EuroCommerce for retail & wholesale

Contribution

13 August 2020

EuroCommerce 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 version 10.

In general, we could suggest including more examples on PIS through the document.

Chapter 2: LAWFUL GROUNDS AND FURTHER PROCESSING UNDER THE PSD2

Point 26: The processing of personal data by the ASPSP consisting of granting access to the personal data requested by the PISP and AISP in order to perform their payment service to the payment service user is based on a legal obligation. In order to achieve the objectives of the PSD2, ASPSPs must provide the personal data for the PISPs´ and AISPs´ services, which is a necessary condition for PISPs and AISPs to provide their services and thus ensure the rights provided for in Articles 66(1) and 67(1) of the PSD2. Therefore, the applicable legal ground in this case isArticle6 (1) (c)of the GDPR.

We welcome some clarification for ASPSP but would appreciate additional clarification for PISP and merchants with personal data, for example is the IBAN or proxy of IBAN (phone number, email), consumer names being considered as personal data or sensitive data in PSD2/GDPR and how they should be processed in PISP and in merchants POI environments.

Chapter 3: EXPLICIT CONSENT

Point 37: Central to the notion of "explicit consent" under Article 94 (2) of the PSD2is the gaining of access to personal data to subsequently process and store these data for the purpose of providing payment services. This implies that the payment service provider is not yet processing the personal data, but needs access to personal data that have been processed under the responsibility of any other controller. …/…

Point 43: Explicit consent under the PSD2 is different from (explicit) consent under the GDPR. Explicit consent under Article 94 (2) of the PSD2 is an additional requirement of a contractual nature. When a payment service provider needs access to personal data for the provision of a payment service, explicit consent in line with Article 94 (2) of the PSD2 of the payment service user is needed.

We welcome the clarification on explicit consent between PSD2 and GDPR.

Chapter 4: THE PROCESSING OF SILENT PARTY DATA

Point 47: A lawful basis for the processing of silent party data by PISPs and AISPs - in the context of the provision of payment services under the PSD2 - could thus be the legitimate interest of a controller or a third party to perform the contract with the payment service user. The necessity to process personal data of the silent party is limited and determined by the reasonable expectations of these data subjects. 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. If feasible, also encryption or other techniques must be applied to achieve an appropriate level of security and data minimisation.

We would welcome a clarification on how the processing of personal data could/should be done.

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

Point 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 welcome the clarification of the differences in meaning between GDPR sensitive personal data and PSD2 sensitive payment data.

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

Point 61: The TPP accessing payment account data in order to provide the requested services must also take the principle of data minimisation into account and must only collect personal data necessary to provide the specific payment services requested by the payment service user. As a principle, the access to the personal data should be limited to what is necessary for the provision of payment services. As has been shown in Chapter2, the PSD2 requires ASPSPs to share PSU information on request of the PSU, when the PSU wishes to use a payment initiation service or an account information service.

Point 62: When not all payment account data are necessary for the provision of the contract, a selection of the relevant data categories must be made by the AISP before the data are collected. For instance, data categories that may not be necessary may include the identity of the silent party and the transaction characteristics. Also, unless required by Member State or EU law, the IBAN of the silent party's bank account may not need to be displayed.

We would welcome an example on a PIS service that would clarify the status on information, such as IBAN/proxy of IBAN and customer ID, to be provided by PSU/ASPSP to PISP to perform PIS at POI.

Point 69: Controllers are obligated to take adequate measures to protect the personal data of data subjects (Article24 (1) GDPR). The higher the risks associated with the processing activity carried out by the controller, the higher the security standards that need to be applied. As the processing of financial data is connected to a variety of severe risks, the security measures must be accordingly high.

We would welcome more clarity on what qualifies as a high risk in a PIS domain. What is the definition of high or severe risk? How should low value proximity payment information be processed?

~ End ~