The Consumer Voice in Europe

GUIDELINES 06/20 ON THE INTERPLAY ON THE SECOND PAYMENT SERVICES DIRECTIVE AND THE GDPR

BEUC comments on the EDPB public consultation

Contact:Jean Allix – financialservices@beuc.eu

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2020-086 – 15/09/2020

Why it matters to consumers

The PSD2 "opened the door" to open banking by requiring banks to grant third parties access to payment accounts based on consumers' consent, with the aim of promoting market competition. Access to other accounts (e.g. savings accounts, investment accounts) are not covered by PSD2 but for the time being only by GDPR.

But GDPR applies also to the processing of personal data, including processing activities carried out in the context of payment services, as defined by the PSD2.
The EDPB guidelines will further clarify the interplay between PSD2 and GDPR. These guidelines need to ensure strong protection for consumers as it is essential that they remain in control of their data and that their rights are fully respected.

BEUC comments

BEUC welcomes the EDPB consultation on the interplay between PSD2 and GDPR. BEUC submitted comments related to this interplay in April 2019. We are happy that many of our concerns have been taken in account in particular for purpose limitation, data minimisation, and profiling.
Nevertheless, we want to underline some problems of understanding of the guidelines due to two main reasons.

1. Payment market as a two-sided market

A classic payment is a 'four corners' model: one consumer, one retailer, one acquiring bank (retailer's bank) and one issuing bank (consumer's bank). Using the terminology of PSD2 the two banks are Account Servicing Payment Service Provider (ASPSP). Regarding payments, the Payment Initiation Service Provider PISPs become an intermediary between the retailer and the consumer's bank, cutting the direct relationship between the retailer and its bank. In several points in the draft guidelines, ASPSPs are mentioned but without indicating if it is the consumer's bank, guardian (controller) of the data or the retailer's bank who is responsible for the request of the Strong Costumer Authentication (SCA). According to PSD2, banks PISPs and AIS are Payment Services Providers (PSPs). When the term PSP is used in the guidelines, it is sometimes difficult to identify which category of PSPs is involved. Another ambiguity is the fact that any bank can act as an AIS and therefore ask its client to give it access to their account in another bank.

2. Lack of differences between PISPs and AISs

2.1. PISPs

A PISP initiates a payment by contacting the consumer's bank and asks this bank to generate a credit transfer. For on-line transactions, a retailer displays on their website the list of the payment instruments they are ready to accept, usually cards but also credit transfers. In more and more countries, retailers are adding PISPs brands, the main reason being that the PISPs services are less expensive than card payments. A PISPs has thus a contract with a retailer allowing them to accept payments made with the PISP brand. If the consumer at the time of the transaction does not have a contract with this PISP, they are directed to the registration system of the PISP to sign a contract to be able to use these services. At the time of the issuance of PSD2 (2015), the PISPs needed to know if the funds were available and to be sure that no other transactions (cash withdrawal, direct debit) will have priorities on the availability of the funds. In 2016/17 a lot of discussions has happened on this point, see in particular the European Retail Payment Board (ERPB) report of November 2017. This discussion is now obsolete as many credit transfers are now instant (less than 10 seconds by the rule, 3 seconds on average). Instant credit transfers will become soon the new normal and the classic credit transfers with an execution time of more or less two days will disappear. The huge consequence of this is that the PISP will not have the need to access to the data stored on the consumer's bank account. (see development about that on point 26).

2.2. AIS (Account Information Service)

Before PSD2 this service already existed, the AIS used the consumer's credentials to access the consumer's account by the technique called 'screen scraping'. As explained in our comment last year, the nature of the services provided by the AISs has considerably evolved, it is no more only aggregation of account but collecting data to provide better services such as consumer credit or insurance, as explained in point 8.

Nevertheless, there is a fundamental difference between the activities of the AISs and other activities covered by PSD2: AISs do not provide payment services. There is never a transfer of funds (definition of a payment service) in the activities of the AISs. These characteristics lead to a lot of differences with PISPs. When PSD2 was negotiated, there were concerns about the activities of such companies and the fact that banks were trying to block these activities. To solve the issue, it was decided to include them in the PSD2, even though the service provided is not a payment service.

With the ongoing move to Open Banking, this situation raises a lot of problems as the scope of PSD2 is limited to payment accounts. The EU Commission issued several financial services consultations during the spring, one on the digital finance strategy and another on the retail payment strategy, where BEUC made the following proposal[1]:

"*As the Commission has announced new legislation creating an EU data space for financial services, BEUC's proposal is to withdraw the AISs from PSD2 to integrate them in the scope of this new legislation on data. For consumers, this would have a huge advantage as they would be protected by the same rules for access to their payment account, savings account and other financial data. Otherwise the rules will be different for various kinds of accounts which could be very confusing for consumers.*"

[1] https://www.beuc.eu/publications/beuc-x-2020-072_a_retail_payments_strategy_for_the_eu.pdf, page 10.

The draft guidelines very often put AIS and PISP on an equal footing, neglecting the fact that PISPs need very few or even no data while collecting data is the core business of AIS.

Regarding the interplay between PSD2 and GDPR, the main concern of BEUC's is AISs, not PISPs. For the sake of clarity, it would have been easier to have different points for PISPs and AISs.

Remarks by articles

- **Point 12.** It is indicated that Payment Service Provider could be a controller or a processor. In many points it is indicated "controller shall provide" or "controller may choose". A question is: who is the controller? The bank or the TPP (AIS or PISP) as they are all PSPs.
- **Points 15, 16 and 17.** It is indicated that the controller has to assess which data are objectively necessary for the performance of the contract. As explained in the comment on point 26 in a near future PISPs will not need to have access to data stored by banks.
- **Point 26.** It is indicated that the ASPSP must provide the information necessary for the PISPs and AISs to provide their service. In fact, a PISP does not need any information from the bank. To initiate a payment, the PISP needs the name of the beneficiary, the amount of the transaction, the date and location of the purchase, all information provided by the retailer. It needs also the IBAN of the consumer, that the consumer has provided at the time of the registration. The PISP send this information to the bank to initiate an instant credit transfer. The bank requests a strong customer authentication that can be done through redirection (directly between the bank and the consumer) or through the PISP but the data (credentials) are provided by the consumer. When the authentication is done, the bank executes the payment in less than 10 seconds and the PISPs is informed. In that kind of transaction, there is no need for the PISPs to access to the data stored by the bank.
- **Point 33** is about explicit consent. It should be useful to understand the guidelines' reasoning to mention that PSD2 includes two types of consent, simple consent for the execution of a payment as well as explicit consent for the access to data.
- **Point 34.** According to article 33.2[2] of PSD2 this article 94 about data protection applies to all PSPs except AISs. What are the legal consequences of this exemption? Does it mean that the rule about data access and/or processing are not the same as for other PSPs? This point should be clarified, particularly when a bank is acting as an AIS. This point 34 is the only reference to this ambiguity created by this article 33.2.
- **Point 38** indicates that article 94(2) ensures transparency for the service user. Unfortunately, as mentioned above, this article does not apply to AIS. What are the consequences? Same remark for point 41.
- **Point 43.** It is clear in this point that explicit consent under PSD2 is not the same as explicit consent under GDPR. Nevertheless, this PSD2 consent has to be explicit. Although we understand the interpretation of the Board and that therefore the explicit consent under the GDPR and the PSD2 are different legal tools, as written in our precedent position paper, we think that explicit consent under PSD2 should ensure that the same conditions required for the explicit consent under the GDPR are met. In this sense, the guidelines could be more specific. This means that

[2] The persons referred to in paragraph 1 of this Article shall be treated as payment institutions, save that Titles III and IV shall not apply to them, with the exception of Articles 41, 45 and 52 where applicable, and of Articles 67, 69 and 95 to 98.

existing means to obtain classic valid consumer consent are insufficient. Users tick a cookie box to access a website, for example, without any idea of the consequences of this agreement. It should be useful to insist on this point in this concluding point. We have proposed during all the discussions that the box to tick should be accompanied by a statement saying that the consumer is aware that they are giving access to their financial data.

- **Point 69** indicates that controllers are obliged to take adequate measures to protect personal data. Once again there is no indication which controller. Does it mean that the consumer's bank needs to prevent the AIS to access to some data or that the AIS must not disseminate this information to its clients (point 75 on personal data disclosed to another recipient)?
- **Point 73** about article 13 and 14 GDPR. It would be useful to indicate that in the cases covered by PSD2 quasi all data, except those related to the strong customer authentication, are not provided by the data subject but by the data controller, in that case the consumer's bank. Thus, it is article 14 GDPR which is applicable.
- **Point 77.** BEUC welcomes the idea of the dashboard that the bank will display and the fact that now the EBA has accepted the idea that the consumer can withdraw their consent by contacting the bank and not the AIS. But there is something we do not understand. It is the answer given by the EBA which states that the ASPSP cannot request a copy of the consent given by the consumer. The bank being the guardian of the consumer's data, it should be logical for this guardian to be able to check what the consumer has given their consent to. At the time of the discussion on this point, BEUC proposed to follow the model of the existing legislation for direct debit: the consumer gives their consent (called a mandate) to the retailer but this consent is forwarded to the consumer's bank with the first request for a transaction. Works are ongoing to digitalise all the mandates. As this EBA answer is only interpretative, are we sure it is in conformity with GDPR as regard to the task of a controller?
- **Point 79** about profiling. It is indicated that AIS will make an extensive evaluation of personal payment account data. Point 8 accurately described the activities of AIS. From what we see in the UK where open banking is extensively used by credit providers, payment account data are not enough for them, savings account is also an important point. It should be useful to repeat here that any access to non-payment accounts are only regulated by GDPR and not by PSD2 as briefly indicated in point 8.

END

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).