Lobbying - EDPB : guidelines 6/2020

Introduction

Budget Insight welcomes the opportunity to comment on the EDPB guidelines on the interplay of the Second Payment Services Directive and the GDPR. We would like to express our support for the project to clarify the interplay and bring more transparency for AIS *-account information service-* and PIS *-payment initiation service-* end users.

As a preliminary point, it should be noted that AIS and PIS could be provided as Business to Business to Consumer services and not only as Business to Consumer, thus adding a party to the processing of collected data.

Budget insight has some fundamental general concerns on the implied requirements to obtain adequate consent and does therefore in the first part of this response raise questions on definitions of some terms and resulting understanding.

In the second part, Budget Insight comments on the prevention of processing of special categories of personal data if no suitable derogation is met.

I. Lack of precision in a specific context of a TPP providing services in B2B

According to the Article 6 (1) (b) processing shall be lawful if 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; and Article 7(4) of the GDPR, a distinction is made between processing activities necessary for the performance of a contract and accessory activities which are useful but not necessary.

The EDPB considers that 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.

The provision of payment services by a TPP like Budget Insight includes processing which could be considered as necessary to access the PSU data. According to the lack of precision, all the features developed by Budget Insight in order to give to the PSU a smooth user experience are not covered by the Article 6 (1) (b).

Does that mean for every feature a consent should be collected even if these features are more than useful for our client in B2B and the PSU? These definitions “necessary” and “useful” are extremely important and dangerous for Budget Insight activity if they are not defined knowing this type of activities.

Moreover, the EDPB maintains that “the contracts cannot artificially expand the categories of personal data or types of processing operations” and addresses cases in which “take it or leave it” situation may be created. Budget Insight can provide for its clients several services (account information, payment initiation) in the scope of PSD2, which can be performed independently of one another.

In this situation, how can Budget Insight continue to provide those services without making more heavier the PSU experience. The notion of “take it or leave it” has to be defined in the context of the TPP, and B2B.

II. Preventing the process of special categories of personal data when no suitable derogation is applicable

As indicated and according to article 9 (1) GDPR sensitive data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or data concerning a person’s sex life or sexual orientation should not be processed. On paragraph 57, it is suggested that the “payment service providers may explore the technical possibilities to exclude special categories of personal data”. However, as an AISP it is expected from an end-user that Budget Insight provides unaltered information regarding the account which consent was given. Counter-intuitively, the requirement to exclude special categories would require that an end-user would do a positive act for information to be provided. Also, it would require a prior consent in order for a TPP to act on the technical exclusion of special personal data.

Moreover, ASPSP and TPP are regulated and process similar information, it would be an unbalanced application of the regulation to require AIS providers to exclude special personal data. Moreover, in almost all cases the bank is best placed to undertake the appropriate step to hide a label that would provide information on special personal data as it can undertake additional checks and monitor transactions.

If a technical exclusion should be provided by AISP, these additional algorithms, would difficulty run in real time and therefore either provide a delayed information or subtract information ex post. The technology to exclude those information would either rely on keywords available in the label of a transaction or in case of PIS on the IBAN. In case of reliance on IBAN, this would imply that PISP should maintain a list of IBAN regarding church, political parties … that would be difficult to obtain and to justify in regard to GDPR. Reliance on keywords would be tedious as today there is no framework to identify special personal data. Also, there would be a learning curve implying false positives that would deter customers from AIS because it makes it difficult to rely on altered information, especially for online accounting and money management products. It would also be an onerous and disproportionate compliance cost that would negatively impact competition and customer choice and convenience.

Regarding AISP and PISP AML/CTF requirements, the exclusion of special personal data would undermine the quality of reporting suspect operations to national competent authority.

Conclusion regarding special personal data

An AISP only holds and shares data made available by ASPSP. It does not monitor transactions unless explicitly required by customers as PSD2 states that AISP should provide its service with minimal processing. To require AIS to unprocess special personal data would be in violence of the PSD2 light touch requirement. ASPSP are better placed to carved out special personal data from account information. Moreover, the additional cost of the technical exclusion would disproportionately burden AISP and PISP and may alter the quality of a suspect transaction report.