Ms. Andrea Jelinek
Chairperson
European Data Protection Board
(by email)

Brussels, 27 October 2020

European Payment Service Providers' comments on the EDPB Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

Dear Ms. Jelinek,

Together we as the representative bodies of different European Payment Service Providers, speaking on behalf of the various categories of PSPs under PSD2 and representing the European payments industry, welcome the opportunity given by the European Data Protection Board to participate in the public consultation on the Guidelines 06/2020 on the interplay between the PSD2 and the GDPR. Both through their individual responses and via this joint statement, we wish to ensure coherence not only between the GDPR and the PSD2, but also 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.

In this respect, we believe the final Guidelines should clearly distinguish between the respective data protection responsibilities of the different types of payment service providers that exist – ASPSPs, EMIs, PIs, PISPs, and AISPs – according to the roles described in PSD2. By clearly defining to whom each provision is addressed, the guidance becomes both easier to interpret and implement. Data protection has always been, and always will be, one of the key priorities of the payments industry. At the same time, however, we believe the Guidelines risk imposing obligations on all Payment Service Providers that not only contradict PSD2 but also go beyond what is technically feasible. In this respect, we would like to draw your attention on three main issues.

Special categories of data

As a general remark, we do not agree with the assumption that "financial transactions can reveal sensitive information about an individual data subject". Such an interpretation is overly broad and would have significant unintended consequences in practice. Actually, financial transactions per se rarely reveal sensitive information about individual data subjects. It follows that to extrapolate information about any of the personal data mentioned in Article 9 GDPR from the financial transaction

data of a PSU it is necessary that an ad hoc processing has to be intentionally undertaken by the controller. This is also confirmed by the EDPB Guidelines in the context of social media or profiling, where the EDPB stated that where the data itself is not explicitly special category data, the additional purpose of the processing (such as data analysis, inference or combination), determines whether the processing of special category data takes place. If this would be the case, controllers have to apply all the safeguards laid down in Article 9(1) GDPR. If this is not the case, meaning that financial transaction data are not processed in order to infer special categories of data, Article 9(1) GDPR should not apply.

Silent party data

We understand the EDPB is concerned with the scope of the processing of silent party data. On the other hand, PSUs have a legitimate expectation that relevant details of their payment transactions are considered for account information or payment initiation services, independent of the type of PSP they are using for these purposes. PSPs have no means of knowing about or reviewing the contract between the PSU and other PSPs, meaning that for example ASPSPs cannot know the purpose for which the TPP requests to access the payment account of the PSU. As a consequence, ASPSPs are not allowed under PSD2 and do not have any obligation to examine and intervene with regard to the legality of a possible secondary exploitation by the AISP/PISP in relation to the processing of silent party data, since the responsibility for this data processing and for compliance with GDPR in this context lies solely with the AISP/PISP. We believe that the final Guidelines should clarify this.

In this respect, and due to the lack of contracts between PSPs as per PSD2 and the resulting impossibility for PSPs to exert any control over one another, we also ask that the final Guidelines should clarify that it is not the responsibility of "all parties involved" to "establish the necessary safeguards for the processing in order to protect the rights of data subjects", but that of the party that is concretely processing the data.

Data filtering and data minimisation

Pursuant to PSD2, ASPSPs are obliged to provide AISPs with the same information from designated payment accounts and associated payment transactions made available to the payment service user when this PSU is directly requesting access to the account information (see Article 36(1)(a) RTS). Indeed, pursuant to PSD2, ASPSPs 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 them. The only grounds for refusing access to PSUs' payment accounts are precisely listed by PSD2, so that any other refusal would result in a breach of EU law and/or national law. The filtering of the relevant information envisaged in paragraphs 57 and 63 of the Guidelines would be contrary to ASPSPs' obligation under PSD2 and would require them to hide some data before complying with their PSD2 obligation to share all the data with the TPPs. This would possibly lead to negative outcomes for

consumers, as the legislation gives the consumer the right to access/view the same data through a TPP as when directly accessing via an ASPSP.

Additionally, it must be emphasized that in reality it is not always possible to assess whether a piece of information falls within the list of special categories of data. It is not technically feasible for ASPSPs 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 its use (e.g. whether the PSP tries to draw assumptions and interferences combining the data with other information already in its possession). We believe that mandating ASPSPs to implement such filters would not only be discriminatory, as it would only apply to those ASPSPs that have already heavily invested in implementing a dedicated interface, but it would also undermine full implementation of PSD2, as it would discourage the adoption and further development of APIs, thus frustrating the objectives of PSD2. Under the GDPR each data controller shall undertake its own assessment and determine the scope of data minimisation in relation to the intended purposes and the risks involved. In line with this principle, we would welcome clear acknowledgment that each data controller is responsible for implementing appropriate measures, including data minimisation in respect of its own data processing activities and is not responsible for ensuring it on behalf of other parties.

We would like to emphasize that our individual responses to the consultation contain many more common concerns in addition to the issues listed above. We jointly call upon the EDPB to take our observations into account when finalising these Guidelines.

We thank you in advance for your attention to this matter. We remain at your disposal should you have any question.

Yours sincerely,

Wim Mijs
Chief Executive
European Banking Federation (EBF)

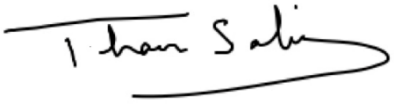
Chris De Noose
Managing Director
European Savings and Retail Banking Group (ESBG)

Hervé Guider
General Manager
European Association of Cooperative Banks (EACB)

Ralf Ohlhausen
Vice Chair
European Third Party Providers Association (ETPPA)

Marcel Roy
Secretary General
European Association of Public Banks (EAPB)

Elie Beyrouthy
Chair
European Payment Institutions Federation (EPIF)



Thaer Sabri
Chief Executive Officer
Electronic Money Association (EMA)

Marc Roberts
Chair
European FinTech Association (EFA)

Robrecht Vandormael
Secretary General
Payments Europe (PE)

CC: John Berrigan, Director-General, DG FISMA, European Commission

CC: José Manuel Campa, Chairperson, European Banking Authority