Revolut

Revolut Ltd
The Columbus Building
7 Westferry Circus
London
E14 4HD
United Kingdom

European Data Protection Board
Rue Montoyer 30,
B-1000 Brussels

16 September 2020

Dear Sirs

Revolut response to Guidelines 06/2020 on the interplay of the second Payment Services Directive and the GDPR ("Guidelines")

Revolut is a financial technology company headquartered in the UK. We provide innovative and market-leading fintech products to more than 12 million customers globally.

We would be grateful for your consideration of our comments.

1. General Comments

The guidance appears to emphasise AISP services rather than PISP services. It would be useful to include more examples in relation to PISP services and recognise the different relationships and data flows that PISP services may involve.

We have noted that the language used to define PISP activity is inconsistent with the PSD2 definition at para 6 of the guidance. Suggest that this is aligned with the PSD2 definition.

2. Processing of Personal Data for the Provision of Payment Services (Article 6(1)(b) of the GDPR (processing is necessary for the performance of a contract))

Relevant Articles of Guidance:

Article 10

Articles 66 (1) and 67 (1) PSD2 determine that the access and the use of payment and account information services are rights of the payment service user. This means that the payment service user should remain entirely free with regard to the exercise of such right and cannot be forced to make use of this right.

Article 11

Access to payment accounts and the use of payment account information is partly regulated in Articles 66 and 67 PSD2, which contain safeguards regarding the protection of (personal) data. Article 66 (3) (f) PSD2 states that the PISP shall not request from the payment service user any data other than those necessary to provide the payment initiation service, and Article 66 (3) (g) PSD2 provides that PISPs shall not use, access or store any data for purposes other than for performing the payment initiation service explicitly requested by the payment service user. Furthermore, Article 67 (2) (d) PSD2 limits the access of AISPs to the information from designated payment accounts and associated payment transactions, whereas Article 67 (2) (f) PSD2 states that AISPs shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules. 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. The contract should be lawful, fair and transparent under Article 5 of the GDPR and also comply with other consumer protection laws.

Article 16

The EDPB guidelines 2/2019 also make clear that, in light of Article 7(4) of the GDPR, a distinction is made between processing activities necessary for the performance of a contract and terms making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract. 'Necessary for performance' clearly requires something more than a contractual clause.15 ***The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur.*** *Merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b) of the GDPR.*

Article 17

Article 5 (1) (b) of the GDPR provides for the purpose limitation principle, which requires that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. When assessing whether Article 6(1)(b) is an appropriate legal basis for an online (payment) service, regard should be given to the particular aim, purpose, or objective of the service. ***The purposes of the processing must be clearly specified and communicated to the data subject, in line with the controller's purpose limitation and transparency obligations. Assessing what is 'necessary' involves a combined, fact- based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal". Article 6(1)(b) does not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject,*** *even if it is necessary for the controller's other business purposes.*

Revolut comment: Articles 16 and 17 are more restrictive than the original PSD2 provisions described at Article 10 and 11. They require not only that the processing of personal data is restricted to processing for the purpose of delivering the relevant payment service, but seek to control the manner of processing such that there is an onus on the payment service provider to compare different methods of processing data to deliver the service and choose the one that is involves the least processing of personal data. This may restrict innovation - for example the user may prefer additional features in an AISP service that involve more processing but overall deliver a better user experience. We would suggest that the purpose limitation is linked to the provision of the PSD2 payment services, rather than further narrowing in a way which may limit innovation.

3. Further Processing (Can AISPs or PISPs further process the personal data accessed in connection with the performance of a payment services contract?)

Relevant Articles of Guidance**:**

Article 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.

Article 21

Articles 66 (3) (g) and 67 (2) (f) of the PSD2 have to be taken into careful consideration. As mentioned above, Article 66 (3) (g) of the PSD2 states that the PISP shall not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer. Article 67 (2) (f) of the PSD2 states that the AISP shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.

Article 22

*Consequently, Article 66 (3) (g) and Article 67 (2) (f) of the PSD2 considerably restrict the possibilities for processing for other purposes, meaning that the processing for another purpose is **not allowed, unless the data subject has given consent pursuant to Article 6 (1) (a) of the GDPR** or the processing is laid down by Union law or Member State law to which the controller is subject, pursuant to Article 6 (4) of the GDPR. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the restrictions laid down in Article 66 (3) (g) and Article 67 (2) (f) of the PSD2 make clear that any other purpose is not compatible with the purpose for which the personal data are initially collected. The compatibility test of Article 6 (4) of the GDPR cannot result in a legal basis for processing.*

Revolut Comment: We have difficulty with the concept that further processing can only take place if the ***data subject has given consent pursuant to Article 6(1) of the GDPR.*** Where the payment services are provided to business customers rather than individuals this leaves no mechanism with which to obtain consent for further processing. In clarifying this issue we would ideally wish to avoid the need to operate different processes for business and corporate customers.

4. Special Category Silent Party Data

<u>Relevant Articles of Guidance</u>**:**

Article 56

In cases where the derogation of article 9 (2) (g) GDPR does not apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR, seems to remain the only possible lawful derogation to process special categories of personal data by TPPs. The EDPB Guidelines 05/2020 on consent under Regulation 2016/679 states[31] *that: "Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore, controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j).* ***When service providers rely on Article 9 (2) (a) GDPR, they must ensure that they have been granted explicit consent before commencing the processing." Explicit consent as set out in Article 9 (2) (a) GDPR must meet all the requirements of the GDPR. This also applies to silent party data.***

Article 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.*

Revolut comment: We recognise the need for the guidance to explore the possible legal basis under GDPR for the processing of special category silent party data in connection with PSD2 payment services. However the content of the draft guidance is causing concern to payment service providers due to the unrealistic nature of some of the explored solutions (specifically, obtaining explicit consent and the suggested technical measures where no other derogation applies). The proposed filtering out of silent party data would appear extremely challenging and potentially inconsistent with AML obligations and disruptive to payment processing generally. In the spirit of what PSD2 was seeking to achieve we suggest it would be helpful if the guidance de-emphasised consent and filtering as possible solutions and emphasised the need for legislative solutions.

5. Data Retention

Relevant Articles of Guidance:

Article 65

Besides collecting as little data as possible, the service provider also has to implement limited retention periods. Personal data should not be stored by the service provider for a period longer than is necessary in relation to the purposes requested by the payment service user.

Revolut comment: We suggest it would be helpful if the guidance addressed data retention in more detail e.g. by including some worked examples and recommended retention periods for the scenarios described.