only grounds for refusing access to PSUs' payment accounts are precisely listed by PSD2, so that any other refusal would consist in a breach of EU law and/or National law.

Finally yet importantly, we believe it is not technically feasible for banks to process all the data on a case by case basis to determine whether such information falls within the special categories of data listed by the GDPR, as it also depends on the use made of it, e.g. whether the TPP tries to draw assumptions and interferences combining the data with other information already in its possession. It is also not clear what would happen after a piece of information was found to belong to the list of special categories of data.

Overall, we have the feeling that the current wording of the draft Guidelines puts additional and unnecessary burdens on banks, while the focus should be on the use of data made by AISPs (and PISPs) instead. Accordingly, as mentioned before, we strongly emphasize that the controller is obliged to comply with the requirements of the GDPR and the technical-organisational measures for data protection for his own sphere. Thus, we believe there is no room for imposing additional requirements on banks to prevent a breach of data protection obligation by TPPs.

6 Data minimisation, security, transparency, accountability and profiling

6.2 Data minimisation measures

63. In this respect, the possible application of technical measures that enable or support TPPs in their obligation to access and retrieve only the personal data necessary for the provision of their services could be considered, as part of the implementation of appropriate data protection policies, in line with article 24 (2) GDPR. In this respect, the EDPB recommends the usage of digital filters in order to support AISPs in their obligation to only collect personal data that are necessary for the purposes for which they are processed. For instance, when a service provider does not need the transaction characteristics (in the description field of the transaction records) for the provision of their service, a filter could function as a tool for TPPs to exclude this field from the overall processing operations by the TPP.

ESBG Comments:

We would welcome a better explanation of the principles laid down in paragraph 63. Indeed, this recommendation appears broader than that in paragraph 57, as it is referred to all payment account data, as well as more binding, as it uses the word "recommends" instead of "may". However, we would like to point out, once more, that that these filters, for how we understand they are envisaged, would be discriminatory, as they cannot be implemented by ASPSPs that opted for an adapted interface. In other words, mandating banks to implement such filters may undermine the full implementation of PSD2, as it would put additional burdens on banks that have already heavily invested to implement dedicated interfaces, thus discouraging the adoption and further development of APIs and eventually frustrating the objectives of PSD2.

Unless the EDPB is referring to filters that would allow banks to share data limited to a certain timeframe (e.g. all the data referring to all transactions occurred in the last 15/30/60/90 days), ASPSPs cannot be required to filter the payment account information AISPs may be granted access to. If this were the case, we would welcome further clarity from the EDPB. In this respect, please also refer to our comment to paragraph 57.

6.4 Transparency and accountability

72. With regard to transparency (Article 5 (1)(a) of the GDPR), Article 12 of the GDPR specifies that controllers shall take appropriate measures to provide any information referred to in Articles 13 and 14 of the GDPR. Furthermore, it requires that the information or communication about the processing of personal data must be concise, transparent, intelligible and easily accessible. The information must be in clear and plain language and in writing "or by other means, including where appropriate, by electronic means". The Article 29 Working Party 'Guidelines on transparency under Regulation 2016/679', as endorsed by the EDPB, offers specific guidance for compliance with the principle of transparency in digital environments.

ESBG Comments:

Controllers, meaning both ASPSPs and TPPs, are obliged to provide information in accordance with Article 13(f) GDPR only for their respective areas. An ASPSP, for instance, has no means to be informed about the processing of the accessed payment account data by an AISP. Therefore, it should be specified that the obligation to provide information in this case lies within the duty of the AISP.

For the provision of account information services, the respective AISP shall, with the explicit consent of the account holder, be granted access to his payment account data by the ASPSP. According to Article 67(2) PSD2, it is the sole responsibility of the AISP to obtain the consent of the payment service user and to describe the scope of the access and processing of the data (see Article 67(2)(d) and (f) PSD2). The account holder is thus informed about the kind of data and its purpose processed by the AISP in accordance with Article 13 GDPR.

Due to lack of knowledge, the ASPSP cannot inform the account holder about the data processed by the AISP, especially since there is no contractual relationship between the ASPSP and the AISP (see Article 67(4) PSD2) and there is no joint responsibility in accordance with Article 26 GDPR.

The payment account data accessed by the AISP may also contain "silent party data". Information in accordance with Article 14 (1) and (2) GDPR by the AISP accessing the data is likely to be expendable due to the exceptions in Article 14(5)(b) GDPR and virtually impossible due to missing address information. Article 11 GDPR does not require an investigation. This should be made explicitly clear in the Guidelines.

About ESBG (European Savings and Retail Banking Group)

The European Savings and Retail Banking Group (ESBG) represents the locally focused European banking sector, helping savings and retail banks in 21 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion in corporate loans, including to SMEs, and serve 150 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable, responsible 21st century banking. Learn more at www.wsbi-esbg.org.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ■ www.wsbi-esbg.org

Published by ESBG. September 2020.