16/09/2020

EFA Input on EDPB Guidelines on the interplay of PSD2 and the GDPR

Introduction

EFA welcomes the Guidelines' clarification as to the lawfulness of processing data for other purposes than the ones set out in the PSD2 (see below under 1). However, in EFA's opinion, the Guidelines need to further clarify technical measures and information requirements in regard to data of Silent Parties (see below under 2).

1. Data of the User: Processing for different purposes

The Guidelines acknowledge the new payment services and the business models that are enabled through them: Payment initiation service providers ("PISPs") and account information service providers ("AISPs"; PISPs and AISPs together "TPPs") can request account servicing payment services providers ("ASPSPs"), usually banks, to initiate transactions or to transfer account information of a payment service user ("User"). The TPP can offer services to the User such as initiating a payment transaction, giving an overview over bank accounts held by different banks, providing budget planning, monitoring services, as well as services that entail creditworthiness assessments of the User.

The Guidelines establish much needed clarity regarding the different types of services offered in respect to account information data. These services range from budget monitoring to creditworthiness assessments and have different requirements regarding lawful processing; some types of processing are covered by the PSD2 while other types of processing fall under the GDPR.

The distinction between services covered by the PSD2 and "further processing" is relevant and helpful: "Further processing" requires an explicit consent within the meaning of the GDPR (Art. 6 (1) (a) GPDR); whereas processing for services covered by the PSD2 requires a contractual consent within in the meaning of Article 94 (2) of the PSD2.

2. Personal data related to Silent Parties

When processing account information, TPPs will frequently process data of Silent Parties, e.g. displaying the identity of the recipient or the payer of a wire transaction. To acknowledge this, the Guidelines should clarify that Silent Party Data has to be processed in order to provide AIS and PIS services. TPPs need to have access to the full set of account information, otherwise they cannot provide services as payment overview and categorization in compliance with the PSD2.

In EFA's opinion, the Guidelines may lead to a significant impediment of the service provision because they lack clarity regarding the requirements for processing of special categories of personal data 2 ("Sensitive Data") related to Silent Parties.

EFA | European FinTech Association a.s.b.l
Rue Washington 40
1050 Brussels, Belgium

Commercial/Association register number: 0741.453.152
EU Transparency Register: 514240237898-38

www.eufintechs.com
admin@eufintechs.com

Hence, we recommend clarification regarding the following two topics:

- **Clarification regarding digital filters**

The PSD2 introduced an open banking standard that is governed by regulatory technical standards that are considered to be exhaustive when it comes to the requirements for the data transfer between ASPSPs and AISPs / PISPs.

The EDPB's Guidelines recommend the usage of "digital filters" in order to support TPPs in their obligation to only collect personal data necessary for the purposes for which it is processed.

In EFA's opinion, the requirement of a digital filter is misleading in a way that it might include an obligation of the ASPSPs to only share certain data or data points with TPPs under PSD2.

Such a requirement would bring an enormous amount of legal uncertainties to the ASPSPs as they might no longer be able to rely on and comply with the standards set out in the PSD2 and RTS.

Therefore, the Guidelines need to clarify that the transfer of data from the ASPSPs to the TPPs always meet the requirements of Art 9 (2) (g) GDPR.

While the transfer of the account information to TPPs has to be considered legal under Art 9 (2) (g) GDPR, it could be clarified that the receiving party is obliged to implement and uphold security measures that prevent the misuse of Sensitive Data of Silent Parties. TPPs are able to implement measures that fit the respective business requirements: If it is the AISP's business model to display account information, all account information needs to be displayed to the User; however, if an AISP only shows aggregated account information data or conducts creditworthiness assessments, then the AISP might be obliged to filter out any Sensitive Data of a Silent Party.

However, it is very important that only the TPPs are obliged to implement security measures, not the ASPSPs. Under the PSD2, ASPSPs are legally obliged to provide account information upon request, they do not have the right to decide on which account information is transferred to the TPPs, and consequently are not allowed to implement digital filters.

- **Clarification regarding information requirements**

The Guidelines clarify that a processing of personal data of Silent Parties is possible under the PSD2.

However, further clarification is needed that neither the ASPSPs nor the TPPs have an obligation to inform the Silent Party of the processing. It should be clarified within the Guidelines that the Silent Parties do not need to be informed according to Art. 14 No. 5 (b) GDPR ("provision of such information proves impossible or would involve a disproportionate effort").