

Statement 2/2024 on the financial data access and payments package

Adopted on 23 May 2024

The European Data Protection Board has adopted the following statement:

1 BACKGROUND AND PURPOSE OF THIS STATEMENT

1. On 28 June 2023, the European Commission (EC) published three proposals regarding payments services and financial data access. The legislative package consists of a proposal for a framework for Financial Data Access (FIDA)¹, a proposal for a Payment Service Regulation (PSR)² and a proposal for a Payment Service Directive (PSD3)³. According to the EC, these proposals aim to improve consumer protection and competition in electronic payments, and to empower consumers to share their data in order to access to a wider range of cheaper financial products and services⁴. To this end, these proposals further develop the existing legal framework on payment services (notably the Second Payment Services Directive, or 'PSD2'⁵) and establish a new framework to facilitate access to and sharing of financial data having regard to certain financial services (FIDA).

¹ Proposal for a Regulation of the European parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, COM/2023/360 final, 28 June 2023.

² Proposal for a Regulation of the European parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010, COM/2023/367 final, 28 June 2023.

³ Proposal for a Directive of the European parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, COM/2023/366 final, 28 June 2023.

⁴ EC Press release on the Financial data access and payments package, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543.

⁵ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23 December 2015.

- 2. On 22 August 2023, the EDPS provided two comprehensive opinions on these proposals⁶. Since these opinions have been published, the co-legislators have taken up their work on the proposals. The Plenary of the European Parliament (EP) has adopted its final report⁷ on the PSR Proposal on 23 April 2024. The ECON committee has adopted a report on the FIDA Proposal on 30 April 2024⁸.
- 3. The EDPB welcomes that the EP's reports take on board most of the recommendations issued by the EDPS in Opinion 38/2023 on the FIDA Proposal and some of the recommendations issued by the EDPS in Opinion 39/2023 on the PSR Proposal. However, some recommendations on the FIDA proposal have not yet been implemented in a satisfactory manner and many recommendations on the PSR proposal have not yet been taken on board.
- 4. In particular, this statement points out to topics where further alignment with the guidelines issued by the EDPB⁹ and the Opinions of the EDPS should be made, in order to ensure a higher level of protection of personal data compared to the one already provided by the EP reports.
- 5. In addition, the EDPB notes that on 18 December 2023, the Spanish Presidency of the Council of the European Union has published a progress report providing a summary of the discussions of six meetings of the Council working group on the PSR and PSD3 proposals¹⁰. The progress report states that, during these discussions, many Member States stressed the importance of the issue of data sharing for the purpose of preventing and countering fraud. This topic, due to the processing of personal data involved, is very relevant from the privacy and data protection perspective.
- 6. Considering that the Council's work is focusing on fraud prevention, this statement provides recommendations in this regard, building upon the practical experience of national data protection authorities on this matter. In particular, the EDPB considers that additional safeguards should be included in the legislation regarding the sharing of data for fraud purposes in order to ensure the fundamental right to data protection.

2 RECOMMENDATIONS

2.1 Need for clear rules for the recording and the disclosure of personal data in the context of the transaction monitoring mechanism of the PSR Proposal

⁶ EDPS Opinion 39/2023 on the PSR and PSD3 Proposals, available at: https://www.edps.europa.eu/system/files/2023-08/2023-0729_d2434_opinion_en.pdf and EDPS Opinion 38/2023 on the FIDA Proposal, available at: https://www.edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf

⁷ EP Report on the PSR Proposal, 23 April 2024, https://www.europarl.europa.eu/doceo/document/A-9-2024-0052 EN.html

⁸ ECON Report on the FIDA Proposal, 30 April 2024, https://www.europarl.europa.eu/doceo/document/A-9-2024-0183 EN.html

⁹ In particular, EDPB Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0, Adopted on 15 December 2020 ('EDPB Guidelines 06/2020'), available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

¹⁰ Council, Progress Report of 18 September 2023, available at: https://data.consilium.europa.eu/doc/document/ST-16676-2023-INIT/en/pdf

- 7. The EDPB notes that Article 83 of the PSR Proposal provides the obligation for payment service providers ('PSPs') to have transaction monitoring mechanisms ('TMM') in place in order to improve, inter alia, the prevention and detection of fraudulent transactions.
- 8. While acknowledging the importance to prevent payment fraud, the EDPB deems that the inclusion of robust data protection safeguards is necessary to protect the interests and fundamental rights and freedoms of individuals that would be subject to the TMM.
- 9. This applies in particular to cross-border data sharing by PSPs, for which the specific requirements for the processing (which may include the creation of dedicated databases) and disclosure of personal data for the purpose of fraud prevention should be clearly defined in the enacting terms of the PSR Proposal.
- 10. The EDPB takes note of some developments in the EP's report on the PSR Proposal in this respect¹¹. However, the EDPB considers that these developments do not include sufficient safeguards from a data protection perspective. Consequently, the EDPB calls on the EU colegislators to include the below recommendations in the PSR to ensure that the level of interference with the fundamental right to the protection of personal data of persons concerned is necessary and proportionate to attain the objective of preventing payment fraud.
- 11. With regard to the **processing** of personal data via the TMM, the EDPB recommends that the PSR:
 - further specifies the categories of personal data that PSPs will process in the context of TMM. In particular, a definition of "information on the payment service user" should be provided;
 - provides, under Article 83(1)(c), for an obligation for PSPs to clearly and objectively identify
 the factual conditions triggering the TMM in relation to transactions before processing them
 via the TMM;
 - provides for an obligation for PSPs to document the reasons underpinning the processing of personal data in the TMM for the purpose of subsequent verifiability by competent authorities;
 - provides that the access to data processed in the TMM is limited to authorised, specially qualified personnel of the PSPs;
 - provides for an obligation for PSPs to inform the data subjects about the criteria underlying the processing of their personal data in the TMM (e.g., upon the opening of the payment account), including about when and how their personal data will be processed in the context of the TMM;
 - provides that personal data processed in the context of the TMM is used only for the purposes listed in Article 83(1) of the PSR Proposal and, in particular, that this data is not reused for the purpose of establishing the credit score of the customers;

¹¹ Such as clarifying that measures and instruments used by account servicing payment service providers in response to suspected fraud or to comply with Regulation (EU) 2016/679 (e.g., to verify whether the Third Party Provider has a GDPR legal basis for processing) would not constitute prohibited obstacles to data access by payment initiation and account information service providers (Article 44(1a)).

¹² Referred to in Article 83(2)(a) of the PSR.

- provides that PSPs are not granted the right to use all types of data collected in relation to TMM also for the purpose of strong customer authentication as an element of 'inherence' pursuant to Article 3(35) of the PSR Proposal¹³. This recommendation is justified by the fact that 'inherence' elements must refer to something the user is¹⁴. While having in mind the requirement for PSPs to provide a very low probability of an unauthorised party being authenticated as the payment service user¹⁵, the EDPB recommends limiting the categories of data that may be processed for the purposes under Article 83(2) of the PSR Proposal.
- defines appropriate data storage periods for the personal data collected under Article 83 of the PSR Proposal and justifies such retention period in a Recital.
- 12. With regard to the **transmission** of personal data collected in the context of the functioning of the TMM, the EDPB recommends that the PSR:
 - provides that exchanges of data under Article 83 of the PSR Proposal are, in principle, limited to exchanges between PSPs. In particular, the EDPB has concerns about the possible extension of the obligation to share information for PSPs not only among them but also with public authorities¹⁶. Should the co-legislators decide to enable data sharing with public authorities, the EDPB strongly recommends including specific conditions and limits for such data sharing (e.g., only where there is a justified suspicion that a serious criminal offence has taken place), together with accompanying data protection safeguards.
 - does not task the European Banking Authority (EBA) with setting up a dedicated IT platform to allow PSPs to exchange information under Article 83 of the PSR Proposal¹⁷. The establishment of such unique IT platform would centralise sensitive transaction information. This would entail a higher level of interference with the fundamental right to the protection of personal data of individuals, as well as higher security risks (e.g., in case of data breach), compared to a distributed/decentralised data processing as it is currently the case with PSPs. However, in case such an IT platform is provided in the Proposal, the EDPB highlights the need for the Proposal (for instance, in a Recital) to adequately demonstrate the necessity and proportionality of the interference with individuals' fundamental right to the protection of personal data;
 - defines the term "information sharing agreement" in the enacting terms of the PSR;
 - limits the transmission of data to what is strictly necessary to warn the other PSP of fraudulent payment transaction. In this respect, the EDPB is concerned that amendments proposed by

¹³ As proposed in the EP Report, in new final paragraph of Article 83(2) of the PSR Proposal.

¹⁴ According to the EBA, inherence "includes biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these". See EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06), para. 18, avilable at:

 $[\]frac{https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf$

¹⁵ See also EBA answer 2020_5353 On the requirements for 'inherence' in strong customer authentication (SCA), available at: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5353

¹⁶ As proposed in the EP Report, in new Article 83(3a) of the PSR Proposal.

¹⁷ As proposed in the EP Report, in new Article 83(4a) of the PSR Proposal.

- the EP to Article 83(2) of the Proposal would significantly enlarge the scope of transmitted data to cover not only the IBAN of the payee but also detailed personal data about them¹⁸;
- limits access to transmitted data by the receiving PSP to authorised and qualified staff of the PSPs;
- clarifies in a recital what would constitute sufficient evidence under Article 83(3) of the PSR Proposal and includes in the enacting terms of the Proposal the fact that such evidence should be shared with the receiving PSP, in order to enable the receiving PSP to take appropriate and proportionate measures;
- provides that, in the event a PSP shares information with another PSP, this should not automatically lead to the blocking of the execution of the payment order by the PSPs without further analysis, but could instead justify a more in-depth check of the transaction.
- 2.2 Obligations for Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) under the PSR Proposal

Transparency

13. The EDPB takes the view that Article 43(4)(b) of the PSR Proposal should include an obligation for PISPs and AISPs to inform account servicing PSPs about the customer account to which access is being sought. In addition, PISPs and AISPs should inform the account servicing PSP about the legal basis under Article 6(1) GDPR and (if applicable) the exception under Article 9(2) GDPR that they would rely on to access the personal data of the payment service user.

Data minimisation

- 14. The EDPB recalls that, in accordance with the principle of minimisation enshrined in Article 5 (1) (c) GDPR, access to personal data by AISPs and PISPs should be limited to personal data that are strictly necessary to provide the requested service to the customers. ¹⁹ Moreover, the EDPB recalls that the controller must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each purpose of the processing are processed pursuant to the obligations to respect the requirements of data protection by design and by default established in Article 25(1) and 25(2) of the GDPR²⁰.
- 15. In this regard, the EDPB notes that large amounts and a wide variety of categories of personal data will likely be shared by data holders with data users under the FIDA Proposal and by account servicing PSPs with PISPs and AISPs under the PSR Proposal. Therefore, the EDPB recommends having due regard to the data minimisation principle²¹ in the context of the rules for the exchanges of financial data in the Proposals. Compliance with this principle is of paramount importance in the context of financial services not only under the privacy and data protection

Adopted 5

.

¹⁸ As proposed in the EP Report, in the proposed amendments to Article 83(3) of the PSR Proposal, referring to name, personal identification number, organisation number, modus operandi and other transaction information of a payee.

¹⁹ See, in this regard, EDPB Guidelines 06/2020, paras. 59-67.

²⁰ See in this regard, EDPS Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, Adopted on 20 October 2020, available at:

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb guidelines 201904 dataprotection by design and by default v2.0 en.pdf

²¹ Article 5(1)(c) GDPR.

- viewpoint, but also to limit the risk of financial exclusion which might arise due to the collection and storage of personal data that is financially irrelevant²².
- 16. The EDPB therefore welcomes that the ECON Committee's report would significantly limit the scope of data sharing in the FIDA Proposal, such as excluding data which is derived or inferred from data provided by a customer as a result of profiling from the scope of the Proposal²³. The principle of data minimisation is furthermore covered in Recital 10 of the FIDA Proposal and will be implemented via technical requirements in so-called Financial Data Sharing Schemes that data holders and data users must adhere to.
- 17. However, Article 47 of the PSR Proposal would not limit access to personal data by AISPs to data that are strictly necessary to provide the requested service. Based on the experience of national data protection authorities in their supervisory activities, it can be noted that AISPs often access more personal data than they should when requesting the account information necessary to provide their respective service. The access to such unnecessary information is not in line with the principle of data minimisation. Therefore, the EDPB calls for expressly including the obligation for account servicing PSPs to deploy technical measures that enable or support AISPs and PISPs in their obligation to access and retrieve only the personal data that is necessary for the provision of their services²⁴, in the PSR Proposal.

2.3 The legal meaning of the term 'permission' under the FIDA and PSR Proposals

- 18. The EDPB welcomes the further clarifications proposed by the ECON committee to the FIDA Proposal on the legal meaning of the term "permission", which is used instead of the notion of "explicit consent"²⁵. The ECON Committee report on the FIDA Proposal clarifies that 'permission' should not be construed as 'consent' or 'necessity for the performance of a contract' under the GDPR²⁶. The EDPB welcomes this amendment, as it considers it important to disambiguate the term 'permission' from the data protection legal basis provided under the GDPR.
- 19. The EDPB calls for the inclusion of a similar clear differentiation between the term 'permission' and the legal basis for processing under the GDPR, in particular the legal basis of 'necessity for the performance of a contract', in the legal text of the PSR Proposal²⁷.
- 20. The EDPB also strongly recommends to reconsider Article 49(4) of the PSR Proposal, which states that account servicing PSPs must not verify the permission granted by the payment service user to AISPs and PISPs. It should on the contrary be possible for account servicing PSPs to verify the permission obtained by AISPs and PISPs from the customer before granting them access to her or his account information.

²² This is one of the objectives pursued by the FIDA Proposal, as explicitly mentioned in Recital 15 of the Proposal.

²³ As proposed in the EP Report, in the amended Recital 9 of the FIDA Proposal.

²⁴ See EDPB Guidelines 06/2020, para. 64.

²⁵ The term "explicit consent" is currently used in Article 94 of PSD2. The EDPB has had the chance to clarify that the term in that provision does not equate to "consent" under the GDPR, given that under PSD2 it is a contractual consent and cannot be regarded as an additional legal basis for processing of personal data. See EDPB Guidelines 06/2020, paras. 36 and 37.

²⁶ As proposed in the EP Report, in the amended Recital 48 of the FIDA Proposal.

²⁷ Article 65a of the EP Report on the PSR Proposal only distinguishes 'permission' from 'consent'.

2.4 Requirements for permission dashboards under the FIDA and PSR Proposals

- 21. The EDPB calls on the co-legislators to specify in Article 43 of the PSR Proposal that the permission dashboard should not be designed in a way that would unduly influence payment service users to grant or withdraw permissions, in line with Recital 65.
- 22. In relation to the FIDA Proposal, the EDPB calls for the permissions dashboard under Article 8 of the Proposal to require data users to inform data holders about the legal basis under Article 6(1) GDPR and (if applicable) the exception under Article 9(2) GDPR that they rely on to access personal data contained in the customer dataset.

2.5 Special categories of personal data under the PSR Proposal

- 23. The EDPB recalls that processing of special categories of personal data under the GDPR is prohibited, pursuant to Article 9(1), and only allowed if any of the exceptions in Article 9(2) applies. Therefore, the EDPB calls on the co-legislators to specify in the PSR Proposal in relation to which specific, designated payment service the providers of payment systems and PSPs are allowed to process specific special categories of personal data pursuant to Article 80. Furthermore, justifications as to why the processing of special categories of personal data for specific payment services is necessary and proportionate and cannot be avoided via alternative means should be provided in a Recital.
- 24. The EDPB also reiterates the recommendation made by the EDPS to clarify the definition of 'sensitive payment data' (referred to, in broad way, as "data which can be used to carry out fraud, including personalised security credentials")²⁸ by further specifying the categories of personal data falling under this definition.

2.6 Regulatory cooperation under the PSR Proposal

- 25. The EDPB notes that the Article 93(3) of the PSR Proposal provides that competent authorities shall cooperate with "other authorities from any sector concerned as applicable to each case".
- 26. The EDPB recommends that the PSR Proposal expressly refers to cooperation between the authorities which are competent for the supervision of the provisions of the PSR Proposal and data protection supervisory authorities. These authorities should exchange information with each other to ensure cooperation on their respective supervisory tasks. This is necessary for the effective and coherent enforcement of administrative sanctions and administrative measures, in particular where the same practices by entities covered by the Proposals and EU data protection law could lead to sanctions from financial authorities and data protection supervisory authorities. Therefore, the EDPB recommends that data protection supervisory authorities are explicitly mentioned in Article 93(3) in line with Recital 97 and Article 48(5) of the PSR Proposal and that modalities for such cooperation be further specified, notably with regard to the exchange of confidential information.

For the European Data Protection Board
The Chair
(Anu Talus)

²⁸ Article 3(38) of the PSR Proposal.