Brussels, 16 September 2020
DV 0_3

EACB comments on Guidelines on the Interplay between PSD2 and GDPR

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.800 locally operating banks and 53,000 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 84 million members and 719,000 employees and have an average market share in Europe of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) welcomes the opportunity to provide the European Data Protection Board (EDPB) with its comments on the draft Guidelines on the proposed Guidelines on the Interplay between PSD2 and GDPR. The implementation of PSD2 and indeed GDPR has proved to be a complex exercise and we are keen for the guidelines to set the right direction. In this context we have, in consultation with the membership of the EACB, formulated the following observations which we would ask the EDPB to take into consideration.

Comments

1. Definitions: the third category of new service providers that PSD2 introduces, i.e. CISP is never mentioned in the entire document. We would welcome clarification as to the reason for not doing so.

2. Paragraph 12 the text reads: "Depending on specific circumstances, payment service providers could be a controller or processor under the GDPR". However, AISPs and PISPs are licensed parties, with their own responsibilities to be compliant to all relevant legislation. Such role does not seem to match with the role of processor under the GDPR.

3. Paragraph 16 seems to suggest that a contract always has a main object. But nowadays the relationship between a bank and its clients usually contains various services, such as a payment account combined with a creditcard and the use of online banking services.

4. Paragraph 22 explains that it follows from the text of articles 66 and 67 of PSD2 that any further processing of personal data bij AISPs and PISPs should be based on consent or a legal obligation. We would appreciate some further explanation, since article 67 (2f) only says that data protection rules have to be taken into account. And the data protection rules allow data processing on the basis of for example legitimate interest, so why can't they be the basis for data processing by a AISP/PISP.

5. Paragraph 23 states that AISP and PISP are obliged to comply with the rules laid down by the AML ("These obliged entities are therefore compelled to apply the customer due diligence measures as specified in the directive. The personal data processed in connection with a PSD2 service are, therefore, further processed based on at least one legal obligation resting on the service provider").

   We would like to understand if, for the EDPB this means that the obligation to perform the AML due diligence is the direct responsibility of the TPP even if the relationship with the PSU does not derive from the establishment of an ongoing relationship of if TPPs donot move sums of money independently. Or does the performance of AML due diligence remain for a duty of the ASPSP as holders of the current account relationship?

   The service offered by TPP would not appear to be among the specific cases indicated by the AML Directive for the execution of the ADV. Perhaps the responsibility for reporting any suspicious money laundering operation could fall on the PISP alone, even if the PISP never gets hold of the funds and the payment info and is not an active part of the operation.

6. Section 3 "Explicit Consent".

   We expressly welcome the statements made under Section 3 "Explicit Consent". The guidelines come to the conclusion that "Explicit Consent" within the meaning of the provisions of the Second Payment Services Directive must be distinguished from "Explicit Consent" under the provisions of the General Data Protection Regulation. Section 3.3 "Conclusion" states that "Explicit consent under Article 94 (2) of the PSD2 is an additional requirement of a contractual nature."

   On the basis of this understanding, it remains possible, for example, to carry out transfers and direct debits without having to obtain in addition to the express contractual commissioning of the payment service user, which should always be available, a consent under data protection law. Any other assessment would significantly impair the functionality of European Payments.

7. Section 4 Processing of silent party data.

   The GLs specifically refer to a situation where an AISP/PISP requires silent party data for the provision of its services and state that a lawful basis for the processing, in this case, "*could thus be the legitimate interest of a controller or a third party to perform the contract with the payment service user*". The GLs are clear in saying that in this case the bank cannot refuse to share the data (otherwise it would be in breach of the law), but the AISP/PISP shall only require the information necessary to the provision of its services (principle of data minimisation). In other words, the AISP/PISP is mandated to perform an assessment of what data really needs and shall only require that amount of data. Since banks are not aware of the contract between the PSU and the TPP, they are not in a position to question whether the required data is right or whether it is too much. Hence, when the GLs say "*the controller has to establish the necessary safeguards for the processing in order to protect the rights of data subjects. This includes technical measures to ensure that silent party data are not processed for a purpose other than the purpose for which the personal data were originally collected by PISPs and AISPs. If feasible, also encryption or other techniques must be applied to achieve an appropriate level of security and data minimisation*" (para 47) we would appreciate clarification that they do not refer to ASPSPs, as banks would have no means to know what data (and how) is being processed once shared with a TPP. It is always the TPP's responsibility to collect, process and protect (all) the data they have decided to collect.

8. Section 5 Special categories of data.

   Although financial transactions may contain references to special categories of data, they themselves have not been classified as a special category of personal data under the GDPR. Indeed, If financial transaction data are not processed in order to collect special categories of payment data but merely to execute a payment, no special regime should be required. Because in order to recognize those data, extra data processing would have to be conducted. This should be stated explictly in the Guidelines. Our understanding is that a controller should not be obligated to comply with the Art 9 requirements if the intention is not to analyse e.g. individual's health or religious beliefs. Furthermore, it should be made clear that no additional consent for the ASPSP is needed for the normal processing of payment data, which may contain special categories of payment data.

Additionally, it is not entirely clear if the GLs are referring to special categories of data of the PSU, or to special categories of data of the silent parties. In the latter case no valid consent can be collected. The distinction above is crucial as paragraph 57 states that where the PSP cannot show a derogation is met, "*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*".

More generally, it seems that the EDPB is suggesting banks implement tools to prevent access to certain data which, on a financial transaction by financial transaction basis, are simply part of the information necessary to execute a payment. It is only if processed or used by a TPP that the information would become a special category of data. The EACB is strongly opposed to any such suggestion as:

- It would create discrepancies between what a customers sees via the customer interface and what a customer sees when using an AISP which is against PSD2 and considered an "obstacle" as per the different Guidelines and Opinions issued by the European Banking Authority under the RTS on SCA and CSC.

- Implementation of technical measures would have serious impact for banks as such operation would be hardly feasible,or at the least disproportionately costly considering that they would have to implement a solution to a something for which the responsibility lies with TPPs.

- It is not always so easy to understand whether a piece of information falls within the list of special categories of data. For instance, a single payment to a trade union may not necessarily show any affiliation/political belief. It can then be argued that it is not feasible for banks to sort out ex ante whether the requested information is sensitive enough to justify the exclusion from the data shared with the TPP, especially considering it mostly depends on how the TPP itself wants to use the data.

9. Section 6 Data Minimization Measures.

Paragraph 62 states that in the event that national legislation provides for it, it must be possible not to show the IBAN code of the silent party (i.e. the person who has not requested the provision of the specific service). However, this limitation could certainly be risky from the point of view of fraud (typical virus technique, phishing etc.). This is by the way not only the case of the silent party IBAN or name/identification. The guideline should be reconsidered with this in mind.
Paragraph 63, It is requested to specify more clearly the concept of "digital filter" and who should develop this implementation. Furthermore, if it's an ASPSP to use them, how to reconcile, as mentioned under point 8 above, this idea with the idea of "obstacles" as addressed by the different Guidelines and Opinions issued by the European Banking Authority under the RTS on SCA and CSC this forecast with the absence of obstacles to TPPs.

Paragraphs 64, We confirm that only payment accounts (for which the following definition is given: 'Payment account' means an account held in the name of one or more payment service users, which is used for the execution of payment transactions;) are in the PSD2 perimeter and not others such as e.g. deposit accounts, investment accounts etc. We would ask the EDPB to clarify that ASPSPs cannot be held responsible in case TPPs process data beyond payment accounts because they access the information on client accounts via, for example screen scraping and not the PSD2 interface and that, in this case, the relevant TPP might be in breach of GDPR.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser, Consumer and Retail Banking (chiara.delloro@eacb.coop)