The Consumer Voice in Europe

BEUC'S RECOMMENDATIONS TO THE EDPB ON THE INTERPLAY BETWEEN THE GDPR AND PSD2

Contact: Jean Allix – financialservices@beuc.eu

David Martin – digital@beuc.eu

BUREAU EUROPÉEN 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 • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2019-021 -11/04/2019

BEUC – The European Consumer Organisation is an umbrella group that represents 43 independent national consumer organisations from 32 European countries.

We welcome that the European Data Protection Board (EDPB) is analysing the interplay between the General Data Protection Regulation (GDPR) and the Payment Services Directive (PSD2). This is an important issue for consumers. We therefore appreciate the opportunity to contribute to the workshop organised by the Financial Matters Expert Subgroup of the EDPB on 27 February 2019.

Why is open banking important for consumers?

1. It is important for the future of financial services and the data economy.

'Open banking' will lead to more diversity among financial services providers, exposing banks to healthy competition that will have the potential to provide more innovative and better services. These services may for example include payment initiation, money management and investment advice, credit and insurance products, or cheaper energy offers. Open banking might serve as a test case for how data access regimes could work in other sectors in the future (e.g. connected cars).

2. It is important from a fundamental rights perspective, notably data protection and privacy.

If done right, it can give consumers more choice and control over their bank account data, for example by being able to easily choose which companies can or cannot access their bank account data and for what purpose(s).

The **PSD2 "opened the door'' to open banking** by requiring banks to grant third parties access to payment accounts based on consumer's consent, with the aim of promoting market competition. Access to other accounts (e.g. savings accounts, investment accounts) is currently under discussion.

BEUC recommendations

Third Party Providers (TPP) and access to data

PSD2 differentiates three categories of third-party providers (TPPs) that can access consumers' banking data to be able to provide the services requested by the consumer:

- Card-Based Payment Instrument Issuers (CBPII) – Article 65
- Payment Initiation Services (PIS) – Article 66
- Account Information Services (AIS) – Article 67

Banks can also provide these services themselves. If a bank decides to act as an AIS, it will allow the consumer to access all his/her accounts – also from other banks –through the mobile app of this bank. The drawback can be that this bank will have access to the consumer's data in other banks.

The aim of CBPII and PIS providers is **to enable a payment.** They only need, and must only access information that is necessary to determine whether the payment can or cannot be made (for example: to check if there are sufficient funds to initiate the payment).

AIS providers **aggregate information from the consumer bank account(s) for performing the service requested by the consumer.** For example, this can be advice on money management, credit scoring, access to targeted credit offers, insurance comparison, etc. Contrary to the two other types of third parties, AIS providers are not initiating or executing payments. This is why the conditions to get a licence for AIS providers are much simpler than getting a licence to be a CBPII or a PIS provider.

It is important to note that **most** of the services provided by AIS providers **constitute profiling under the GDPR.**

On the other hand, it is important to recall that **providers need a licence** to become a TPP. This is regulated by the PSD2 and will become mandatory by a new technical standard which will enter into force in September 2019. The license delivered in one country benefits from the 'passport principle' in the EU. In countries where this is already possible, credit providers have requested licences. It is important to highlight **that not only traditional financial service providers are requesting licenses.** For example, Google has received a Lithuanian license which covers PIS and AIS.

Accessing bank data by third-party providers is one of the main novelties introduced by PSD2. It creates **new opportunities** to develop services for consumers, something which is good, **but** it also raises **many critical questions and concerns** related to:

- Consumer control: How to ensure that consumers remain in control of their account data?
- Consent: What role for consent vs provision of service? How should consent be understood?
- Data minimisation and purpose limitation: How to make sure TPPs do not get access to more data than they need to provide the service requested by consumers and that they do not use for other purposes? What can be considered compatible purposes in these scenarios?
- Profiling.
- Processing of sensitive data.

Consent vs explicit consent

The first question that must be asked is the following: ***Are we sure that consumers know exactly what they are giving their agreement to?***

Our findings suggest the answer to this question is "no":

- A recent study by BEUC's UK member **the Financial Services Consumer Panel** showed that consumers are not giving informed consent when they share their financial data. Most people did not read terms and conditions and did not understand them even when they had read them. They saw terms and conditions as too long and complicated, full of legal jargon, and "not written with consumers in mind."

- Another recent study by BEUC's German member **vzbv**, came to similar conclusions. The survey was assessing what consumers think they are consenting to with **e-payment providers based on the knowledge of the terms and conditions.**

It is essential that the consumer knows exactly what he/she is giving their agreement to and that their rights under the GDPR also apply here.

PSD2 makes references to "consent" and to "explicit consent" in different articles. GDPR makes also reference to these two terms. Various stakeholders have been arguing that consent means different things in PSD2 and GDPR.

BEUC agrees that the meaning of "consent'' is different in the two legislations. However, in order to ensure a high level of consumer protection we consider that the term "explicit consent" in the PSD2 should be interpreted taking the GDPR as the model to follow. Therefore, **we need to differentiate between (simple) "consent" and "explicit consent".**

If you look at the articles where **"consent"** is mentioned under PSD2 (what we call "simple" consent), all references relate to **consent given to authorise a payment transaction**.

These references are not new. They were already in PSD1 – which did not contain any mentions to "explicit consent". This "simple" consent is not related to access or processing of data but to the authorisation of a payment transaction. In the GDPR, consent is related to the processing of data, therefore we are not operating on the same ground and it is reasonable that "simple'' consent under PSD2 and "simple'' consent under GDPR are just different, as they relate to different things.

When it comes to **explicit consent** in PSD2 it **should be understood within the meaning of the GDPR** for the following reasons:

1. **PSD2 only mentions "explicit consent" in situations where access to consumer data is given**. "Explicit consent" is used in the three articles related to TPPs (Arts. 65-67), and in the article referring to data protection (Art. 94.2). Therefore, it makes sense that in this case explicit consent is understood and held up to the same standards as in the GDPR, given that we are in a similar "data processing" situation.

2. **Article 94 of the PSD2 states that access to data shall be in accordance with Directive 95/46/EC.** This directive has been repealed and now should be understood as a reference to the GDPR (Art. 94 of the GDPR). In addition, Article 94.1 already existed in a not very different form in the PSD1 with the idea to fight against fraud. The novelty in the PSD2 is Article 94.2, which makes express reference to explicit consent (without defining what explicit consent means).

3. **Recital 89 of the PSD2 also references concepts which were in discussion at the time of preparation of the GDPR**, such as protection by design and by default.

4. From a purely data processing perspective, **it may be that the legal ground under the GDPR is the performance of a contract, but this does not exclude that explicit consent required under PSD2 should be interpreted in the sense that the agreement given by the consumers when concluding the contract should be held up to the same standards as explicit consent under the GDPR** (e.g. informed, meaningful, separate from other issues, etc.).

   That being said, as explained further below in the section about profiling, **access to bank account information can very often reveal sensitive data which would fall under Article 9 GDPR.** Explicit consent under the GDPR should be required as the legal basis for processing in those situations where special

categories of data would be involved. Otherwise, banks and TPPs would be actively circumventing the GDPR. In this sense, PSD2 is not *lex specialis*. To be a *lex specialis*, PSD2 should have given a specific definition of explicit consent. To ensure adequate protection, banks should implement technical measures to separate account data that might reveal information that would fall under Article 9 of the GDPR (e.g. payments to a religious organisation, payments related to medical treatments) from other account data.

Since 2017 BEUC has been participating in the expert groups of the European Commission and the Euro Retail Payments Board (ERPB), discussing the implementation of the PSD2 and the development of RTS (Regulatory Technical Standard) for the implementation of PSD2. We are also a member of an ERPB technical expert group on open banking. In these meetings, BEUC has made a proposal on explicit consent, mirroring one of the examples of explicit consent from the WP29 guidelines on consent (example n°17 on page 9):

> *'by ticking this box, I agree that company "XXX" will have access to the following financial data (list data for which the access is being requested) managed by the ASPSPs (bank) "YYY".*

Ensuring that consumers are fully aware of what they might be agreeing to and can remain in control of who can access their banking data is of utmost importance. Consent should be a cornerstone for protection and not a routine 'tick the box'' exercise. This is especially key as we see how services use different techniques to prompt the consumer to simply agree to everything[1] and how contracts and terms and conditions often contain unfair and illegal terms[2].

Silent party data processing

Silent party data in this context related to data that the TPP can collect which are not directly related to the consumer, but for example to the beneficiary of the payment or to the joint account holder.

PIS providers only need and must refrain from accessing information that is not necessary to determine whether the payment can or not be made.

Once again **most of our concerns relate to AIS.** Being able to access all the data of the consumer, the AIS provider can collect information related to all the transactions (debit and credit) made by the consumer.

It is prescribed by Art. 58.1.a of PSD2 that the bank statement available on the screen indicates the name and the IBAN of any beneficiary. Thus, this information is available for the TPP.

In addition, if the account is a joint account, the TPP can access to information about the other holder. This raises the question of how consent would work in this situation. In the case that it would be possible for the AIS to operate under legitimate interests for processing silent party data, it must be made clear to that party that his/her data are being processed and given the opportunity to object.

[1] See report from the Norwegian Consumer Council: ''Deceived by Design'' and BEUC letter to Ms. Jelinek on this topic.
[2] See recent judgement in France against Google

Profiling

There is no doubt that most of the activities carried out by AIS in the context of PSD2 would constitute profiling under the GDPR and would involve automated decision making in the sense of article 22 GDPR.

Access to bank account information will in many cases reveal **sensitive data** that would fall under Article 9 GDPR. For example, recurring payments or donations to a political party, or the payment of a subscription to a religious magazine or membership fees to a trade union.

It is essential to stress that the GDPR rules that apply to special categories of data and automated decision-making, including profiling, are highly relevant to and fully apply in the PSD2 context.

Whereas special categories of data are processed, explicit consent should be required as prescribed in the GDPR and consumers should be able to exercise all their rights. In accordance with Article 9 GDPR, only explicit consent would allow the processing of sensitive personal data in the context of PSD2. Other exemptions referred to in Article 9.2 do not apply. In particular, users' data are not manifestly made public (Art. 9.2.e) and are not necessary for reasons of substantial public interest (Art. 9.2.g) as the issue here is not the functioning of payment systems but only the access by the TPP.

Data minimisation and security measures

Compared to PSD1, PSD2 has two major innovations: security and access by third parties. Security is also reflected in the provisions related to data access. TPPs shall ensure that security credentials of the user are not accessible to other parties and are transmitted through safe and efficient channels (Arts. 66.3.b and 67.2.b). For banks it is indicated that they must communicate securely with a TPP, using the standards elaborated by the EBA, to ensure the safety of payment services users' funds and personal data (Art. 98.2.b).

PSD2 includes rules about data minimisation and purpose limitation in the three articles dealing with the 3 categories of TPPs (Arts 65-67):

- For **CBPII**, the only data they can get is a simple **YES or NO** answer.
- For **PIS**, providers can only get the **data related to the payment** to be processed and not to use data for purposes other than the provision of the service explicitly requested by the consumer.
- For **AIS**, once again, the situation is much more complicated. Art. 67.2 of the PSD2 indicates that the TPP will not use, access or store any data for purposes other than performing the service explicitly requested by the user. But **what is the service explicitly requested by the user when the consumer gives access to a credit provider to get a loan?** For example, a credit provider is interested by a lot of data on the resources of the consumer, but also in his/her way of life, maybe his/her health, his/her monthly expenses, etc. Will all those data be considered necessary for performing the service? BEUC recommends the EDPB to continue following opinion 06/2014 of the Article 29 Working Party, which states that the **"necessity" for the performance of a contract needs to be interpreted strictly**.

In addition, **the interpretation given by the European Banking Authority**[3] in its opinion on the implementation of the regulatory technical standards on strong customer

[3]See EBA-Op-2018-04, June 2018, paragraph 13).

authentication (SCA) and common and secure communication raises concerns. According to the EBA, banks do not have to check that consent has been given to the PIS and AIS services. This creates serious problems from a data minimisation and a security perspective, contradicting the GDPR.

This means that the bank which is storing the data is unable to check which data the consumer has given access to. From a consumer perspective this is in contradiction with the GDPR obligations regarding security of processing and data minimisation.

Consent must be verifiable by the banks to increase security. Verifying that consent has been given would add a necessary layer of security and would ideally help ensure that TPPs do not access data beyond what they need and have been given access to.

In its opinion, the EBA also indicates[4] it suffices that AISs and PISs can rely on the authentication procedure. The EDPB has already stated that authentication must not be confused with the consent itself[5]. **BEUC shares the same opinion: authentication is not consent.**

We furthermore do not agree to another interpretation of PSD2 by the EBA: According to the EBA[6], it is not possible for a consumer to instruct his/her bank not to give access to a TPP or another bank (the so-called 'opt out'). The consumer should always have the right to instruct his/her bank to never give access to his/her data or to whom not to share his/her data.

The EDPB was not consulted about the content of the RTS. This is regrettable and it is an opportunity for the EDPB to show the contradictions with data protection law so the PSD2 is not interpreted in a way so as to circumvent the obligations of the GDPR. We therefore recommend that the EDPB in its guidelines respectfully disregards the EBA opinion and clarifies what banks should do in line with the GDPR.

Processing of special categories of data

As stated earlier, access to bank account information can reveal sensitive data which would fall under Article 9 GDPR. The risk that sensitive data would be revealed reinforces our interpretation that explicit consent as required under PSD2 should be held up to the same standards as explicit consent in the GDPR. This is regardless of the actual legal basis for processing the data according to the GDPR, which could be the necessity for the performance of the contract between the TPP and the consumer.

That being said, in those cases where special categories of data are involved, "explicit consent" should be the legal ground for processing the data under the GDPR. "Performance of a contract" is not a lawful legal basis to process special categories of data and, besides explicit consent, none of the legal bases included in Article 9 GDPR are applicable in this situation.

Measures should be put **in practice to avoid revealing sensitive data when accessing** such data is **not necessary for the service that is being provided to the consumer.** In particular, as previously mentioned, technical measures should be put in place to separate account data that might reveal personal data that would fall under Article 9 of the GDPR from the rest of the account data. **Consumers** should be able to **choose** which bank account **data** they are **giving access to**. At the moment it is an 'all or nothing' choice as best. Consumers do not have choice to decide if they would like to disclose al or only certain (for example non-sensitive) account data. Even if the consumer indicated to

[4]See EBA-Op-2018-04, June 2018, paragraph 13.
[5]See footnote 8 in EDPB letter to MEP In't Veld: https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en
[6] See answer that the EBA gave to question 2018-4309.

the TPP that s/he gives access to certain data, the bank, guardian of the data, will not be aware of it. This is at odds with the rules on consent and the basic principles for data processing under the GDPR.

Moreover, BEUC is of the opinion that when the GDPR will be reviewed, financial data should be generally qualified as a special category of data and subject to additional protections, like the categories of data currently falling under Article 9 of the GDPR.

Processing of personal data for other purposes

As requested by PSD2, the industry is creating new channels for TPPs to access consumer data directly, without using the consumer home banking channel.

As TPPs get access to the data of consumers' payment accounts for a service that has been requested by the consumer. PSD2 states (articles 66.3.g and 67.2.f) that TPPs shall not use, access or store any data for purposes other than performing the service explicitly requested by the user in accordance with data protection rules. There is indeed the question of whether TPPs could further process the data for compatible purposes to those for which the personal data were initially collected.

The principle of purpose limitation should be strictly applied in the PSD2 context. Further compatible processing should be strictly limited, clearly predefined and clearly communicated to the consumer, if not completely prevented, in this situation:

- **There cannot be reasonable expectations from the consumer** that his/her data could be used for something else beyond the service that has been requested and it is hard to consider which purposes could be considered compatible.

- The fact that **sensitive data** could also be revealed further **advises against allowing further processing**. In particular taking into account that further processing is not allowed when data is processed on the basis of consent, and for sensitive data that would fall under Article 9 the legal basis for processing should be explicit consent.

Additional remarks

In addition to the points already mentioned, we would like to add three further remarks:

1. **PSD2 covers only payment accounts.** When an AIS provider wants to have access to savings accounts or investment accounts, PSD2 does not apply. Only the GDPR applies. This point is very important for the future. It is also a matter of implementation of Article 20 GDPR (the right to data portability).

2. **It does not make sense for AIS to be excluded from the scope of Article 94 of the PSD2, as set out in Article 33.2 of the Directive.** EDPB should clarify what this exclusion entails in practice in terms of the applicable rules and obligations.

3. **The authorities competent for granting TPP licenses and enforcing PSD2 should co-operate with DPAs** in the application of relevant PSD2 rules.

Conclusions

To sum up our recommendations:

1. Explicit consent required under PSD2 should mirror the requirements of explicit consent under the GDPR, regardless of what the legal basis for processing is under the GDPR.
2. The activities of AIS can fall under the GDPR provisions related to profiling and automated decision making. Consumers must be adequately protected and be able to fully exercise their rights.
3. Strong data minimisation and purpose limitation must be ensured. Consumers should be able to control which data they give access to and services should not access more data than they need to provide the service requested by the consumer. Further processing of account data for compatible purposes should be strictly limited.
4. Access to account data that might reveal information considered sensitive under Article 9 GDPR should be separated from access to other account data. "Performance of a contract" cannot be a lawful legal basis for the processing of special categories of data. Therefore, for such data, in addition to the explicit consent required under PSD2, explicit consent should also be required as a legal basis for processing under the GDPR.
5. Banks should have an obligation to verify consumers' consent to increase security.
6. Strong co-operation between national authorities in charge of ensuring PSD2compliance of businesses with national data protection authorities is crucial for effective and meaningful protection of consumers.

BEUC hopes that the EDPB guidelines will further clarify the interplay between PSD2 and GDPR and will ensure a high level of protection for consumers. Open Banking can bring benefits, but it is essential that consumers remain in control and that it is implemented in a way that their rights are fully respected.

More information about BEUC position:

- **Position paper on Consumer-Friendly Open Banking.**

- 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).