Partners4Innovation comments in response to the public consultation regarding the Guidelines 06/2020 published by the European Data Protection Board on the interplay of the Second Payment Services Directive and the GDPR.

16.09.2020

General comments

We would welcome some clarification with regards to the scope of the Guidelines. In fact, a number of paragraphs refer to payment service providers in general, whereas others focus on PISP and AISP specifically (e.g. par.15).

We would also recommend defining from the outset the privacy roles of actors involved in the provision of payment services (ASPSPs, AISPs and PISPs). Multiple paragraphs of the Guidelines address the activities of Data Controllers without specifying which of the above actors are being referred to.

The circumstances in which a payment service provider can be qualified as a Data Processor, as mentioned in paragraph 12, are also not clearly defined within the Guidelines.

Furthermore, the Guidelines provide no specific indication as to which categories of personal data the ASPSP is required to give the PISP/AISP access to (e.g. par. 25). This, combined with the fact that, under certain circumstances, data processing for other purposes may occur and that the provision of payment services entails the processing of a set of data necessary for contract execution, calls for a clear identification of the categories of personal data that may be communicated.

Chapter 3: EXPLICIT CONSENT

3.2.1 EXPLICIT CONSENT UNDER ARTICLE 94 (2) PSD2

Par.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

Partners4Innovation S.r.l.
Via Copernico 38, 20125 – Milano
P.I. e C.F. 04841830963
REA: MI – 1776551
Tel.+39 02 92852779
Fax +39 02 93660546
info@p4i.it
www.p4i.it

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 nature 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.

We welcome the intention to clarify the meaning of "explicit consent" under the PSD2. However, the term "contractual consent" may be unclear in the context of national legal systems, thus opening to interpretive ambiguity. We therefore recommend using a different terminology.

Chapter 4: THE PROCESSING OF SILENT PARTY DATA

4.2 THE LEGITIMATE INTEREST OF THE CONTROLLER

Par.46: The GDPR may allow for the processing of silent party data when this processing is necessary for purposes of the legitimate interests pursued by a controller or by a third party (Article 6 (1)(f) GDPR). However, such processing can only take place when the legitimate interest of the controller is not "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".

In view of the fact that the *silent party* may be unaware of the processing carried out by the payment service provider (in its capacity as Data Controller) and that there may therefore be no relationship with the latter, it is not possible to assess the requirement of "reasonable expectations" regarding a given processing activity as required by Recital 47 of the GDPR.

4.3 FURTHER PROCESSING OF PERSONAL DATA OF THE SILENT PARTY

Par.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.

In absence of an adequate lawful basis for further processing of the *silent party* data, the anonymization of such data should be carried out. It would also be appropriate to establish whether such provision also extends to ASPSPs.

Chapter 5: THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA UNDER THE PSD2

5.1 SPECIAL CATEGORIES OF PERSONAL DATA

Par.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.

We recommend that the duty of mapping out and categorising precisely what kind of personal data will be processed is placed on PISPs and AISPs.

5.2 POSSIBLE DEROGATIONS

Par. 54: It should be pointed out that the list of derogations in Article 9 (2) GDPR is exhaustive. The possibility that special categories of personal data are included in the personal data processed for the provision of any of the services falling under the PSD2 must be recognised by the service provider. As the prohibition of Article 9 (1) GDPR is applicable to these service providers, they must ensure that one of the exceptions in Article 9 (2) GDPR is applicable to them. It should be emphasised that where the service provider cannot show that one of the derogations is met, the prohibition of article 9 (1) is applicable.

The Guidelines should specify that the burden of proof as to the admissibility of the derogations to Article 9(2) GDPR for payment service providers lies solely with PISPs and AISPs as Data Controllers.

5.4 EXPLICIT CONSENT

Par. 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 states31 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.

A discrepancy is detected in relation to the provisions of paragraph 49, according to which: "...*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*...". It is therefore necessary to clarify how explicit consent for the processing of special categories of data related to such subjects can be applied in this paragraph.

Chapter 6: DATA MINIMISATION, SECURITY, TRANSPARENCY, ACCOUNTABILITY AND PROFILING

6.2 DATA MINIMISATION MEASURES

Par. 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.

Regarding data collection activities carried out by TPPs, we would welcome more specific indications about which types of data ASPSPs may share with AISPs and which types should be excluded, thus supporting the implementation of appropriate digital filters and the definition of the corresponding liabilities. Considering the principle of technological neutrality established by PSD2, it would also be useful to clarify the nature of digital filters as mentioned within the Guidelines, as we detect a risk that such filters may interfere with the duty of ASPSPs to provide access to user data.