Stockholm, 15 September 2020

Comments from Trustly Group AB on Guidelines 06/2020 on the interplay of PSD2 and the GDPR

Dear Sir/ dear Madam,

Trustly Group AB ("**Trustly**") welcomes the opportunity to provide feedback on the European Data Protection Board's ("**EDPB**") Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR dated 17 July 2020 (the "**Guidelines**").

Trustly will in this response provide a number of comments on the contents of the Guidelines.

Briefly about Trustly

Trustly is a licensed payment institution licensed by the Swedish Financial Supervisory Authority. Trustly holds licences as a payment initiation service provider ("**PISP**") and account information service provider ("**AISP**"). In addition, Trustly holds licenses allowing Trustly to execute payment transfers as well as money remittance services. Trustly provides its payment services in a number of jurisdictions in Europe and has for those purposes passported its licenses to the relevant jurisdictions. Moreover, Trustly is providing payment services in the US and Australia. Globally Trustly process approximately 12 million transactions a month.

Trustly takes security and personal data protection matters seriously and has dedicated individuals tasked with making sure that Trustly is complying with relevant laws and regulations. This includes a DPO, GDPR specialist lawyers as well as Chief Information Security Officer.

Summary of comments on the Guidelines

1. The notion of who a payment service user is, needs to be more carefully considered in the Guidelines. The definition of payment service user in PSD2 confirms that it can be either a *payer* or a *payee*. When used in the context of the Guidelines it appears to be assumed that the payment service user is always a payer.

2. There is a risk that the Guidelines will be interpreted as being relevant only with regard to PISPs and AISPs albeit that that does not appear to be the intention. Our understanding is that certain parts of the Guidelines indeed are applicable to all payment service providers that fall within the scope of PSD2, such as Article 94. Hence, we suggest that the Guidelines are more clearly divided into one section that applies to all payment service providers and a separate section that applies to providers of payment initiation service and account information service providers specifically. Moreover, the Guidelines should underline the importance that all payment service providers comply with GDPR. Currently the Guidelines can be perceived as addressing an increased risk that PISPs and AISPs pose, although there is no empirical evidence supporting such a conclusion.

3. The Guidelines interpret Article 66 and 67 unnecessarily strict with regard to the processing of personal data that PISPs and AISPs can undertake, risking unwanted consequences for PISPs and AISPs effectively limiting their ability to provide service to the benefit of consumers.

4. The Guidelines can be made clearer with regards to the interpretation of explicit consent under Article 94 by explicitly acknowledging that there is room for interpretation/manoeuvre depending on the specific payment services provided by the relevant payment service provider.

5. The sections dealing with special categories of data and silent party data should be reconsidered in order to better reflect the actual circumstances under which AISPs/PISPs offer their services as well as to avoid inconsistencies between different parts of the respective sections.

1. Notion of payment service user

The Guidelines often refers to the notion of the payment service user. However, the Guidelines do not take in consideration that several PISPs, Trustly included, consider that the merchant taking receipt of a payment is the customer of the PISP. In other words, it is the payee that is the customer of the PISP, not the payer. While PSD2 acknowledges that in the definition of the payment service user, it would seem as if EDPB has not taken that into account.

In certain circumstances PSD2 is clear on the fact that a PISP and/or ASPSP has obligations towards the payer, see e.g. Article 66 (3) (g) of the PSD2 that states that the PISP shall not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the *payer* and Article 66 (1) of the PSD2 that states that Member States shall ensure that a *payer* has the right to make use of a payment initiation service provider.

However, whenever the word payment service user is used in the context of PSD2 it should be considered if the payment service user in that context is the payer or the payee. Accordingly, we suggest that the Guidelines analyses in what "capacity" the notion of payment service user is used in the Guidelines. For example would we believe that when used in paragraph 65 the notion of payment service user, at least from Trustly's point of view, is referring to the payee. Our customers (i.e. a payee) would typically expect to be able to retrieve their transaction history for a longer period of time than compared to interest of the payer being able to see his/her transaction history. Moreover, paragraph 11 should be amended to correctly cite Article 66 (3) (f) of the PSD2 as that Article is referring to the payer, not a payment service user.

2. Scope of the Guidelines

In paragraph 4 of the Guidelines it is stated that "*the main focus of these guidelines is on the processing of personal data by AISPs and PISPs*". Accordingly, a reader can be assumed to draw the conclusion that unless clearly stated otherwise the contents of the Guidelines is directed to PISPs and AISPs. An example is Section 3 on explicit consent which can be understood as being relevant for PISPs only (as AISPs are not in scope of that Article as per Article 33 (2) of the PSD2). In this respect it is to be noted that Article 94 (2) is not applicable in relation to PISPs only, on the contrary it applies to *all* payment service providers that are licensed in accordance with PSD2 (with mentioned exemption set out in Article 33 (2)).

In case it is not clearly stated that Section 3 applies to all payment service providers there is an obvious risk that PISPs will be at a competitive disadvantage as compared to other payment service providers since other payment service provider will not be required to obtain explicit consent for its processing of personal data, whilst PISPs will.

3. Article 66 and 67 - explicit consent and further processing

We do not agree with the statements in paragraph 22 that Article 66 PSD2, from a GDPR perspective, considerably restricts the possibilities for processing for other purposes than as explicitly consented to by the payer. As with any other processing of personal data, a data controller needs to comply with GDPR and among others the basic principles (Article 5), legal basis (Article 6) and providing information (Article 13) in a transparent way (Article 12). However, as long as GDPR is complied with, processing of personal data is per default allowed, this also includes processing that is based on another legal basis than consent. The restriction imposed by PSD2 in Article 66 should rather be understood as limitations from a PSD2 regulatory perspective entailing that a PISP cannot use information pertaining to the payer's payment accounts to initiate a new payment order unless the payer has explicitly consented to the new payment order.

We believe that the proposed interpretation of Article 66 in the Guidelines, and the conclusion that any other processing than providing the payment service that is requested is (typically) not allowed, will result in unintended consequences. For example, Trustly only provides its payment initiation payment services upon the request of the payer (i.e. with the payer's explicit consent) as the payer is actively choosing to pay with Trustly and is proceeding through Trustly's iframe by choosing his/her bank, bank account to pay from as well as authenticating the payment. In other words, is the payer in control of the payment and can at any time choose to abort. As part of this payment process Trustly will gather and store some data, such as the identity of the payer, the account from which the payment was made and the amount that is paid. This information can be said to be information that is necessary to perform the payment. In other words has Trustly so far complied with Article 66.

However, assume that there is some kind of error with our service and we need to troubleshoot/investigate. As part of that troubleshooting/investigation we may want to review transaction history for a number of payers to understand how severe the error is and detect the root cause of the error. Based on our understanding of paragraph 22, especially the interpretation that the compatibility test of Article 6 (4) of the GDPR cannot result in a legal basis for any other processing, Trustly would not be able to perform such troubleshooting/investigation since it would not be processing for the payment service that is requested, no consent for troubleshooting/investigation has been obtained (which is effectively not possible at the time of troubleshooting/investigation since it may involve a review of a large number of transactions) and there are no legal basis provided by Union or Member State law mandating troubleshooting/investigation. Whereas, such further processing for the purpose of troubleshooting/investigation may be lawful in line with the compatibility test of Article 6 (4) of the GDPR and in light of Article 5 (1) (b) and recital 50 of the GDPR.

Hence, our suggestion is that it in the Guidelines is clarified that as long as a PISP at the time of gathering and later processing of the personal data complies with GDPR, such processing of personal data is indeed lawful. This conclusion is not contradicted by Article 66 PSD2 which should be understood as requirements from a PSD2 perspective only.

4. Article 92 - explicit consent

We share the EDPB's conclusion in paragraph 43 in the Guidelines, regarding that explicit consent under the PSD2 is a different concept as compared to (explicit) consent under the GDPR and that explicit consent in line with Article 94(2) of the PSD2 is an additional requirement of a separate nature.

We would like to point out that the PSD2 does not stipulate any requirements as to how a payment service provider shall acquire explicit consent from a payment service user (which in this context can be either a payer or a payee), contrary to what is set out for a valid consent in line with Article 7 of the GDPR. In other words there are also no requirements as to how a PISP obtains a legal basis for its processing of personal information in the context of payment services in light of Article 94 (2) of the PSD2. The requirement would rather entail that the users of payment services are made fully aware of the specific categories of personal data that will be processed and the specific (payment service) purpose for which the users' personal data will be processed.

That said, in our view, it is up to each payment service provider to choose, at their own discretion, how to implement appropriate solutions to be able to comply with Article 94 (2) of the PSD2, taking into account inter alia the unique characteristics of the provided payment service. This discretion is rather necessary for payment service providers to be able to comply with the regulations in practice. We believe that the Guidelines would benefit by acknowledging this fact.

Needless to say, payment service providers of course despite such a statement have a – separate – obligation to comply with the requirements set out in the GDPR for processing of personal data, in particular as regards e.g. the principles (Article 5), legal basis (Article 6) and providing information (Article 13) in a transparent way (Article 12).

5. Processing of special categories of personal data and silent party data

We find the EDPB's reasoning regarding processing of special categories of data pursuant to Article 9 in the GDPR problematic. PISPs and AISPs offer services which inherently involve a

risk of processing special categories of data, since transactions are being processed, in different ways. However, processing of special categories of data is not the initial purpose of such service providers when providing their services, but becomes an indirect consequence. In other words, PISPs and AISPs are not knowingly asking for special categories of data, but may receive such information as a consequence of providing services that in themselves do not require processing of special categories of data.

That said, it is very difficult, in practice, to completely avoid the processing of special categories of data, since in theory, any transaction could contain such data. Thus, the requirement to obtain explicit consent in accordance with Article 9 (2) (a) of the GDPR in this regard for each individual transaction that may contain special categories of data, is quite burdensome as each transaction would have to be assessed individually on a case-by-case basis. Even if it may be possible to implement technical measures for the purpose of trying to filter out transactions which contain special categories of data, the measures would pose their own set of problems, e.g. they would be quite costly and would also slow down the services, which could have serious implications for the industry of payment services.

Moreover, it is worth noting that a PISP or an AISP relies on accounts servicing payment service providers (i.e. banks) when providing its services and any processing of special categories of data by a PISP or an AISP would to the same extent be made by a bank. Based on our understanding, banks are not asking for explicit consent from the user in relation to each and every transaction that may entail processing of special categories of data. From the Guidelines it, however, seems that the limitations described in Sections 4 and 5 would apply to AISPs and PISPs only. If that is the case we would expect the Guidelines to provide a rationale for such a conclusion or otherwise. If the intention is that Section 4 and 5 applies to all payment service providers it should be clarified in line with our comment under Section 2 above.

Additionally, the EDPB's reasoning in relation to this subject appears to be inconsistent when it comes to processing of silent party data that may constitute a special category of data. On one hand, the Guidelines state that "*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…*" and on the other hand, they state that "*in cases where [substantial public interest] does not apply, obtaining explicit consent…seems to remain the only possible lawful derogation…This also applies to silent party data.*". This is also inconsistent in light of Article 11 in the GDPR, which states that "*If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.*".

In light of this, we would like to urge the EDPB to reconsider its position regarding processing of special categories of data in relation to payment service providers.