16 September 2020

EBF_042474

# EBF response to the European Data Protection Board's consultation on the Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR

**Key points**:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's consultation on the draft guidelines on the interplay of the Second Payment Services Directive and the GDPR.
- The final EDPB Guidelines should **ensure coherence with existing legislation, notably the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication (the RTS on SCA and CSC).** They should also not result in new technical measures, given that the PSD2 (level 1) implementation deadline for member states was 13 January 2018 and the compliance deadline with the level 1 EBA RTS on SCA and CSC for market participants was 14 September 2019.
- It is important to make **a clear distinction between the respective GDPR responsibilities of the payment service providers – ASPSP, PISP and AISP – based on the roles described in the PSD2**. We therefore suggest clarifying at each stage of the Guidelines the addressee(s) of the various obligations.
- In regard to processing of special categories of personal data (SCPD), we doubt the presumption in the Guidelines that financial transaction data are, per se, SCPD. **The Guidelines should recognize that Article 9 (2)g GDPR provides a legal basis for the processing of SCPD to the ASPSP, PISP, and AISP.**
- On further processing under PSD2, the Guidance should be amended to clarify **that AISPs and PISPs can process personal data relating to payments on other Article 6 bases, for example the basis of legitimate interests,** provided this is linked to provision of the core AIS/PIS, and subject to meeting other GDPR requirements. The current interpretation in the Guidelines risks

**European Banking Federation aisbl**

**Brussels /** Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
**Frankfurt /** Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
**EU Transparency Register /** ID number: 4722660838-23

**www.ebf.eu**

preventing a range of legitimate and important data processing activities by TPPs.

- The current proposals on data minimisation measures, particularly the recommendation on digital filters, do not take into account **that it is the responsibility of each PSP, as the data controller, to respect the principle of data minimisation.** The Guidance also does not consider **that filtering would imply interfering with the data to be accessed by TPPs**, whereas the aim of PSD2 is allowing the access to the account information as is. **For ASPSPs using digital filters could result in a breach of legal obligations.**

# EBF position:

The European Banking Federation (EBF) welcomes the European Data Protection Board (hereafter 'EDPB') draft guidelines on the Interplay of the Second Payment Services Directive (hereafter PSD2) and the opportunity to respond to this consultation. While there are elements which the draft Guidance clarifies, for example, the welcome confirmation that explicit consent under Article 94 PSD2 is different from (explicit) consent under GDPR, other elements are more worrying, such as further processing under the PSD2, processing of Special Categories of Personal Data (SCPD) and data minimisation measures. In particular, EBF members are concerned on the lack of coherence in some cases with existing legislation, notably the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication (RTS on SCA & CSC)[1], which could lead to creating further uncertainties instead of resolving existing ones and result, in some cases, a breach of legal obligations on the part of ASPSPs.

The **final Guidelines should ensure coherence with existing legislation, notably the RTS on SCA & CSC[2],** particularly so as to avoid any new technical requirements. It would be useful for the EDPB to discuss this with the European Banking Authority.

Please find below detailed comments. Please note that the titles of each section correspond with the titles in the draft Guidelines.

[1] 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
[2] ibid

## 1. Introductory paragraphs

### a) On the scope

In paragraph 3 (p.4) the text defines the scope of the guidelines as "*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*." Accordingly, we recommend **the Guidelines be amended to clarify when referring to a "controller" whether this relates to AISPs/PISPs or ASPSPs.** In most cases, on our reading, this should be amended to be a clear reference to the PISP and AISP (and not the ASPSP) through the text, except Section 2.4 "Lawful ground for granting access to the Account (ASPSPs)".

In general, in order to make the Guidelines precise and easy to understand, it would be helpful for the EDPB to begin each section/subsection by clearly specifying the exact addressee(s). Otherwise, misunderstandings will arise, especially from the perspective of the account servicing payment service providers (ASPSP). In this regard, we would also suggest that the Guidelines state that the GDPR obligations of AISPs and PISPs do not intend to place any system design obligation on ASPSPs**. It should be clear that AISP and PISP are responsible for their own compliance with the GDPR and have their own individual responsibilities as data controllers**[3]. As soon as ASPSPs grant access to the account following the rules set out in the RTS on SCA & CSC, obligations stemming from the GDPR rest with the AISP and PISPs.

We also note that Card-based Payment Instrument Issuers (CISPs) are not mentioned in the Definitions Section (1.1) or in the document as a whole. We believe it should be defined or we would welcome a clarification from the EDPB as to why CISPs are not included in the text.

### b) Clear terminology

Paragraph 3 (p.4) mentions that "*this document addresses conditions for **granting access** to **payments account information** by ASPSP's*". As such, the ASPSP does not grant access to the account, the Payment Service User (PSU) is the one providing consent to the TTP to access the account. ASPSP's obligations therefore do not include any activity which could be considered "granting". When it comes to PIS and AIS services, the ASPSP is obliged to provide for the TPP a channel for secure communication and authentication functionalities, execute the payment orders or service requests as without discrimination. **For these reasons we would also propose changes to other sections in the text where the same terminology "granting access to" appears**, including:

- Paragraph 25 (p.10-11): "*The effective application of such rights would not be possible without the existence of a corresponding obligation on the ASPSP, typically*

[3] The controller, as defined in Article 4 (7) GDPR, is obliged to meet the requirements set out in the GDPR regarding the legal basis for data processing (Article 6 GDPR), the information obligations (Articles 12, 13, 14, 21 GDPR, etc.) and the technical and organisational data protection measures for the controller's own sphere of responsibility.

*a bank, **to grant** the payment service provider access to the account…*" Suggested change: "to provide"

- Paragraph 26 (p.11): "*The processing of personal data by the ASPSP consisting of **granting access** to the personal data requested by the PISP and AISP".* Suggested change: "to provide".
- Paragraph 27 (p.11):_"*…the obligation for ASPSPs **to grant** access should stem from the national law transposing the PSD2."* Suggested change: "to provide".

We would also suggest clarifying that an ASPSP is not obliged to provide access to such payment accounts which are not accessible online (Articles 66(1) and 67(1) of the PSD2). This could be included at the end of the paragraph 9 (p. 7). Overall, when the PSD2 specific definitions are referred to in the Guidance, we recommend using the terminology of the PSD2. For the accounts subject to PSD2 regulation therefore prefer the expression "payment accounts".

Also in regard to terminology ,in several instances, the text refers to "payment services" and "payment services providers" (e.g. paragraphs 12, 25, 34, 36, 37, 55), which are much wider in scope than PIS and AIS, incorporating for example the processing of payments. The considerations for "traditional" payment services are likely to be very different than for PISPs and AISPs. We would therefore encourage consistency throughout the guidance, and clearly indicating in all the sections/subsections the specific addressee(s).

### c) Additional comments

In paragraph 8 (pp.6), the draft Guidelines state that "*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***." While mentioning that PSD2 does not apply to accounts other than payment accounts is understandable, this sentence may also raise doubts, as it does not mention GDPR, unlike the preceding sentence. As a result, we would recommend clarifying, as is done in the previous sentence for services, that access to information relating to accounts other than payments accounts is covered by the GDPR.

Paragraph 12 (p.7) of the draft Guidance reads "*Depending on specific circumstances, payment service providers could be a controller **or processor** under the GDPR.*" However, PISPs and AISPs would in most cases determine the purposes of processing as set forth by the PSD2 and therefore act as **data controllers**. We therefore believe that AISPs and PISPs would rarely act as data processors when performing AIS and PIS. We suggest modifying the text accordingly.

Finally, EBF members hold reservations on the following text in paragraph 11 "The *latter emphasises that, within the context of the account information services, personal data can only be collected for specified, explicit and legitimate purposes. **An AISP should therefore make explicit in the contract for what specific purposes personal account information data are going to be processed for, in the context of the***

***account information service it provides**."* This section in the guidance risks confusing the basis of processing with the requirement to have a clear contract. In order to prevent such confusion, it would be helpful for this paragraph of the Guidance to signpost the discussion in paragraphs 14 and 15 (p.8) on the basis for processing and explicit consent to the access to the payment account.

## 2. Lawful Grounds and Further Processing under the PSD2

### a) Article 6(1)b of the GDPR (processing is necessary for the performance of a contract)

The legal ground for processing personal data upon accessing the payment accounts by the TPP will mainly be the "necessary for the performance of a contract" between the PSU and TPP. However, other processing grounds may be possible, provided they are applicable.

A distinction needs to be made between possible multiple, compatible purposes in the context of one specific service or contract and the fact that a TPP may be able to offer different services based on the access provided by the bank upon the consent that the PSU has granted to the TPP. Therefore, the reference to the "***main object of the specific contract***" in paragraph 16 (p.9) may lead to the conclusion that in every contract there will only be one service. **This does not take into account that – especially in the context of the contract regarding online services, several services could be included**.

### b) On further processing, under the PSD2

Taking the discussion of i) PSD2 Articles 66(3)(g) and 67(2)(f)[4], ii) the basis for processing under the GDPR and iii) GDPR 'further processing' rules, the draft Guidance seems to imply that the personal data of the PSU (as opposed to silent parties) must be processed on the basis of 'contract' (Article 6(1)b GDPR). Other PSU personal data processing is seemingly only permitted on the basis of 'consent' or 'legal obligation' (Paragraphs 20-24, p.10).

The impact of this interpretation would be that no processing would be possible that could not be considered necessary for the performance of the contract under the strict approach of GDPR (absent 'consent', a legal obligation or legitimate interest). **This would therefore prevent a range of legitimate and important data processing activities by TPPs** (e.g. anonymizing personal data is considered processing, normally based on the legitimate interest of the stakeholder or analytics with the goal of improving the service).

The following considerations need to be taken into account:

[4] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

- While Articles 66(3)(g) and 67(2)(f) PSD2 do constrain AISP and PISP processing, **these provisions do not constrain processing to what is '(strictly) necessary' to provide the AIS/PIS.**
- As with the term 'explicit consent', in our view these limitations should be interpreted more broadly than the GDPR test of being 'necessary'. **In particular, they should not be interpreted as limiting processing to only what can be based on 'necessary for contract', with related processing that has a different basis permitted.** All legitimate grounds for processing provided by the GDPR should be considered valid, also for the further processing of data by TPPs.
- The Guidance also seems to suggest that any processing beyond what is strictly necessary to provide the payment service is 'further processing' and subject to Article 6(4) of GDPR. Yet **a controller can collect certain data for multiple purposes under Article 5(1)(b) GDPR, and these purposes can have different Article 6 bases for processing, subject to meeting the relevant requirements**, such as the legitimate interests 'balancing test' , the transparency obligations under Articles 13 and 14 GDPR, and correctly applying the different data subject rights that exist as a function of the Article 6 basis. For example, the name of the data subject that would like to have a service from a bank or from a TPP will need to be processed because it is necessary to perform the contract, but also to abide by legal obligations to perform customer due diligence. In this case, there are two purposes that exist from the moment the customer data is collected; neither is 'further processing.'
- Article 94(1) PSD2 allows processing for fraud and should therefore be considered as permitted further processing.

Taking together the above, **we recommend amending the guidance to clarify that AISPs and PISPs can process personal data relating to payments on the basis of legitimate interests, and indeed other Article 6 bases provided this is linked to provision of the core AIS/PIS, and subject to meeting other GDPR requirements[5]**.

Similarly, the final guidance should clarify that Articles 66(3)(g) and 67(2)(f) PSD2 only apply to TPPs' data processing in relation to personal data acquired under the PSD2 framework. Data acquired by other means are not subject to these provisions.

More specifically in this section, **we also have strong reservations on the strict interpretation in Paragraph 22 (p. 19) of the draft Guidance that there can be no positive result to a compatibility test under Article 6(4) GDPR. It is the responsibility of the controller, on a case by case basis, to assess whether further processing is possible or not (the accountability principle and Article 24 GDPR).** The Guidance therefore cannot preclude that there can be no positive result to a compatibility test under Article 6(4) GDPR. We would recommend to delete this interpretation from the Guidance, also taking into account the wider consequences it could have for the application of the GDPR.

[5] This should not involve further responsibilities on ASPSPs.

Finally, paragraph 23 touches upon responsibilities under EU Anti-money laundering legislation[6] . We would recommend the EDPB deletes the references to AML matters and customer due diligence as these questions are dealt with in a different for a (e.g. EBA work on Risk Factors). Keeping the references in the final Guidance would result in confusion for ASPSPs, AISPs and PISPs.

## 3. On explicit consent

### a) Explicit consent under Article 94(2) PSD2

Overall, **we welcome the confirmation in the draft Guidance that explicit consent under Article 94 PSD2 is different from (explicit) consent under GDPR**. This is a key point for EBF members, and we strongly support the EDPB confirmation.

Given this confirmation, we are concerned about the statement in paragraph 38 **that consent under Article 94 (2) PSD2 must be "*understood in coherence with the applicable data protection legal framework*".** The intended meaning here is not clear and, in our opinion, seems a potential contradiction that would create additional complexity. We would therefore recommend deleting this reference in the final Guidelines.

### b) Mingling contractual consent with the basis for processing

Despite the correct statement that PSD2 consent is contractual and not related to the basis for processing, there are a number of elements in this section of the guidance which nonetheless mingle these concepts. This risks confusing PSUs.

First, the following section in Paragraph 36 (p.13), raises several questions for EBF members: "*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*."

Through the contract with the payment service provider (and the privacy notice), the data subject is informed about the processing of personal data required for the provision of payment services. Article 52 PSD2 covers all the explicitly required information and conditions of the framework agreement.

**As the consent provided by article 94(2) PSD2 is a contractual consent, it is confusing to refer to an "explicit" agreement or "explicit" acceptance, as these terms could be understood as a reference to GDPR** (where the guidelines clearly state that the two are different). In a contractual consent, terms and conditions are either consented to or not; it is not possible to agree to a contract "unexplicitly."

The **request for the data subject's explicit acceptance/agreement to the specific clauses in the contract therefore seems irrelevant and it is in contradiction with**

[6] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

**the recognition that the lawful bases for processing personal data for the provision of payment services under the GDPR is in principle article 6(1)(b) of the GDPR**. It also seems to create a new legal obligation that follows neither from the GDPR nor from the PSD2. We would therefore recommend deleting this section, or at least clarifying that the "consent in the agreement to the contract as a whole", rather than "explicit consent to specific clauses".

Similarly, in paragraph 41(p.14), the Guidance includes the following "*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***."

However, this information **is already reported in the contract with the PSU** and in information provided under GDPR Articles 13 and 14. **Therefore it does not seem necessary to include a further repetition in any other/additional contractual clauses**. Like with paragraph 36, the Guidance appears to create a new legal obligation that does not flow from either the PSD2 or GDPR. The PSD2 does not say that that PSUs must have "accepted" the different processing purposes.

We would therefore suggest to rephrase paragraph 41, **to specify that the contract's clause about the explicit consent under Article 94(2) need not detail the categories of processed data and the processing purposes, provided that these topics are already included in the contract signed by the customer and/or in other documents related to the contract with the customer.**

### c) Additional comments

Finally, Paragraph 34 in the draft guidelines reads "*Pursuant to Article 33 (2) of the PSD2, this requirement of the explicit consent of the payment service user does not apply to AISPs. However, Article 67 (2) (a) of the PSD2 still provides for explicit consent for AISPs for the provision of the service."* Referring to AISPs and not to PISPs risks introducing a misunderstanding that the requirement would not be necessary for PISPs. We would therefore suggest rephrasing the section to make explicit that Article 94 applies to PISPs.

## 4. On the processing of Silent Party Data

### a) The legitimate interest of the controller

In paragraph 47 (p.15), the draft Guidelines state that "*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."***

The **sections in bold seems to imply that it is necessary for the ASPSP to implement "specific technical measures" for this silent party data** which are different from the other technical measures already put in place by the controller to be accountable and ensure the protection of all data that is processed.

**However, it is the responsibility of the Third Party Provider (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" and particularly of the ASPSP**.

It should also be noted that if the ASPSP were to introduce these types of measures in regard to the data that needs to be made accessible to TTPs, **the risk exists that ASPSPs would infringe their obligations under PSD2.** Inter alia, the ASPSP has to provide access in order for an AISP to be able to provide the PSU with the same data as the PSU can access in the ASPSPs own online customer[7].

Moreover, it should be noted that the provision of account information services or the provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the PISPs and AISPs on the one hand and ASPSP providers on the other[8]. This prevents 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.

**We would therefore recommend specifying this in the text and stressing that the ASPSP is not required to undertake any specific technical measures regarding silent party data that needs to be disclosed to TPPs**. Any further protection of such data falls under the responsibility of TPPs.

### b) Further processing of personal data of the silent party

The position included in paragraph 49 (pp.15-16) with regards to the further processing of the personal data of the silent party is too restrictive. We recall that the GDPR does not prohibit collecting personal data from another person than the data subject. **As a result, the Guidelines cannot set, as an absolute principle, that there will be no legal ground, in any case, for further processing and that the compatibility test under Article 6(4) GDPR cannot offer grounds for further processing**. It is the responsibility of the controller to assess if it is possible or not (the accountability principle and Article 24 GDPR).

The legal basis for such further use should be assessed on a case by case basis by the controllers (the AISP/PISP). The AISP should be able to process the silent party data if it can satisfy the test in Article 6(4) or ground the processing on one of the legal basis set forth in Article 6(1) GDPR.

[7] Article 36, RTS on SCA & CSC
[8] See Articles 66 and 67 PSD2

More specifically in this section, in paragraph 48 (p.15) the reference to paragraph 29 should be replaced with a reference to paragraph 20, which covers "further processing".

## 5. On the processing of special categories of personal data under the PSD2

### a) General comments

There are two points that EBF members would like to stress in regard to processing of special categories of personal data under PSD2:

1. **Financial transaction data is not mentioned under Article 9(1) GDPR as a special category of personal data. It therefore cannot be presumed that financial transaction data are, per se, special categories of personal data (SCPD).**

To extrapolate information about religious beliefs or any other category of the sensitive personal data mentioned in Article 9(1) GDPR, or to observe "behavioural patterns" (as mentioned in paragraph 51, p.17 of the Guidance) from the financial transaction data of a PSU, **processing has to be intentionally undertaken by the controller (with the purpose element in mind).** If this is the case, controllers would apply the conditions proscribed in Article 9 GDPR (explicit consent or the possible derogations). **However, if financial transaction data are not processed in order to infer SCPD, Article 9(1) GDPR should not apply[9].**

Although paragraph 51 (p.17) states that it could be possible to make inferences about health, political affiliation, etc. from payments, records – **it is important to note that this is not evident from the payments data itself**. Payments to medical providers, trade unions, political parties etc., are not necessarily indicative of that individual's health, union membership or political affiliation. In many instances, individuals make payments (even repeating payments) on behalf of family members or other individuals. As such, it is not possible to reliably determine the individual to whom the payment is relevant, as this will not necessarily be the payor. Similarly, payments can be for unknown services that are not related to health, political opinion, etc. For example, recurring payments to a union might be rental payments for shared office space.

[9] We would also like to flag recital 51 of the GDPR in relation to photographs. Under such a recital, "*The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person*". Likewise, only when financial data are purposely analysed to identify behavioural patterns relating to special categories of personal data (e.g. the need to health treatments), the processing of special categories of personal data will occur. Also, such an interpretation if applied to banks would jeopardize their data protection compliance putting them in a situation where compliance cannot be ensured.

**We therefore recommend that the EDPB revises the draft Guidance to state that payments data is not inherently SCPD unless the controller is doing additional processing to derive SCPD inferences.**

2. **Article 9 (2)g GDPR already provides a legal basis for the processing of SCPD for both ASPSP and TPPs**.

We would recommend **to update the Guidance to recognize that Article 9 (2)g GDPR, in any case, already would provide a legal basis for the processing of SCPD to the ASPSP, PISP, and AISP**.

ASPSPs, for their part, **have a legal obligation to comply with a legitimate PSD2 data request from a TPP. As such, any SCPD contained in the transfer is required and this transfer is permitted under Article 9 (2) (g) GDPR on the basis that PSD2 is EU law with a public interest objective** (greater consumer control over data and market competition).

Breaking this down in further detail, Article 9(2)(g) allows processing of SCPD if a set of criteria are satisfied. In our view, PSD2 already meets these criteria:

- Processing must be necessary for reasons of substantial public interest → PSD2 clearly satisfies this criterion, setting up a framework for the provision of electronic payments to the benefit of EU residents and citizens, and encouraging market competition and innovation by opening up access to payments data to new market players.
- The processing must be on the basis of EU or Member State law → PSD2 is EU law, and member states law implementing it is "member state law".
- The processing must be proportionate to the aim pursued, respect the right to data protection and include appropriate safeguards → PSD2 includes numerous provisions to ensure proportionality and protect individuals' rights and interests. In particular:
    - It applies to a specific, tightly defined data set.
    - It contains a detailed framework to ensure transparency and control by customers, such as requiring customer consent (noting that this is not GDPR-style consent) and setting up a legal and technical structure for secure customer authentication and communication.
    - It sets limits on the purposes of data processing.
    - It sets up a regulatory framework for payment services providers, with supervision and licensing by competent authorities.

**We would therefore recommend that the guidance be amended to recognize that Member State laws that implement the PSD2 already provide a legal basis for ASPSPs to provide AISPs and PISPs access to SCPD and for AISPs and PISPs to process SCPD under GDPR Article 9(2) (g) where this processing is necessary to**

**provide a payment service, and that, subsequently, there is no requirement for the ASPSP, PISP, or AISP to obtain explicit consent from the PSU or from the silent party**. In addition, we would like to note that the existence of a public interest was stated by the European Commission during its presentation to the EDPB workshop on the interplay of PSD2 and GDPR (27 February 2019) (in which the EBF participated to).

**b) No suitable derogation**

EBF members have **significant reservations with regards to paragraph 57 (p.18), which suggests that payment service providers, absent a derogation, could implement technical measures to redact SCPD from payment data. Such techniques are hard to imagine being effectively implemented in practice.** Applying any such technique would also first necessarily imply the processing of the account information data to reveal racial origin, or political beliefs or data relating to the health of the data subject. Such processing needs also be carried out on the basis of a derogation. The question is which one would it be?

Furthermore, this kind of redaction would have two negative side effects:

1. Legitimate TPP use cases could be rendered impossible. For example, an AISP that enables customers to organise and classify payments in their transaction record would not be able to function correctly if, for example, payees and / or payors were redacted**. Focusing on the whole, the key objective should be that a user/PSU should experience the same usability and "see" the same data whether the entrance is via a bank or through a TPP.**
2. If an ASPSP were to redact data transferred to TPPs or in some other way prevent their access to data to which they are entitled under PSD2**, the ASPSP would be in breach of its obligations under PSD2. The Guidance should not recommend measures that would force firms to breach their legal obligations.**

It is also important to recall that controllers are accountable according to Article 24 of the GDPR to implement "*appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR*." **It is up to controllers to determine these measures which are not only of technical nature.** As a result, it is confusing to associate this issue – the prevention of processing of special categories of personal data – only to financial transaction data and PSD2 as this issues can arise in other contexts. It is also unclear what is mean by "certain data points" in the paragraph.

We would once more, in general terms, strongly encourage that the final guidelines should not produce new technical requirements for PSPs in addition to the ones already set by the RTS on SCA & CSC and EBA opinions clarifying the RTS.

**c) Additional comments**

In paragraph 52 (p.17), the EDPB states that "*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****."* However, in general, this mapping exercise already takes place when filling in the record of processing activities (Article 30 GDPR), meaning a DPIA should not be required. In addition, and following from our arguments above, financial transaction data are processed for the purpose of payment services and are not "per se" special categories of personal data. As a result, there is also no need for a DPIA as laid down in Article 35(3b) GDPR. We therefore recommend deleting the sentence in bold in the final Guidelines.

In paragraph 55 (p.18), which states that "*the processing of the special categories of personal data must also be demonstrated to be necessary for the reason of the substantial public interest,* ***including interests of systemic importance."*** We would welcome specific examples of "interest of systems importance" as the adjective "systemic" already refers to a particular definition which is specific to the banking sector. In EBF members view, one example of systemic importance could be the maintenance and operation of a modern payment system.

## 6. On data minimisation, security, transparency, accountability, and profiling

### a) Data minimisation measures

#### i. Recommendations on the use of technical measures (including digital filters)

EBF members have strong reservations on the following EDPB recommendations under paragraphs 63 and 64 (p.20):

- Paragraph 63: "*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.****"*
- Paragraph 64: *"Accordingly, under the PSD2,* ***technical measures have to be implemented*** *to ensure that access is limited to the necessary payment account information*".

First of all, the two paragraphs could be interpreted **as ASPSPs having to monitor the data collection by the PSP, restrict access to a particular part of account data relevant to the individual TPP need, and ensure that the PSP only collects the data necessary for the purposes for which they are processed**. **It is the responsibility of each PSP, as the data controller, to respect the principle of data minimisation.**

Second, Paragraph 63 recommends that filters must be established so that the TTP obtains the information it needs, i.e. that it can obtain it categorised. **This is not contemplated in the PSD2 or its implementing regulations**; on the contrary, it is up to the TPP to establish these mechanisms.

Third, the Guidelines insist that only the data necessary for the provision of the service is accessed, **but the PSU has the right and the service provider has the obligation to give him/her access to the same data as when he/she accesses his/her online**

**bank account. Any filtering by the ASPSP would imply interfering with the data to be accessed by TPPs.** PSD2 aims at allowing the access to the account information as is. The use of digital filters by ASPSPs would result in a breach of their legal obligations.

**We would therefore suggest the updated Guidance to include following:**

- Implementing filters can only be successfully done from a data minimisation perspective by TPPs irrespective of the way the TPP retrieves the data at the ASPSP (embedded or re-direct retrieval model- see comments below);
- ASPSP has no knowledge of the business model of the TPP and cannot tailor information to their needs;
- ASPSP needs to respect its obligation under the RTS not to create 'obstacles'[10], so cannot ask the PSU to confirm the consent provided to the TPP;
- ASPSP is obliged in accordance with the RTS to provide the same information to the AISP as the PSU has access to in the online environment.

Overall, the ASPSP does not have to assist the TPPs in their own responsibility or to "control" them. EBF members again emphasize that the Guidelines should not result in new technical measures, given that the PSD2 (level 1) implementation deadline for member states was 13 January 2018 and the compliance deadline with the level 1 EBA RTS on SCA and CSC for market participants was 14 September 2019.

## II. Additional comments on data minimisation measures

**Article 31 of the RTS on SCA & CSC describes two optional techniques to enable TPP's access to a PSU's account.** "*Account servicing payment service providers shall establish the interface(s) referred to in Article 30 by means of a dedicated interface* ***or*** *by allowing the use by the payment service providers referred to in Article 30(1)* ***of the interfaces*** *used for authentication and communication with the account servicing payment service provider's payment services users*." Article 33 of the RTS also describes requirements for contingency measures in the event of unavailability of the dedicated interface (s.c. fallback solution). These measures include the identification of the TPP and use of the authentication method provided to PSU.

When the TPP accesses via a modified user interface or when a TPP uses the fallback solution for the TPP access into account, **an ASPSP cannot put in place technical means that allow the selection of the information to collect.** It is the AISP itself that has to self-limit according to the provisions of Article 36.3 of the RTS on SCA & CSC.

The EDPB's proposal under paragraph 62 (p.20) - "*the IBAN of the silent party's bank account may not need to be displayed*" - would cause an ASPSP to breach its obligations under the RTS as it has to provide to the AISP/PISP all information the PSU has access to in its online banking environment. This includes the IBAN of the silent party. As mentioned previously, in accordance with Article 36 of the RTS on SCA & CSC, the ASPSP has an

[10] Article 32 RTS on SCA & CSC

explicit obligation to provide the AISP with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data, as defined in Article 4(32) PSD2. **We would therefore recommend to delete this proposed requirement, recalling that a user/PSU should experience the same usability and "see" the same data whether the entrance is via a bank or through a TPP**.

Finally, with regards to the following text in paragraph 65 (p.20) "*besides collecting as little data as possible*" we would also like to note that minimisation of data could impact the TPP in regard to the PSD2 objective of providing new, innovative services.

### b) On transparency and accountability

With regards to paragraph 71 (p.21), we understand that these principles should be respected by the PSP who processes the data for its activities under the PSD2 and would encourage the Guidelines to clarify this, also in line with our recommendation in the Introduction, to clearly specify the addressee(s) in the different sections/subsections.

Paragraph 73 (p.20) notes that "*For the services under the PSD2, Article 13 GDPR is applicable for the personal data collected from the data subject and **Article 14 is applicable where personal data have not been obtained from the data subject***" however, for the text in bold, the draft Guidance does not indicate the specific cases the EDPB is referring to **and we would welcome further clarification of these.**

Under paragraph 77 (p.21-22)**, the text suggests the use of a privacy dashboard** to provide information to the individual data subject, noting that such a dashboard "*could provide an overview of the TPPs that have obtained the data subjects explicit consent and could also offer relevant information on the nature and amount of personal data that has been accessed by TPPs*". We recommend that the guidelines clearly indicate that it is not part of ASPSP information obligation under GDPR (or PSD2).

Paragraph 77 further notes that **an ASPSP** "*may offer the user **the possibility to withdraw a specific explicit PSD2 consent through the overview**, which would result in a denial of access to their payment accounts to one or more TPPs.*" **However, the ASPSP is not allowed to interfere in the contractual relationships existing between the user/data subject and TPPs** and it has no contractual relationship with TPPs. **This issue is under the TPPs' scrutiny/responsibility and has to be addressed only in the contractual relationship between the PSU and AISPs/PISPs.**

We would also refer to the RTS on SCA & CSC and the EBA opinion on obstacles under Article 32(3) of the RTS on SCA and CSC[11]. Article 32(3) RTS explicitly mentions additional checks of the consent given by PSUs to AISPs/PISPs as a potential obstacle. Therefore, a general, ex-ante consent required by the ASPSP in order for PSUs to be able to use the AISPs/PISPs' services is an obstacle under Article 32(3) RTS. This does not preclude the possibility for the PSU to request to the

[11] Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC

ASPSP to deny access to their payment account(s) to one or more particular TPPs. In such case, ASPSPs should ensure that any restriction of TPPs' access is done in compliance with the PSD2 including the requirements in Article 68(5) PSD2.

In this regard, we note that in some jurisdictions, approaches have been developed in which a 'dashboard' can be provided, optionally, by ASPSPs. The final EDPB Guidance should not, however, result in formulating a requirement for their imposition in all jurisdictions nor result in an obligation where such dashboard is voluntarily provided by ASPSPs to facilitate the withdrawal of consent.

### c) Profiling

As regards profiling under paragraph 80 (pp.22), the draft Guidance states that "*Likewise, under Article 15 of the GDPR the data subject has the right to request and obtain information from the controller about the existence of automated decision-making, including profiling, the logic involved and the consequences for the data subject, and, in certain circumstances, a right to object to profiling,* ***regardless of whether solely automated individual decision-making based on profiling takes place***." We would like to emphasize that compliance with legal obligations (e.g. AML) or profiling needed for the performance of a contract (e.g. authentication of the payment user) cannot be objected. Therefore, the purposes of the profiling and the legal ground of the processing related to it are essential regarding the right to object, and we recommend acknowledging this in the final Guidelines.

**ENDS**

**For more information:**
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

**About the EBF**

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

**www.ebf.eu @EBFeu**