SPARKASSE
Verband Österreich

Response to the EDPB consultation 06/2020 on the Guidelines on the interplay between PSD2 and GDPR

The Austrian Savings Banks Association welcomes the opportunity to provide the EDPB with our response to your draft Guidelines on the interplay between PSD2 and GDPR:

No. 3 Please clarify whether the Guideline applies to all payment services pursuant to Annex 1 PSD2, or solely to the newly created payment services pursuant to Annex 1 numbers 7, 8 PSD2.

No. 12 For the sake of legal certainty, please provide examples under what circumstances a payment service provider could be regarded as a data processor. It is our strong believe that a financial service provider can never be regarded as data processor, if and as long as it provides services under a license issued by a financial markets authority and renders these services within the statutory framework of a financial regulatory law. It is not up to the data subject to determine the purposes and means of this processing.

No. 15 It is not clear what is meant by the second sentence. Please amend.

No. 28-43 We are aware that Art 94 (2) PSD2 expressly states the requirement of an "*explicit consent*". Still, we want to take the opportunity to point out the irrationality of this clause and its incongruity within the context of Union law:

- The provision of payment services is a regulated financial service.
- Payment service providers (PSP) need to obtain a license issued by the relevant national competent authority and are subject to their monitoring.
- The legal relation between PSPs and payment service users (PSU) is mainly regulated by PSD2. The technical components for the provision of payment services is regulated, among others, by the SEPA-regulation (260/2012/EU), the SEPA-Credit Transfer Rulebook (issued by the European Payments Council) and the Regulation on the Transfers of Funds (2015/847/EU).
- This tight regulatory corset does not leave room for any deviations by single PSPs – on the contrary: the "inflexible", schematic and heavily standardizes payment infrastructure is the reason why it is possible to transfer money within one day (or within seconds in the scope of SEPA INST) throughout the whole European Union. Before this standardization, it took an average of 4,6 days to transfer money.

- If a PSU wants to make use of fast and reliable payment services, he/she has no other choice than to get into a contractual relationship with a licensed PSP.
- The amount of personal data which gets processed for the provision of payment services is also regulated and standardized (see for example https://www.stuzza.at/en/payment-transactions/payment-transfer-formats.html).
- All this is regulated by law, industry standards and framework contracts. It is counterintuitive why the PSU has to provide an additional "consent", **to something that is not even up to his/her discretion**. If the PSU does not "consent" to the processing of his/her data, he/she simply cannot make use of the payment services. There is no legal or factual way to render payment services (i.e. open an account, transfer money, etc) without the processing of personal data. A "forced" consent would also have **detrimental effects for the general public's understanding of GDPR**, because one of the main concepts of a consent ("freely given") would suddenly be scrapped when it comes to payment services.
- In addition, the access to a payment account is an enforceable right within the EU (Art 15, 16 Directive 2014/92/EU). Making the access to an account or the rendering of basic payment services conditional to a consent, runs counter to Directive 2014/92/EU.
- In the light of all this, it is our strong believe that it is sufficient to provide the PSU with the *information* that and which of his/her data is processed when making use of payment services. **The PSU does not have to "consent" to the processing, if the processing of personal data is necessary for rendering payment services**.

No 50-57 We are aware of the high standards the GDPR sets for the processing of sensitive data. However, please consider the practical consequences of this specific part of the guideline:

- Data qualifying as "sensitive" in the sense of Art 9 GDPR can only occur while processing payment services if the PSU actively chooses to do so: (1) Either by his or her choice of words in the free-text-fields provided in the payment reference etc or (2) by means of the quality of the beneficiary of the payment (i.e. the recipient).
- However, (2) is not as clear as it seems at the first instance: If, for example, a PSU were to transfer money to a "Cancer Treatment Center", this alone does by no means reveal any sensitive data. Maybe he/she is in perfect health and participated at a workshop or an awareness program hosted by the Center; maybe he/she donated the money. Another example: If a PSU were to transfer money to a Political Party, it may be the exact opposite of his/her revealing his/her political beliefs: Maybe he/she lost a defamation battle in court *against* the Political Party (i.e. they represent *not* his/her beliefs) and now has to pay damages. The list of examples goes on.
- Regarding (1) – free text fields – there remains ambiguity as well.

- If a male PSU transfers money to another male PSU and chooses “Netflix and Chill” as payment reference – does this reveal his sexual orientation? Does the PSP have to ask for his explicit consent before making the transfer? Does the AISP have to filter this transaction, i.e. “censor” the PSU from his own choice of words?
- If a German speaking PSU enters “Krebs” in the free text field of the payment reference, does he/she refer to the disease (“cancer”), the zodiac sign (“Cancer”), the family name (“Krebs”) or the animal (“Crab”/crustacean)?
- If the PSU is versed in a foreign language that is *not* spoken in the PSP’s country of residence – either because he/she is an expat, a refugee, etc – and composes the payment reference in this language - how is the PSP supposed to even realize that a free-text field contains sensitive data?
- If a PSU makes a transfer to a Hospital with the reference “Cancer Treatment Bill no. 12345”, maybe he/she pays the bill for his/her daughter, his/her spouse or a friend.
- The list goes on.

- We believe we have made it clear that the approaches suggested in the Guideline (asking for explicit consent or implementing technical measures) are not practicable. Contrary to popular belief or what some tech companies want us to believe, there is no “artificial intelligence” or algorithm that is capable of handling such ambiguities as mentioned above.

- We strongly believe that the processing of sensitive data for the sole purpose of rendering payment services **is of substantial public interest (Art 9(2)(g) GDPR)**:
  - The need for a smooth operation of payment systems is enshrined in the Treaty on the Functioning of the European Union itself (Art 127).
  - The integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market (Recital 5 PSD2).
  - Payment services are essential for the functioning of vital economic and social activities. (Recital 7 PSD2).
  - An integrated market for electronic payments in euro, with no distinction between national and cross-border payments is necessary for the proper functioning of the internal market (Recital 1 SEPA-Regulation).
  - SEPA is regarded as essential for the Europe 2020 strategy which aims at a smarter economy in which prosperity results from innovation and from the more efficient use of available resources (Recital 2 SEPA-Regulation)
  - Banking (i.e. ASPSP) is considered a critical infrastructure by Directive (EU) 2016/1148.

- The smooth functioning of the internal market and the development of a modern, socially inclusive economy increasingly depends on the universal provision of payment services (Recital 3 Directive 2014/92/EU).
- The access to a payment account is an enforceable right within the EU (Art 15, 16 Directive 2014/92/EU).
- Without PSPs and the infrastructure provided by them, the Europe's economy would crash within the blink of an eye.

- All of this shows that the provision of payment services and the associated processing of data are of a **substantial public interest**. It is appropriate to the aim pursued (only such sensitive data are processed that the PSU him-/herself chooses to disclose), PSD2 respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (see esp Art 66, 67 PSD2).
- Hence, the **processing of sensitive data in the course of rendering payment services** as defined in Annex 2 of the PSD2 **does not require the PSU's explicit consent nor is there a need to "filter" sensitive data**.
- Obtaining the PSU's consent would also run counter to the PSP's obligation to a maximum 1-day execution time pursuant to Art 78 PSD2, or the even shorter execution time of less than 60 seconds when the payment order is executed within the SCT Inst scheme. As to the transaction volume, the share of SCT Inst scheme in the total volume of SCT was 5.92% in Q1 2020 (compared to 1.02% in the Q1 2019).

No 63,64 Please note that ASPSPs are obliged to not alter or modify the data that AISPs/PISPs are accessing. Digital filters and similar measures would be in breach of Art 32(3) Commission Delegated Regulation (EU) 2018/389. See also the European Banking's Authority opinion on said Regulation (EBA-Op-2018-04, page 4 and number 18).