NORDIC
API GATEWAY

Feedback to EDPB Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

Introduction

Paragraph 12

Depending on specific circumstances, payment service providers could be a controller or processor under the GDPR.

Our opinion regarding the roles of the payment service providers (PSPs) is that PSPs are always controllers and not processors, whether ASPSP, AISP or PISP.

As emphasized by the PSD2 recital 87, also referenced in these Guidelines para. 14, PSD2 *concerns only contractual obligations and responsibilities between the payment service user and the payment service provider.* The definition of a PSP includes AISPs, PISPs and ASPSPs. [1] Therefore, each payment service provider must have in place a compliant contract with the PSU, which means that each PSP determines the purpose and means of processing activities.

The above rationale can also be deduced from:

- para 37 which states that *[...] the payment service provider [...] needs access to personal data that have been processed under the responsibility of <u>any other controller</u>.*
- para 40 which makes a reference to Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), clarifying that *"<u>controllers</u> should avoid identifying only one broad purpose [...]''*

There is a certain collaboration between the PSPs, but not to the extent that one PSP would be limited to processing activities instructed by another. The collaboration between the PSPs is characterised by an independent transfer of data which helps the data subject use financial services and be in control of their finances.

Consequently, PSPs involved in the payment chain are controllers (whether ASPSs, AISPs or PISPs), as they each define how data is being processed under their control.

EXPLICIT CONSENT

Paragraph 35

Explicit consent under Article 94(2) PSD2 should therefore be regarded as an additional requirement of a contractual nature in relation to the access to and subsequently processing

[1] Art. 4(11) and Annex 1, PSD2.

and storage of personal data for the purpose of providing payment services and is therefore not the same as (explicit) consent under the GDPR.

Paragraph 38

While the PSD2 does not specify the substantive conditions for consent under Article 94 (2) PSD2, it should, as stated above, be understood in coherence with the applicable data protection legal framework and in a way that preserves its useful effect.

PSD2 and GDPR are two different legal frameworks that use the exact same wording, explicit consent, yet the nature is different under PSD2 and GDPR.

These Guidelines clarify the contractual nature of the explicit consent under PSD2 enshrined in the legal basis for performing the contract under GDPR.

However the practical implications of such difference may not be clear since processing should be aligned with GDPR requirements overall.

We would appreciate some more clarification and maybe practical examples on this matter.

THE PROCESSING OF SILENT PARTY DATA

Paragraph 48

Consent of the silent party is legally not feasible, because in order to obtain consent, personal data of the silent party would have to be collected or processed, for which no legal ground can be found under Article 6 GDPR.

Overall, we would appreciate a clarification and maybe some practical examples on whether consent can be collected or processed and what type of consent - contractual under PSD2 or legal ground under GDPR.

At the same time, in this context we would welcome a clarification about data processing of silent party data already done by the ASPSP.

THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA UNDER THE PSD2

Paragraph 52

[...] it is recommended to at least map out and categorize precisely what kind of personal data will be processed.

A precise categorization of personal data is not feasible, as the PSP does not know in advance where the funds will be transferred, and therefore cannot foresee whether the payee is an indirect identifier of the data subject which reveals sensitive personal data (e.g. hospital, pharmacy, union). Nor can the TPP anticipate whether the data subject will add a description to a certain transaction that may contain sensitive personal data.

Paragraph 56

Explicit consent as set out in Article 9 (2) (a) GDPR must meet all the requirements of the GDPR. This also applies to silent party data.

Para 48 above states that consent of the silent party is legally not feasible, yet according to para 56, silent party's consent must be collected in compliance with the art. 9 (2) (a) of the GDPR. It is confusing whether it is legally feasible or not.

Can the explicit consent of contractual nature under PSD2 also be considered as a derogation under Art. 9 (2) (a) GDPR?

We would appreciate a clarification on this matter.

Paragraph 57

[...] technical measures have to be put in place to prevent the processing of special categories of personal data, for instance by preventing the processing of certain data points. In this respect, payment service providers may explore the technical possibilities to exclude special categories of personal data and allow a selected access, which would prevent the processing of special categories of personal data related to silent parties by TPPs.

It is very difficult, if not impossible for a TPP to influence the occurrence of processing sensitive data, especially in terms of who is the payee (e.g. union), as processing these data, i.e recipient of funds, represents the essence of TPP services and also a legal obligation to have knowledge of the recipient.

According to Articles 66 and 67 PSD2, access to payment data is already restricted to what is necessary in order to perform the service. Preventing access in relation to sensitive data would lead to the TPP being blocked, and the reasons for being denied access to a payment account must be related to unauthorised or fraudulent access[2].

Implementing technical measures to prevent processing of special data, is already defined as processing. In this sense, the controller would have to perform processing in order to identify data that might be considered a special category, in order to filter it.

This is even the case if the controller does not have a purpose of this processing, except for the filtering itself.

The technical solution would in essence put the data subject at a higher risk, than leaving the data without identification of the special category data.

DATA MINIMISATION, SECURITY, TRANSPARENCY, ACCOUNTABILITY AND PROFILING

Paragraph 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.

Both under PSD2 and GDPR, the data that can be processed are only the payment account data necessary for providing the service. Such a selection is not possible in the current environment. ASPSPs are obligated to transfer all data that is available through the ASPSP channel (RTS art 36 (1)).

Paragraph 68

Where a data breach involves financial data, the data subject may be exposed to considerable risks.

We would appreciate a more clear explanation of what considerable risk means, and some practical examples where a DPIA is needed.

[2] Art. 68 (5), PSD2.