POLISH BANK ASSOCIATION

Polish Bank Association's comments on the European Data Protection Board's "Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR"

Warsaw, September 2020

Introduction

Polish Bank Association welcomes the proposed *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR* (hereinafter referred to as the "Guidelines") as a mean for providing further guidance on data protection aspects in the context of the PSD2, in particular on the relationship between relevant provisions of the GDPR and the PSD2.

At the same time, Polish Bank Association would like to use the ongoing public consultation as an opportunity to comment on the Guidelines and present its following remarks.

Comments on the Guidelines

The Guidelines indicate that *"(...) Articles 66(5) and 67(4) of the PSD2 state clearly that the provision of payment initiation services and of account information services shall not be dependent on the existence of a contractual relationship between the PISP/AISP and the ASPSP"* (chapter 2, section 2.4, paragraph 25, page 11).

The Guidelines further state that *"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 is Article 6 (1) (c) of the GDPR"* (chapter 2, section 2.4, paragraph 26, page 11).

At the same time, the Guidelines also refer to Article 9(1) of the GDPR, which prohibits the processing of *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"* (chapter 5, section 5.1, paragraph 50, page 17).

As it is indicated in the Guidelines, *"(...) financial transactions can reveal sensitive information about individual data subject, including those related to special categories of personal data. For example, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes. Trade union membership may be revealed by the deduction of an annual membership fee from a person's bank account. Personal data concerning health may be gathered from analysing medical bills paid by a data subject"* (chapter 5, section 5.1, paragraph 51, page 17).

As regards the term "sensitive payment data", the Guidelines indicate that according to the EDPB *"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"* (chapter 5, section 5.1, paragraph 52, page 17).

In this regard, the Guidelines recommend *"at least mapping out and categorizing precisely what kind of personal data will be processed"* (chapter 5, section 5.1, paragraph 52, page 17).

Having in mind the abovementioned statements, Polish Bank Association suggests that the Guidelines should further specify whether ASPSP – when providing AISP and PISP with information containing sensitive data – would be obliged to conceal such information by, for example, blurring them or deleting part or whole transaction description, alternatively – whether it would be obliged to assess if it has adequate consent of the data subject.