EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

22 August 2023

Opinion 39/2023

on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under ***Article 42(1)*** *of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.*

This Opinion relates to the Proposal for a Regulation on payment services in the internal market[1] and the Proposal for a Directive on payment services and electronic money services in the Internal Market[2]. This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725. This Opinion is limited to the provisions of the Proposal that are relevant from a data protection perspective.

[1] COM(2023) 367 final.
[2] COM(2023) 366 final.

Executive Summary

On 28 June 2023, the European Commission issued a 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 (the 'PSR Proposal') and a 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 (the 'PSD3 Proposal'), together 'the Proposals'.

Payment services often involve processing of personal data which can reveal sensitive information about an individual data subject. The EDPS therefore welcomes the efforts made to ensure consistency with the General Data Protection Regulation ('GDPR'). He also stresses the need to clearly differentiate the 'permissions' under Proposal from and the legal basis for processing of personal data under the GDPR.

One of the aims of the Proposal is to enable providers of payment systems and of payment services to process special categories of personal data in the public interest of the well-functioning of the internal market for payment services. As the processing of such data is liable to constitute a serious interference with the rights to respect for private life and to the protection of personal data, it is important that legislation be precise enough to show the objective connection between each category of data in a specific payment context and the public interest objective to be achieved.

The EDPS welcomes that the Proposal would require account servicing payment service providers ('ASPSPs') to provide the user with a dashboard to monitor and manage the permission she or he has granted. To further reduce the risk of unlawful sharing of personal data by ASPSPs, the EDPS recommends:

◦ ensuring that the dashboard makes reference to the specific designated payment service(s) for which she or he granted her/his permission;

◦ ensuring that access requests remain limited to what is necessary to provide the requested service;

◦ ensuring clarity regarding the legal basis of access requests;

◦ allowing ASPSPs to verify the permission granted by the payment service user or to introduce appropriate alternative safeguards in the PSR Proposal.

Finally, the EDPS recommends ensuring close cooperation between competent authorities under the Proposal and data protection supervisory authorities to ensure consistency between the application and enforcement of the Proposal and EU data protection law. The EDPS therefore recommends expressly referring to supervisory authorities responsible for monitoring and enforcing data protection law in Article 93(3) of the PSR Proposal.

Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ('EUDPR')[3], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 28 June 2023, the European Commission issued a 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 (the 'Payment Services Regulation Proposal' or 'PSR Proposal')[4] and a 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 (the 'Payment Services Directive 3 Proposal' or 'PSD3 Proposal')[5], hereinafter referred together as 'the Proposals'.

2. Three Annexes accompany both the PSR Proposal and the PSD3 Proposal (six Annexes in total), outlining the types of payment services (Annex I), as well as the type of electronic money services (Annex II) falling under the scope of the draft Proposals. Finally, Annex III provides a correlation table on the provisions of Directives 2015/2366/EU and 2009/110/EC with the provisions in the Proposals.

3. The EDPS notes that the types of services covered by the Proposals seem to be essentially the same as the ones covered by 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 ('PSD2')[6].

4. The specific objectives of the PSR Proposal[7] are to:

    a. strengthen user protection and confidence in payments, notably by: improving the application of Strong Customer Authentication (SCA); creating a legal basis for exchange of information on fraud; extending International Bank Account Number

[3] OJ L 295, 21.11.2018, p. 39.
[4] COM(2023) 367 final.
[5] COM(2023) 366 final.
[6] 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, 23.12.2015, p. 35.
[7] COM(2023) 367 final, page 5-6.

('IBAN') verification to all credit transfers; and improving user rights and information;

b. improve the competitiveness of open banking services by: (i) requiring account servicing payment service providers ('ASPSPs') to put in place a dedicated data access interface and "permissions dashboards" to allow users to manage their granted open banking access permissions; and (ii) setting out more detailed specifications of minimum requirements for open banking data interfaces;

c. improve enforcement and implementation of the legal framework for payment services in Member States, notably by: replacing the PSD2 with a directly applicable Regulation ('PSR Proposal') clarifying aspects of the PSD2 which are unclear; and improving cooperation between competent authorities and other authorities; and

d. improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs, including payment initiation service providers (PISPs) and account initiation service providers (AISPs).

5. The Proposals are presented in conjunction with the Proposal for Regulation on Financial Information Data Access ('the FIDA Proposal')[8], covering among others access to financial data other than payment account data, which falls under the scope of the Proposals that form the subject matter of the present Opinion[9].

6. In essence, the PSR Proposal would:

   a. establish requirements on transparency of conditions and information requirements for payment services[10];

   b. establish rights and obligations in relation to the provision and use of payment services, including rules on data access interfaces for account information services and payment initiation services[11] and on data access management by payment service users[12]; on data protection[13]; on fraud reporting and transaction monitoring mechanisms and fraud data sharing[14]; on SCA[15]; on enforcement procedures, competent authorities and penalties[16]; on intervention powers by the European Banking Authority (EBA)[17].

7. The PSD3 Proposal is largely based on Title II of the current PSD2, regarding "Payment Service Providers", which only applies to payment institutions. It updates and clarifies the provisions relating to payment institutions and integrates electronic money institutions as a sub-category of payment institutions. It also includes provisions concerning cash withdrawal services provided by retailers or independent ATM deployers[18].

[8] COM(2023) 360 final.
[9] COM(2023) 367 final, page 4.
[10] Articles 4-26 of the PSR Proposal.
[11] Articles 35-38 of the PSR Proposal.
[12] Article 43 of the PSR Proposal.
[13] Article 80 of the PSR Proposal.
[14] Articles 82-84 of the PSR Proposal.
[15] Articles 85-86 of the PSR Proposal.
[16] Chapter 8 of the PSR Proposal.
[17] Chapter 9 of the PSR Proposal.
[18] COM(2023) 367 final, page 7.

8. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 29 June 2023, pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 147 of the PSR Proposal and Recital 77 of the PSD3 Proposal. In this regard, the EDPS also positively notes that he was already previously informally consulted on the Proposals pursuant to Recital (60) of the EUDPR.

2. General remarks

9. The EDPS recognises the importance of strengthening user protection and confidence in payments. He also supports the aim of improving the enforcement and implementation of the regulatory framework applicable to payment services in Member States, as well as the aim of improving the competitiveness of open banking services.

10. The Explanatory Memorandum to the PSR Proposal notes that the fundamental right to data protection is particularly concerned by this Proposal[19]. It also underlines that the processing of personal data must be in line with the General Data Protection Regulation ('GDPR')[20], which applies directly to all of the payment services concerned by the PSR Proposal.[21]

11. The EDPS welcomes Recital 97 of the PSR Proposal, stating in particular that where personal data are processed, the processing should comply with the GDPR, including the principles of purpose limitation, data minimisation and storage limitation. He also welcomes the explicit confirmation that the supervisory authorities under the GDPR and the EUDPR should be responsible for the supervision of processing of personal data carried out in the context of the PSR Proposal. The EDPS also welcomes Recital 99 of the PSR proposal, specifying that the provision of information to individuals about the processing of personal data should be carried out in accordance with the GDPR and the EUDPR.

12. The EDPS notes that PSR Proposal seeks to ensure coherence with the FIDA Proposal. In this regard, the EDPS refers to the recommendations made in his Opinion on the FIDA Proposal, in particular in relation the term 'permission', which is referred to both in the PSR Proposal and in the FIDA Proposal.

3. The role of 'permissions'

13. The EDPS welcomes that the PSR Proposal aims at addressing some of the interactions between the PSD2 and the EU data protection framework. One such interaction, also

[19] COM(2023) 367 final, page 8.
[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.
[21] COM(2023) 367 final, page 8.

mentioned in the Guidelines issued by the EDPB on the matter[22], concerns the distinction between 'explicit consent' under the PSD2, on the one hand, and 'consent' and 'explicit 'consent' under the GDPR, on the other hand.

14. The EDPS remarks that Recital 69 of the PSR Proposal specifies that "*(..) permission should not be construed exclusively as 'consent' or 'explicit consent' as defined in Regulation (EU) 2016/679*". The EDPS considers that the term 'exclusively' introduces a degree of uncertainty and does not allow to differentiate clearly between 'permission' (referring to the acceptance of the commercial service by the consumer), on the one hand, and 'consent' (under Article 6(1)(a) GDPR) or 'explicit consent' (under Article 9(2)(a) GDPR), on the other hand. Recital (69) should therefore be amended to clarify that "*permission should not be construed as 'consent' or 'explicit consent' or 'necessity for the performance of a contract' as defined in Regulation (EU) 2016/679*"[23].

15. The EDPS also recommends specifying - similarly to recital 10 of the FIDA Proposal - the need for payment initiation service providers (PISPs) and account information service providers (AISPs) to secure a lawful ground under the GDPR to process personal data[24]. Likewise, the EDPS recommends clarifying that the granting of permission by a payment service user is without prejudice in particular to the obligations of data users under Article 6 and Article 9 of the GDPR[25].

4. Verification of the permission by the ASPSP

16. The EDPS notes that Article 43(4)(b) of the PSR Proposal would require payment initiation service providers (PISPs) and account information service providers (AISPs) to inform account servicing payment service providers ('ASPSPs') in real time of a new permission granted by a payment service user.

17. The EDPS is concerned, however, that Article 44(1)(c) and Article 49(4) of the PSR Proposal would prevent ASPSPs from verifying the permission given by the payment service user to PISPs and AISPs to access their payment account information. Although the term 'permission' should not be construed as 'consent' or 'explicit consent' within the meaning of the GDPR, a prohibition to verify the permission given by the user may lead ASPSPs to

[22] EDPB Guidelines in 2020 on the interplay of the Second Payment Services Directive and the GDPR, adopted on 15 December 2020, paragraph 44.

[23] In the same vein, the EDPS and the EDPB have recommended to avoid any ambiguity between the term 'permission' within the meaning of the Data Governance Act ('DGA') and legal basis under Article 6 GDPR. See EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), version 1.1, adopted on 9 June 2021, paragraphs 41, 45, 47, 48, 49, 50, 102; see in particular paragraph 50: *"The EDPB and the EDPS also remark that in case of processing of personal data the "permission" referred to in the Proposal cannot replace the necessity of one appropriate legal ground under Article 6(1) of the GDPR for the lawful processing of personal data. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that at least one of the legal basis under Article 6(1) of the GDPR applies. The Proposal should clearly specify this aspect to avoid any ambiguity."*

[24] Recital (10) of the FIDA Proposal states that "*Where the processing of personal data is involved, a data user should have a valid lawful basis for processing under Regulation (EU) 2016/679*".

[25] See in the same vein also Recital 48 of the FIDA Proposal "*The granting of permission by a customer is without prejudice to the obligations of data users under Article 6 of Regulation (EU) 2016/679. Personal data that are made available and shared with a data user should only be processed for services provided by a data user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, when applicable, where the requirements of Article 9 of that Regulation on the processing of special categories of data are met.*"

share personal data with third parties that have *not* secured an appropriate lawful ground under the GDPR (or to share more personal data than intended by the user).

18. Each controller has the duty to ensure that personal data are not further processed in a manner that is incompatible with the purposes for which they were originally collected. Each disclosure by a controller requires a lawful basis and assessment of compatibility, regardless of whether the recipient is a separate controller or a joint controller[26]. Therefore, the EDPS invites the colegislator to reconsider the prohibition applicable to ASPSPs to verify the permission under Article 44(1)(c) and Article 49(4) of the PSR Proposal. In particular, the EDPS recommends to either (i) delete the prohibition applicable to ASPSPs to verify the data access permission under Article 44(1)(c) and 49(4) of the PSR Proposal; or (ii) to introduce appropriate safeguards to protect payment service users against the risk of potential unlawful sharing of personal data by ASPSPs that this prohibition may entail.

5. Strong customer authentication procedures and use of personalised security credentials

19. In 2014, the European Central Bank ('the ECB') recommended that "*There should be no sharing of credentials between the TPPs [Third Party Providers] and the account-servicing PSP; the TPP should either redirect the payer in a secure manner to its account servicing payment service provider or issue its own credentials. Both options should form part of a standardised European interface for payment account access that needs to be developed.*"[27] In 2016, the EBA Banking Shareholder Group also stated: "*In order to protect the consumers, reduce risk and avoid fraud, we recommend that PSC [Personalised Security Credentials] should not be accessed directly by TPP [Third Party Providers]*"[28].

20. The EDPS notes that Article 86(2) of the PSR Proposal would allow PISPs and AISPs to 'rely on' the authentication procedures provided by the ASPSP to the payment service user. At the same time, PISPs would be prevented from 'storing' (Articles 46(2)(a)) and AISPs would be prevented from 'requesting' (Article 47(2)(a)) 'sensitive payment data', which includes 'personalised security credentials'[29].

21. The EDPS considers that any possible sharing with PISPs and AISPs of the credentials that the payment service user uses to authenticate with the ASPSP would create unnecessary risks[30] and should therefore be excluded. To avoid any possible ambiguity, the EDPS

---

[26] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 7 July 2021, p. 45 (paragraph 167 and footnote 76).

[27] ECB Final Recommendations for the security of payment account access services following public consultation, May 2014, page 5.

[28] Draft BSG response to EBA/DP/2015/03 on future draft regulatory technical standards on strong customer authentication and secure communication under the revised payment services directive (psd2), page 2.

[29] Under Article 3(38) of the PSR Proposal, "'*sensitive payment data' means data which can be used to carry out fraud, including personalised security credentials.*"

[30] Storing the PSU's credentials in multiple storage location would increase the attack surface and therefore the risk of unauthorised access (e.g. due to a data breach). Moreover, access to PSU's credentials would increase the risk of unauthorised data processing, since the credentials could be used by AISPs or PISPs to bypass the allowed use of the dedicated data access interface (e.g. an AISP connecting to the web interface of the ASPSP). In addition, allowing the PSU to share with third parties the credentials they use to authenticate with the ASPSP would be in breach of best practices and standards on security. For example, ISO 27002:2022 lists among the user responsibilities to requirement to keep confidential "*secret authentication information such as passwords*", while also stating, "*Personal secret authentication information is not to be shared with anyone.*"

recommends amending Articles 46(2)(a) and 47(2)(a) of the PSR Proposal to state that PISPs and AISPs shall not access (and not merely 'not store' or 'not request') personalised security credentials provided by the ASPSP.

22. Article 89(1) would require the EBA to develop draft regulatory technical standards to specify the requirements of strong customer authentication (SCA). The EBA would also be required to specify the requirements with which security measures have to comply to protect the confidentiality and the integrity of the payment service users' personalised security credentials[31]. The Commission would be delegated the power to adopt the standards developed by the EBA in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010. In this regard, the EDPS reminds the Commission of its obligation to consult the EDPS when preparing delegated or implementing acts that would impact on the protection of individuals' rights and freedoms with regard to the processing of personal data pursuant to Article 42(1) of the EUDPR.

23. Finally, the EDPS also recommends clarifying the definition of 'sensitive payment data' under Article 3(38) of the PSR Proposal (referred to, in broad way, as "*data which can be used to carry out fraud, including personalised security credentials.*") by further specifying the categories of personal data falling under this definition.

6. Special categories of personal data

24. Financial transactions can reveal sensitive information about an individual data subject, including those related to special categories of personal data[32]. Article 80 of the PSR Proposal, read in the light of Recital 98 of the PSR Proposal, states that payment systems and payment service providers must be allowed to process special categories of personal data as referred to in Article 9(1) GDPR and Article 10(1) EUDPR to the extent necessary for the provision of payment services and for compliance with obligations under this Regulation in the public interest of the well-functioning of the internal market for payment services, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. Article 80 also provides a (non-exhaustive) list of such safeguards.

25. Article 9(2)(g) GDPR, which allows for an exception to the prohibition to process special categories of personal data under Article 9(1) GDPR for reasons of substantial public interest, is qualified by a number of conditions and should be interpreted restrictively[33]. These conditions are: (i) the processing of personal data must be necessary for the stated purpose; (ii) it must be based on a Union or Member State law; and (iii) the Union or

---

[31] Article 89(1)(a) and (c) of the PSR Proposal; Article 89(2)(b) of the PSR Proposal provides that, when developing the regulatory technical standards, the EBA shall take into account "the need to ensure the safety of payment service users' funds and personal data".

[32] See EDPB Guidelines on the interplay of the PSD2 with the GDPR, adopted on 15 December 2020, paragraph 52. See also judgment of the Court of Justice of 1 August 2022, *OT v Vyriausioji tarnybinės etikos komisija*, C-184/20, ECLI:EU:C:2022:601, paragraphs 117-128 and judgment of the Court of Justice of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, ECLI:EU:C:2023:537, paragraphs 69-73.

[33] See judgment of the Court of Justice of 4 July 2023, *Meta Platforms and Others* (General terms of use of a social network), C-252/21, ECLI:EU:C:2023:537, paragraph 93 "[..] *the justifications provided for in that latter provision, in so far as they allow the processing of personal data carried out in the absence of the data subject's consent to be made lawful, must be interpreted restrictively (see, to that effect, judgment of 24 February 2022, Valsts ieņēmumu dienests (Processing of personal data for tax purposes), C-175/20, EU:C:2022:124, paragraph 73 and the case-law cited)"* and paragraphs 133-134.

Member State law itself must be proportionate to the specific objective pursued, respect the essence of the fundamental rights to privacy and to the protection of personal data; and provide for suitable and specific measures to safeguard the fundamental rights and the interests of individuals concerned[34].

26. The EDPS considers that Article 80 of the PSR Proposal does not satisfy the requirements of necessity and proportionality. Under the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. They must apply only in so far as is strictly necessary and the legislation which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question[35]. Strict compliance with the principles of necessity and proportionality is particularly important where processing of special categories of personal data are concerned, as the processing of such data is liable to constitute a serious interference with the rights to respect for private life and to the protection of personal data. In light of the seriousness of the interference entailed by the processing of special categories of data, it is important that legislation be precise enough to show the objective connection between each category of data in a specific payment context and the public interest objective to be achieved.

27. In order to satisfy the requirements of necessity and proportionality, the PSR Proposal should:

    a. further delineate the specific purposes of the processing, by specifying the type(s) of payment service(s)[36] for which the payment systems and payment service providers would be entitled to process which special categories of personal data[37]. The PSR Proposal should also provide justifications (in a recital) as to why the processing of the special categories of personal data for the designated service at stake is strictly necessary and cannot be avoided (i.e. it would not be possible to avoid processing of such data); and

    b. clearly indicate which special categories of personal data would be necessary to achieve the specific purpose and to whom (exactly which type of commercial operators) this legal basis would apply.

28. The EDPS considers that in some cases, for instance with regard to the multi-factor authentication of the payment service user, where it is possible to use non-biometric means

[34] See also EDPS Opinion 33/2023 on the Proposal for a Regulation in matters relating to the protection of adults, issued on 18 July 2023, paragraphs 14-15.
[35] Judgment of the Court of Justice of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 105.
[36] Although the types of services covered by the PSR Proposal seem to be substantially the same as the ones under the PSD2, Recital 26 also highlights that new open banking-based business model requires a modification of the definition of account information services to clarify that the information aggregated by the authorised account information service provider may be transmitted to a third party to enable that third party to provide another service to the end-user, with the end-user's permission.
[37] See also the EDPB Guidelines on the interplay of the PSD2 with the GDPR, adopted on 15 December 2020, paragraph 56 [emphasis added]: "*Payments services may process special categories personal data for reasons of substantial public interest, but only when all the conditions of Article 9(2)(g) of the GDPR are met. This means that the processing of the special categories of personal data has to be addressed in a specific derogation to article 9(1) GDPR in Union or Member State law. This provision will have to address the proportionality in relation to the pursued aim of the processing and contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Furthermore, this provision under Union or Member State law will have to respect the essence of the right to data protection. Finally, the processing of the special categories of data must also be demonstrated to be necessary for the reason of the substantial public interest, including interests of systemic importance. Only when all of these conditions are fully met, this derogation could be made applicable to designated types of payment services.*"

of authentication, (explicit) consent of the data subject may be a more appropriate ground for processing sensitive data in accordance with Article 6 and 9 of the GDPR.

29. As regards the safeguards required under Article 9(2)(g) GDPR, the EDPS welcomes the non-exhaustive list of safeguards provided in Article 80 of the PSR Proposal. However, the EDPS recommends also including a reference to log in registration (to verify if undue access took place) requirements.

7. Provision of dedicated access interfaces

30. The EDPS notes that Article 35(6) of the PSR Proposal on the setting up of a testing facility by ASPSPs for their dedicated interface prohibits the sharing of "sensitive payment data or any other personal data" through the facility. The EDPS welcomes this specification since personal data as a rule should also not be processed when testing a functionality, in line with the principles of data minimisation and of data protection by design and by default[38].

8. Data access management

31. The EDPS welcomes Article 43, requiring ASPSPs to provide the payment service user with a dashboard to monitor and manage the permission she or he has granted to AISPS or PISPs covering multiple and recurrent payments. With regard to the information which ASPSPs would be required to convey to payment service users via the dashboard[39], the EDPS welcomes in particular the reference to "the categories of data being shared"[40]. This addition contributes ensuring effective overview and control of personal data flows by the payment service user that is a data subject under the GDPR. However, the EDPS recommends adding to Article 43(2)(a) a reference to the designated service(s) for which the permission is granted[41].

32. Concerning the specific obligations of PISPS and AISPs, the EDPS welcomes in particular the limitation that PISPs and AISPs can process personal data only for the provision of the payment or account information service for which the payment service user has granted her or his permission[42]. The EDPS notes, however, that the requirement under letter (b) of Article 46(2), according to which PISPs can request from the payment service user only the data that are necessary to provide the (payment initiation) service, is not included *mutatis mutandis* in Article 47(2), concerning the obligations of AISPs. He therefore recommends inserting an equivalent provision in Article 47(2) of the PSR Proposal.

---

[38] Article 5(1)(c) and Article 25(1) GDPR.
[39] According to Article 43(2) of the PSR Proposal, the dashboard must provide the PSU with information on:
(i) the name of the account information service provider or payment initiation service provider to which access has been granted;
(ii) the customer account to which access has been granted;
(iii) the purpose of the permission;
(iv) the period of validity of the permission;
(v) the categories of data being shared.
See also Recital 65 of the PSR Proposal.
[40] Article 43(2)(v) of the PSR Proposal.
[41] In line with Article 8(2)(a)(ii) of the FIDA Proposal.
[42] See Article 46(2)(c) and 47(2)(b) of the PSR Proposal.

33. The EDPS also takes positive note of the requirement for ASPSPs to provide payment service users via the dashboard an overview of each ongoing permission given for the account information service(s) or payment initiation service(s), including: the name of the PISP or AISP to which access has been granted; the customer account to which access has been granted; the purpose of the permission; a description of the categories of data being shared; and the period of validity of the permission[43]. To ensure that ASPSPs are able to convey all elements of information under Article 43(2) of the PSR Proposal to payment service users, the EDPS recommends that PISPs and AISPs are required under Article 43(4)(b) to also inform ASPSPs about the customer account to which access is being sought.

34. Additionally, the EDPS recommends that Article 43(4)(b) of the PSR Proposal requires PISPs and AISPs to inform ASPSPs 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 (special categories of) personal data of the payment service user. This would help prevent ASPSPs from granting access to personal data in the absence of an appropriate GDPR legal basis[44].

35. The EDPS welcomes the requirement under Article 43(3) of the PSR Proposal that the dashboard should be "*easy to find in its user interface and that information displayed on the dashboard is clear, accurate and easily understandable for the payment service user*". Recital 65 of the PSR Proposal adds that the dashboard "*should empower customers to manage their permissions in an informed and impartial manner and give customers a strong measure of control over how their personal and non-personal data is used.*"

36. Indeed, in a sensitive area such as payment services, consumers may be particularly unaware of the consequences of sharing their personal data with payment service providers[45]. The EDPS therefore recommends that the PSR Proposal, notably Article 43(b), specifies that the dashboard should not be designed in a way that would unduly influence payment service users to grant or withdraw permissions.

9. Transaction monitoring mechanisms and fraud data sharing

37. Article 83 of the PSR Proposal would establish the obligation for payment service providers to have transaction monitoring mechanisms in place that, among others, enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving PISPs[46].

[43] Article 43(2)(a) of the PSR Proposal.
[44] See also paragraphs 17 and 18 of this Opinion.
[45] The Finance Innovation Lab, '[Open Finance and Vulnerability - A Policy Discussion Paper](#)', July 2021, page 9: "*Terms and conditions around data sharing are difficult to understand and time consuming to read. Researchers at the LSE have found that this makes determining 'informed consent' in financial services very difficult. Contracts often involve complex data chains, which cede control of data to many more firms than is at first apparent. This can result in data sharing impacting access to multiple services. There is therefore a real danger that people will fail to understand the full implications of allowing access to open finance data.*", see also at page 10: "*There is a risk that data sharing becomes a prerequisite for accessing essential financial services.*"
[46] Article 83(1)(c) of the PSR Proposal.

38. Article 83(2) of the PSR Proposal establishes that transaction monitoring mechanisms would be "*based on the analysis of previous payment transactions and access to payment accounts online*" and specifies the data required for this purpose, namely: (a) information on the payment service user, including the environmental and behavioural characteristics which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials; (b) information on the payment account, including the payment transaction history; (c) transaction information, including the transaction amount and unique identifier of the payee; (d) session data, including the device internet protocol address-range from which the payment account has been accessed.

39. Article 83(3) also specifies that transaction monitoring mechanisms should consider, at a minimum, the following risk factors: (a) lists of compromised or stolen authentication elements; (b) the amount of each payment transaction; (c) known fraud scenarios in the provision of payment services; (d) signs of malware infection in any sessions of the authentication procedure; (e) the abnormal use of the access device or the software (in case the access device or the software is provided by the payment service provider).

40. The EDPS welcomes that the Proposal aims to set out, in an exhaustive manner, the categories of data that may be used for transaction monitoring mechanisms purposes. He notes, however, that certain categories of personal data remain considerably broad, taking into account that the Explanatory Memorandum mentions as "*environmental and behavioural characteristics*" the "*location of the payment service user, time of transaction, device being used, spending habits, online store where the purchase is carried out.*"[47]

41. The EDPS also notes that payment service providers already carry out data processing activities for fraud monitoring purposes on the basis of the Article 6(1)(f) GDPR (legitimate interests)[48]. This legal basis requires controllers - such as payment service providers - to carry out a careful balancing test. In order to rely on Article 6(1)(f) GDPR, three cumulative conditions should be met, namely: (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued, and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence[49].The new provisions in Article 83 of the PSR Proposal would, however, create a legal obligation for payment service providers to conduct such processing activities within the meaning of Article 6(1)(c) GDPR. While the processing should still be 'limited' to the categories of data listed, the Proposal does not require payment service providers to carry out a balancing exercise before processing personal data of PSUs for fraud monitoring purposes pursuant to the PSR Proposal.

42. As the PSR Proposal would provide for a legal obligation to process personal data, it should clearly define the boundaries of such processing. This requires clearly determining the categories of personal data that payment service providers would be allowed to process in the context of transaction monitoring mechanisms. In this regard, the EDPS recommends to provide a clear and comprehensive definition of the "information on the payment service user" referred to in Article 83(2)(a) of the Proposal. In addition, the EDPS recommends explicitly stating that the processing of the data categories listed in paragraph 2 may only be performed 'insofar as necessary' to achieve the purposes referred to in Article 83(1) of

[47] COM(2023) 367 final, page 13.
[48] See reference to fraud prevention in Recital 47 GDPR as one of the possible legitimate interests protected by Article 6(1)(f) GDPR.
[49] See Judgment of the Court of Justice of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 95.

the PSR Proposal. Finally, he recommends defining appropriate maximum data storage periods for the personal data collected under Article 83[50].

43. The EDPS welcomes that the information sharing arrangements between payment service providers must be preceded by a data protection impact assessment (DPIA) within the meaning of Article 35 GDPR, to be conducted jointly by the payment service providers participating in the arrangement[51], as well as to prior consultation when applicable under Article 36 GDPR. At the same time, the EDPS notes that the term "information sharing agreement" is not defined in the PSR Proposal and recommends including a definition in Article 3 of the PSR Proposal.

44. The EDPS welcomes that the processing of personal data in accordance with the information sharing arrangement cannot lead to termination of customer relationship with the payment service provider or affect his or her future on-boarding by another payment service provider[52]. This is an important safeguard with regard to the possible impact on the person concerned by the processing of personal data in the context of transaction monitoring mechanisms. However, the EDPS recommends expressly providing in the PSR Proposal - more broadly - that *any* processing of personal data for the purpose of complying with the fraud prevention legal obligations under Article 83 (not only pursuant to Article 83(4)) can only occur for the specific purpose of fraud prevention and cannot lead to termination of customer relationship with the payment service provider or affect the on-boarding of the payment service user with another payment service provider.

45. The EDPS notes that the technical requirements for transaction monitoring mechanisms would be specified in draft regulatory technical standards developed by the EBA and adopted by the Commission via an implementing act[53]. In this regard, the EDPS reminds the Commission of its obligation to consult the EDPS when preparing implementing acts that would impact on the protection of individuals' rights and freedoms with regard to the processing of personal data pursuant to Article 42(1) of the EUDPR.

10. Competent authorities

46. According to Article 91(2) of the PSR Proposal, Member States must designate competent authorities to ensure and monitor effective compliance with the PSR Proposal. These authorities would be either (a) public authorities or (b) bodies recognised by national law or by public authorities expressly empowered for that purpose by national law, including national central banks. Article 93(3) provides that in the exercise of their investigatory and sanctioning powers, including in cross-border cases, competent authorities must cooperate with each other and ensure mutual assistance to the other authorities concerned.

47. Recital 130 of the PSR Proposal rightly stresses that the effectiveness of the legal framework for payment services depends on cooperation between competent authorities, including

[50] See also Recital 102 of the PSR Proposal.
[51] Article 83(4) of the PSR Proposal.
[52] Article 83(6) of the PSR Proposal.
[53] Article 89(1)(g) and (2) of the PSR Proposal.

national authorities responsible for data protection[54]. The EDPS considers that such cooperation would contribute ensuring consistency between the application and enforcement of the PSR Proposal and EU data protection law.

48. In order to ensure a clear legal basis for the exchange of relevant information, the EDPS recommends that supervisory authorities responsible for monitoring and enforcing data protection law be explicitly mentioned in Article 93(3) of the PSR Proposal.

11. Publication of administrative sanctions and measures

49. Article 101(1) of the PSR Proposal provides that in the context of the publication on their website of decisions imposing an administrative sanction or administrative measure on legal and natural persons for breaches of this regulation, and where applicable, settlement agreements, the identity of the natural person subject to the decision imposing an administrative sanction or administrative measure would not be published. Only by derogation from Article 101(1), where the publication of the identity or other personal data of natural persons is deemed necessary by the competent authority, the national competent authority may publish also the identity of the person concerned[55].

50. The EDPS considers that the publication of personal data with the decisions of competent authorities should indeed be the exception, to be decided following a case-by-case assessment. This would leave the option, following such assessment, to competent authorities to publish said personal data in cases of serious infringements and where strong dissuasive effects are needed. The EDPS notes that the publication of personal data of persons who have been sanctioned for an infringement of the Regulation should only occur in duly justified exceptional cases, as making such types of personal data available to the general public could be considered as a serious interference with their fundamental rights enshrined in Articles 7 and 8 of the Charter.

51. Finally, the EDPS welcomes that Article 101(4) of the PSR Proposal states, in accordance with the principle of storage limitation[56], that personal data contained in the publication must be kept on the official website of the competent authority only if an annual review shows the continued need to publish that data to protect the stability of the financial markets or to ensure the effective enforcement of the PSR Proposal, and in any event for no longer than 5 years.

[54] See also Recital 76 of the PSD3 Proposal: "*Any personal data processing in the context of this Directive must comply with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725. Therefore, the supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 are responsible for the supervision of processing of personal data carried out in the context of this Directive.*"
[55] Article 101(2) of the PSR Proposal. See also Recital 136 of the PSR Proposal.
[56] Article 5(1)(c) GDPR.

12. Conclusions

52. In light of the above, the EDPS makes the following recommendations:

(1) to clearly differentiate between the term 'permission' and the legal basis for processing under the GDPR, by clarifying in Recital 62 of the PSR Proposal that „permission should not be construed as 'consent' or 'explicit consent' or 'necessity for the performance of a contract' as defined in Regulation (EU) 2016/679";

(2) to clarify, by way of a recital, that the granting of permission by the payment service user is without prejudice in particular to the obligations of payment initiation service providers and account information service providers under Article 6 and Article 9 of Regulation (EU) 2016/679;

(3) to reconsider the prohibition applicable to ASPSPs to verify the permission under Article 49(4) of the PSR Proposal or to introduce appropriate alternative safeguards in the enacting terms of the PSR Proposal to protect payment service users against the risk of potential unlawful sharing of personal data by ASPSPs that this prohibition may entail;

(4) to amend Articles 46(2)(a) and 47(2)(a) of the PSR Proposal to state that payment initiation service providers and account information service providers shall not access personalised security credentials;

(5) to clarify the definition of 'sensitive payment data' under Article 3(38) of the PSR Proposal, notably specifying the types of personal data covered by this definition;

(6) to specify in relation to which specific type(s) of designated payment service(s) the payment systems and the payment service provider would be entitled to process (which categories of) special categories of personal data in Article 80 of the PSR Proposal;

(7) to provide justifications (in a recital) as to why the processing of the special categories of personal data for the designated payment service(s) in Article 80 of the PSR Proposal is necessary and proportionate and cannot be avoided via alternative technical means;

(8) to include a reference to log in registration (to verify if undue access took place) among the data protection safeguards referred to in Article 80 of the PSR Proposal;

(9) to add to Article 43(2)(a) a reference to the designated payment service(s) for which the permission is granted by the payment service user;

(10) to add to Article 47(2), concerning the obligations of account information service providers, the requirement under Article 46(2)(b), according to which payment service providers can request from the payment service user only the data that are necessary to provide the requested service;

(11) to require payment service providers and account information service providers under Article 43(4)(b) to inform account servicing payment service providers about the customer account to which access is being sought and 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;

(12) to specify in Article 43(b) that the dashboard should not be designed in a way that would encourage or unduly influence payment service users to grant or withdraw permissions;

(13) to clearly determine the categories of personal data that payment service providers would be allowed to process in the context of transaction monitoring mechanisms (notably, providing a definition of "information on the payment service user" referred to in Article 83(2)(a));

(14) to define appropriate data storage periods for the personal data collected under Article 83;

(15) to include a definition of "information sharing agreement" in Article 3 of the PSR Proposal;

(16) to provide in the PSR Proposal that any processing of personal data for the purpose of complying with the fraud prevention legal obligations under Article 83 can only occur for this specific purpose and cannot lead to termination of customer relationship with the payment service provider or affect the on-boarding of the payment service user with another payment service provider;

(17) to explicitly mention supervisory authorities responsible for monitoring and enforcing data protection law in Article 93(3) of the PSR Proposal.

Brussels, 22 August 2023

Wojciech Rafał WIEWIÓROWSKI

p.o. Leonardo CERVERA NAVAS
Secretary-General