Bird & Bird LLP
12 New Fetter Lane
London EC4A 1JP
United Kingdom

Tel +44 (0) 20 7415 6000
DX 119 London

twobirds.com

Andrea Jelinek
European Data Protection Board
Rue Wiertz 60
B-1047 Brussels

16 September 2020

Dear Ms Jelinek

**Response to public consultation on EDPB Guidelines 06/2020 on the interplay between GDPR and PSD2 ("Guidelines")**

## 1. Introduction

1.1 Bird & Bird is grateful to the European Data Protection Board ("**EDPB**") for providing the opportunity for Bird & Bird to comment on the important and complex discussion around the interplay between the Second Payment Services Directive ("**PSD2**") and the General Data Protection Regulation ("**GDPR**").

1.2 Bird & Bird has prepared this response to the Guidelines on behalf of numerous clients across the European Union and further afield operating in the financial services sector who seek to understand their compliance obligations under both PSD2 and GDPR.

## 2. Services under PSD2 and processing activities under GDPR

2.1 We agree with the EDPB's analysis set out at in section 1.2 of the Guidelines. We welcome the summary provided by the EDPB on account information services ("**AIS**") and payment initiation services ("**PIS**") offered to payment service users ("**PSUs**") under PSD2.

2.2 We also welcome the analysis of the EDPB set out in paragraph 11 of the Guidelines which draws comparisons, albeit implicitly, between the provisions set out in Articles 66 and 67 of PSD2 and the data minimisation and purpose limitation principles set out in Article 5 of the GDPR.

2.3 In paragraph 8 of the Guidelines, the EDPB expresses that several different types of services can be offered in connection with an AIS, some of which would not be covered by PSD2 but would instead by covered by GDPR.[1]

[1] The EDPB provides the following example:
"*[S]ome 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 performance* ***on the basis of the collection of information via an account information service*** *fall outside the scope of the PSD2 and therefore fall under the GDPR.*" (emphasis added)

2.4 In its discussion at section 2.2 of the Guidelines, the EDPB recognises that multiple services can comprise the overarching service offering to a PSU. In general, payment services providers ("**PSPs**") will process the personal data of a PSU not only to perform the payment services but also for related purposes, such as fraud prevention and detection, security, and risk management, among others. These related purposes could take place under an 'umbrella' of an overall purpose. This is aligned with Opinion 03/2013 on purpose limitation ("**WP 203**") of the Article 29 Working Party.

2.5 **We would welcome confirmation and further elaboration from the EDPB that the processing of the personal data of PSUs can consist of multiple processing activities as described above, each having its own purpose. This is particularly relevant in understanding the applicability of PSD2 for related services and processing operations, specifically for the discussion on lawful basis in section 3 and on further processing in section 4 of this response.**

## 3. Lawful basis for payment services versus related purposes

3.1 We welcome the confirmation from the EDPB of its position set out in its letter dated 5 July 2018 to MEP Sophie in't Veld that reference to consent under PSD2 should be understood to mean contractual consent, which in turn corresponds to processing necessary for the performance of a contract between the PSP and the PSU under Article 6(1)(b) GDPR.

3.2 As set out at in section 2 of this response, payment services can comprise multiple processing operations, including for related purposes to an AIS or PIS. Many of these related purposes would not involve the processing of personal data on the basis of the performance of a contract under Article 6(1)(b) GDPR but most likely under the PSP's legitimate interests under Article 6(1)(f) GDPR. One such example is the processing of personal data for the prevention and detection of fraud.[2]

3.3 While the EDPB recognises at paragraph 17 of the Guidelines that a controller must assess "*whether Article 6(1)(b) GDPR is an appropriate legal basis for an online (payment) service*", **we seek further clarity from the EDPB that related processing activities – which form part of the overall payment service offering but would not form a necessary part of the contract – can be based on another lawful basis under Article 6(1) GDPR.**

## 4. Clarification needed on whether PSD2 is *lex specialis*

4.1 In its letter dated 5 July 2018 to MEP Sophie in't Veld, the EDPB stated that "*the interpretation and implementation of the articles in PSD2* ***have to be made in light of the GDPR***" (emphasis added). The implication of this statement is that PSD2 is not

[2] The EDPB recognised this possibility in its Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects ("**Guidelines 2/2019**") at paragraph 50, in which the EDPB states:
"*…the processing for fraud prevention purposes…is likely to go beyond what is objectively necessary for the performance of a contract with a data subject. However, the processing of personal data strictly necessary for the purposes of preventing fraud may constitute a legitimate interest of the data controller and could thus be considered lawful, if the specific requirements of [legitimate interests] are met by the controller. In addition [legal necessity] could also be a lawful basis for such processing of data.*"

*lex specialis* and organisations must comply with their concurrent obligations flowing from both GDPR and PSD2.

4.2 The EDPB's approach to purpose limitation and compatible processing in section 2.3 of the Guidelines appears to suggest that PSD2 is *lex specialis*. It is unclear from the Guidelines whether the EDPB truly intended for this to be the case.[3]

4.3 **We ask the EDPB to be explicit as to whether PSD2 should be treated as *lex specialis*, subject to the remaining considerations in the points raised below.**

4.4 Even where the EDPB intended for PSD2 to be treated as *lex specialis,* its position is unlikely to be untenable as a matter of law, at least as regards AIS.

4.5 As the EDPB sets out in paragraph 21 of the Guidelines, Articles 66(3)(g) and 67(2)(f) PSD2 provide that the payment initiation service provider ("**PISP**") or the account information service provider ("**AISP**") (indistinctively the third party provider - "**TPP**") may not process data for purposes other than for the provision of the PIS or AIS, respectively. These provisions have a symmetry with the purpose limitation principle set out in Article 5(1)(b) GDPR. In particular, the PIS and AIS correspond to the notion of specified purposes under data protection law, which has been considered by the Article 29 Working Party in more detail in Section III.1 of WP 203.

4.6 Article 67(2)(f) PSD2 specifically provides that an AISP shall not process data for purposes other than performing the AIS explicitly requested by the PSU, "***in accordance with data protection rules***" (emphasis added). This drafting does not appear in the corresponding provision for PIS and should not be considered to be superfluous. Instead, the EU legislator intended for it to be included and therefore its inclusion requires careful consideration. However, at paragraph 22 of the Guidelines, the EDPB treats AIS and PIS equally, considering that the restriction imposed by the provisions in PSD2 "*considerably restrict the possibilities for processing for other purposes, meaning that the processing for another purpose is not allowed*". This effectively disapplies Article 6(4) GDPR and the possibility for a data controller to consider an assessment of compatibility as provided by the GDPR. As a consequence, the personal data returned as part of an AIS can only be further processed where the data subject has given consent or where EU or Member State law otherwise requires.

4.7 In adopting this position, the EDPB reverses several fundamental considerations, some of which the EDPB had previously taken into account in earlier parts of the Guidelines, including:

4.7.1 Any processing of personal data under PSD2 shall be carried out in accordance with the GDPR (recital 89 of PSD2 and recital 4 of the Guidelines).

[3] There is precedent for designated PSD2 as *lex specialis*. The Article 29 Working Party did so in the Guidelines on the right to data portability adopted on 13 December 2016 and endorsed by the EDPB ("**WP 242**"). In WP 242, the Article 29 Working Party explained that "*if the data subject's intention is not to exercise rights under the GDPR, but rather, to exercise rights under sectorial legislation only, then the GDPR's data portability provisions will not apply to this request*" (page 7). WP 242 specifically refers to PSD2, stating at footnote 15:
"*For example, if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in [PSD2] such access should be granted according to the provisions of this directive.*"

4.7.2 PSD2 concerns only contractual obligations and responsibilities between the PSU and the PSP (recital 87 of PSD2 and paragraph 14 of the Guidelines).

4.7.3 The restriction imposed in Article 67 PSD2 must be understood in accordance with data protection rules (Article 67(2)(f) PSD2).

4.7.4 Where there are two legal norms of the same value one cannot prevail over the other and must instead be applied "*on a case-by-case basis and in a manner that* ***reconciles those obligations and strikes a fair balance between them***" (Case C-73/17 *France v European Parliament*, paragraph 42, emphasis added).

4.8 On the basis of the above considerations, it is difficult to see how the EDPB has determined that Article 67(2) PSD2 disapplies an important part of the purpose limitation principle to an entire ecosystem. Such determination certainly does not strike a fair balance between PSD2 and GDPR. It also disregards how the financial services industry processes personal data generally, while also placing the European open banking ecosystem at a disadvantage compared to other countries and regions.

4.9 **We would welcome further clarity from the EDPB in reconciling the above considerations.**

4.10 As set at point 2.3 of this response, the EDPB confirms that, in a typical example, an AISP can use the account information to perform additional processing operations "*on the basis of the collection of information via an account information service*", such as creditworthiness. The EDPB notes that such additional processing operations for related purposes would fall outside the scope of PSD2 and would instead be governed by the GDPR.

4.11 It is unclear from the Guidelines whether the additional processing operation should be considered as further processing as set out at paragraph 22 of the Guidelines. **We would welcome further clarity from the EDPB on the following questions that arise as a result of the current drafting of the Guidelines:**

4.11.1 Are additional processing operations on data derived from an AIS, such as creditworthiness assessments, to be understood to be further processing and therefore only permissible based on the PSU's consent?

4.11.2 Alternatively, are the additional processing operations as described above an original and concurrent purpose of processing within the meaning of data protection law insofar as they form a necessary part of the contract with the PSU as set out in section 2.2 of the Guidelines?

4.11.3 If 4.11.2 is correct, are additional processing operations that consist of related purposes but which are not necessary for the performance of the contract – such as fraud prevention and detection carried out on the basis of the data controller's legitimate interests – to be considered as further processing and thereby automatically incompatible, or can such related purposes be considered to run concurrently with the original purposes?

## 5. Clarification on special category data in the specific context of financial transactions

5.1 We welcome the EDPB's assessment that 'sensitive payment data' under PSD2 does not correspond to special category data under GDPR. However, we are concerned about the EDPB's approach to determining whether financial transactions in fact reveal special category data. Paragraph 51 of the Guidelines states:

> "*…financial transactions can reveal sensitive information about individual data subject* [sic]*, including those related to special categories of personal data.*"

5.2 The Guidelines go on to provide several examples where special category data *may* be revealed in various contexts, such as donations to certain organisations revealing political opinions.

5.3 The EDPB – like the Article 29 Working Party before it – has avoided such a sweeping approach in determining whether the processing of personal data involves special category data. Instead, guidance issued by the EDPB, as well as by national supervisory authorities, favours a nuanced approach commensurate with the *ratio legis* of Article 9(1) and recital 51 of the GDPR.

5.4 For example, as recently as in its *Guidelines 8/2020 on the targeting of social media users* adopted on 2 September 2020 ("**Guidelines 8/2020**"), the EDPB identifies that personal data may clearly fall within the definition of special category data as it would do so explicitly (section 8.1.1 of Guidelines 8/2020). In cases where the personal data is not explicitly special category data, if assumptions or inferences can be made that would reveal special category data, then the data informing such assumptions or inferences could constitute special category data (section 8.1.2 of Guidelines 8/2020). However, the EDPB recognises that a *de minimis* approach is necessary to avoid absurd conclusions, stating at paragraph 115 of Guidelines 8/2020:

> "*For instance, the processing of a mere statement, or a single piece of location data or similar, which reveals that a user has (either once or on a few occasions) visited a place typically visited by people with certain religious beliefs will generally not in and of itself be considered as processing of special categories of data.*"

5.5 There are conceivably few instances where financial transactions would explicitly reveal special category data. Indeed, a payment to a hospital cannot necessarily reveal health data about the PSU because the payment may not relate to medical services or may even be made on behalf of someone else. In any event, it would not be explicit from the transaction itself that the data consists of special category data. Similarly, neither the account servicing payment service provider ("**ASPSP**") nor the TPP would be able to make assumptions or inferences revealing special category data from a single transaction or even a series of transactions. However, in line with guidance from national supervisory authorities, such information cannot reasonably be treated as special category data unless the controller is specifically processing the information to treat someone differently on the basis of the assumption or inference.

5.6 **We would welcome further clarity from the EDPB on the approach to special category data in the context of financial transactions that falls in**

**line with its current guidance, the previous guidance from the Article 29 Working Party, and guidance from the national supervisory authorities.**

## 6. Special category data of silent parties

6.1 Paragraph 56 of the Guidelines provides that where TPPs process special category data of silent parties, then TPPs will be required to obtain the explicit consent of the silent party for the processing of such data where another condition set out in Article 9(2) GDPR – such as substantial public interest under Article 9(2)(g) GDPR – is unavailable.

6.2 However, at paragraph 49 of the Guidelines, the EDPB's position is that obtaining the consent of silent parties is not feasible. It is therefore difficult to see how obtaining the explicit consent of silent parties is feasible (legally or practically).

6.3 **We would welcome further guidance from the EDPB on how PSPs are expected to collect the explicit consent of silent parties for the processing of special category data in the context of an AIS or a PIS.**

6.4 The EDPB proposes that where a condition under Article 9(2) of the GPDR is unavailable, PSPs should consider restricting or filtering access to special category data of silent parties. However, under PSD2 and specifically under Article 36(1)(a) of the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication ("**RTS**"), ASPSPs must grant AISPs access to the same data they make available to the PSU.[4] Consequently, by applying any restriction or filtering as proposed by the EDPB, ASPSPs will directly violate their obligations under PSD2 and the RTS.

6.5 **We would welcome further clarity from the EDPB on how PSPs are expected to filter special category data in line with their obligations under PSD2 and the RTS.**

Yours sincerely,

Bird & Bird LLP

[4] Article 36(1)(a) of the RTS specifically provides that ASPSPs provide AISPs "*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.*"