EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

22 August 2023

Opinion 38/2023

on the Proposal for a Regulation on a framework for Financial Data Access

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 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[1]*. 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) 360 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 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[2] ('the Proposal'). The objective of the Proposal is to promote the development of data-driven financial services and products by enabling consumers and firms to better control access to their financial data.

The EDPS welcomes that the Proposal seeks to empower customers - including data subjects - to decide how and by whom their data is used. He notes, however, that the definition of 'customer data' is particularly broad, potentially including personal data of a highly sensitive nature. The categories of personal data to be made available under the Proposal should be clearly circumscribed, taking into account the risks for individuals whose personal data would be accessed and used. The EDPS also recommends explicitly excluding data created as a result of profiling from the definition of 'customer data'.

The EDPS welcomes that the Proposal would impose several obligations on data holders and users that could have a positive effect on the level of protection of the personal data. To further this objective, data users should be obliged to clearly outline, for each request, the specific types of customer data they seek access to. The Proposal should also prohibit the denial of the financial services to customers who do not install and avail themselves of the permission dashboard or otherwise enable data sharing by data holders with data users under the Proposal.

The EDPS considers that a clearly identified and strongly enforced data use perimeter is necessary to delineate appropriate uses of personal data and to protect vulnerable consumers. In this regard, the EDPS welcomes that the Proposal provides for the development of guidelines by the European Banking Authority and the European Insurance and Occupational Pensions Authority, in cooperation with the European Data Protection Board (EDPB). To ensure that the guidelines are fully aligned with data protection law, the EDPS considers a formal consultation of the EDPB to be necessary. The EDPS also recommends extending the scope of the future guidelines to other relevant financial products and services, such as to mortgage credit agreements, payment services, other insurance products, investment products, and pension products. The guidelines should also elaborate, where appropriate, on the limits for combining 'customer data' with other types of personal data, such as personal data obtained from third party sources (e.g., social media networks or data brokers).

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. Such close cooperation could be fostered by clarifying the circumstances in which competent authorities may consult and exchange information with data protection authorities.

[2] COM(2023) 360 final.

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 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[4] ('the Proposal').

2. The Proposal aims to promote the development of data-driven financial services and products by enabling consumers and firms to better control access to their financial data[5]. By doing so, the Proposal would make it possible for consumers and firms to benefit from financial products and services beyond payments that are tailored to their needs based on the data that is relevant to them. At the same time, the Proposal aims to address the risks that are inherent to the increased sharing of and access to financial data[6].

3. The Proposal is a sectoral building block that fits into the broader European strategy for data and enables data sharing within the financial sector and with other sectors[7]. It is directly connected with one of the priorities of the Commission's Digital Finance Strategy for the EU, notably of creating a European financial data space to promote data-driven innovation, building on the European data strategy[8], including enhanced access to data and data sharing within the financial sector[9].

4. In essence, the Proposal would:
    a. establish the rules in line with which specific categories of 'customer data' - including personal data - in finance[10] may be accessed, shared, and used by financial

[3] OJ L 295, 21.11.2018, p. 39.
[4] COM(2023) 360 final.
[5] COM(2023) 360 final, p. 1.
[6] COM(2023) 360 final, p. 1-2.
[7] COM(2023) 360 final, p. 3.
[8] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on A European Data Strategy, COM(2020) 66 final, 19.02.2020.
[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, COM(2020) 591 final, 24.09.2020, p. 3 and 4.
[10] Listed in Article 2(1) of the Proposal.

institutions and financial information service providers ('FISPs') - the 'eligible entities'[11] - acting as either data holders[12] or users[13];

b. provide the customer - who may be a natural or legal person[14] - with the right to request that the data holder shares this data with a data user for the purposes and under the conditions agreed between the data user and the customer[15];

c. impose certain obligations on data users receiving data at the request of customers and set certain boundaries on how customer data may be used[16];

d. mandate the European Banking Authority ('EBA') and the European Insurance and Occupational Pensions Authority ('EIOPA') - in cooperation with the European Data Protection Board ('EDPB') - to develop targeted guidelines addressing areas where the data sharing and access envisaged in the Proposal could entail higher exclusion risks for customers[17], thereby establishing a 'data use perimeter'[18];

e. allow customers to monitor and manage the data permissions they have given to data users through financial data access permission dashboards (to be mandatorily set up by data holders)[19]; and

f. introduce requirements for the creation and governance of financial data sharing schemes ('FDSS') - of which data holders, data users and consumer organisations would be parties - to develop (*inter alia*) data and interface standards and a joint standardised contractual framework governing access to specific datasets[20].

5. 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 (54) of the Proposal. In this regard, the EDPS also positively notes that he was already previously informally consulted pursuant to Recital (60) of the EUDPR.

2. General remarks

6. The EDPS acknowledges the importance of ensuring that customers of financial institutions have the opportunity to benefit from open, fair, and safe innovation in the financial sector. He also positively remarks that the Proposal seeks to empower customers - including data subjects under EU data protection law - "*to decide how and by whom their financial data is*

[11] Listed in Article 2(2) of the Proposal.
[12] Article 3(5) of the Proposal: "'*data holder' means a financial institution other than an account information service provider that collects, stores and otherwise processes the data listed in Article 2(1)*".
[13] Article 3(6) of the Proposal: "'*data user' means any of the entities listed in Article 2(2) who, following the permission of a customer, has lawful access to customer data listed in Article 2(1)*".
[14] Article 3(2) of the Proposal.
[15] Article 5 of the Proposal.
[16] Article 6 of the Proposal.
[17] Notably, products and services related to the credit score of consumers and to risk assessment and pricing of consumers in the case of life, health and sickness insurance products. See also recital (18) of the Proposal.
[18] Article 7 of the Proposal.
[19] Article 8 of the Proposal.
[20] Titles IV and V of the Proposal.

used and entitled to grant firms access to their data for the purposes of obtaining financial and information services should they wish"[21].

7. Sharing of customer data under the Proposal between eligible entities would be controlled, as it is subject to the customer's request[22]. At the same time, the EDPS notes that, without appropriate safeguards - such as a clearly identified and strongly enforced data use perimeter[23] - more extensive data sharing and use could, in specific cases, lead to a risk of higher prices for important financial services or exclusion of customers with an unfavourable risk profile. In this regard, particular attention needs to be paid to services that inherently require risk mutualisation, such as insurance[24], or services that may be necessary in the daily life of citizens, such as consumer credit. Consumers in financial services are often the weaker party, subject to risks of abuse, fraud and exploitation[25], and often subject to information and power asymmetries *vis-à-vis* financial service providers.

8. The EDPS notes that the collection and use of personal data to assess creditworthiness will also be regulated by the revised consumer credit directive[26], which provides for clear limitations on the collection and use of personal data (notably, on special categories of personal data and data originating from social networks). The EDPS, as highlighted in his Opinion on the Proposal[27], recalls the importance of such limitations to help ensure among others the proportionality of the processing of personal data in the context of the provision of consumer credit. Proportionality of processing is also highly relevant having regard to access to other financial services such as mortgages or insurance as 'basic' services that are necessary for financial and social inclusion.

9. The EDPS welcomes that Recital (48) of the Proposal underlines that Regulation (EU) 2016/679 ('GDPR')[28] applies when personal data is processed in the context of the Proposal. However, there would be situations where eligible entities or EU bodies such as the EBA would be subject to EU legal acts concerning privacy and data protection other than the GDPR, notably to the EUDPR and the ePrivacy Directive[29]. The EDPS therefore recommends slightly redrafting the initial sentence of Recital 48 of the Proposal according to the following wording: "*Processing of personal data in the context of this Regulation should*

---

[21] Recital (2) of the Proposal.
[22] Articles 4 and 5(1) of the Proposal. See also SWD(2023) 224 final p. 65.
[23] See Article 7 of the Proposal.
[24] In its Impact Assessment, the Commission notes that "*Inappropriate use of financial information could lead to unfair bias or prejudice that is harmful for the consumer. Some consumers could be excluded from a market as a result, whilst those who may choose not to participate in data sharing may end up paying a higher price for services. Consumer associations participating in the Commission's Expert Group pointed to several types of financial exclusion risks related to increased data sharing in the absence of proper safeguards. This includes, amongst others, the risks that more granular risk selection may pose for vulnerable consumers with a higher risk profile. Moreover, there is a risk that consumers who do not decide to share their data may not get access to all the services and products offered. The risk-pooling nature of some sectors, such as insurance provision, could also be at stake, potentially resulting in higher prices for many.*" (SWD(2023) 224 final, p. 17).
[25] Consultative Group to Assist the Poor (CGAP) Technical Note 'Combining Open Finance and Data Protection for Low-Income Consumers', February 2023, p. 5.
[26] See Article 18(2) of the Proposal for a directive of the European Parliament and of the Council on consumer credits (COM(2021)0347 – C9-0244/2021 – 2021/0171(COD)), provisional agreement resulting from interinstitutional negotiations.
[27] See EDPS Opinion 11/2021 on the Proposal for a Directive on consumer credits, 26 August 2021, para. 17.
[28] 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.
[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

be carried out in accordance with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725, as well as, where applicable, with the ePrivacy Directive".

10. The EDPS notes that the Proposal builds on the Payment Services Directive ('PSD2')[30], which enables the sharing of payments account data for payment services and account information services and is currently under revision. He also notes that the Proposal seeks to ensure coherence with the Proposal for a Payment Services Regulation[31] ('PSR Proposal')[32]. In this regard, the EDPS refers to the recommendations made in his Opinion on the PSR Proposal, in particular in relation to the term 'permission', which is referred to both in the Proposal and in the PSR Proposal.

3. Data access and use

3.1. Categories of customer data

11. Article 2(1) of the Proposal outlines which categories of customer data fall within the scope of the Proposal. The following categories of customer data would be shared, accessed and used:
    a. Mortgage credit agreements, loans and accounts, except payment accounts as defined in PSD2[33], including data on balance, conditions and transaction. According to recital (13) of the Proposal, such customer data should also include information relating to sustainability needs and preferences.
    b. Savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate and other related financial assets and the economic benefits derived from such assets; including data collected for the purposes of carrying out an assessment of suitability and appropriateness in accordance with Article 25 of Directive 2014/65/EU[34] ('Market in Financial instruments Directive - MiFiD II'). According to recital (13) of the Proposal, such customer data should also include information relating to sustainability needs and preferences.

[30] 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 (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35.
[31] 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.
[32] Recital (49) of the Proposal.
[33] In contrast, Recital (12) of the Proposal states that "*Credit accounts covered by a credit line which cannot be used for the execution of payment transactions to third parties should be within the scope of this Regulation.*"
[34] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance OJ L 173, 12.6.2014, p. 349–496. Most notably, Article 25(2) and (3) MiFiD II require investment firms to "*obtain the necessary information regarding the client's or potential client's knowledge and experience in the investment field relevant to the specific type of product or service, that person's financial situation including his ability to bear losses, and his investment objectives including his risk tolerance*".

c. Pension rights in occupational pension schemes in accordance with Directive 2009/138/EC[35] ('Solvency II') and Directive (EU) 2016/2341[36] ('Institutions for Occupational Retirement Provision Directive - IORP II Directive'), or on the provision of pan-European personal pension products ('PEPP'), in accordance with Regulation (EU) 2019/1238[37]. According to recital (15) of the Proposal, this would include "*data on pension rights concerns in particular accrued pension entitlements, projected levels of retirement benefits, risks and guarantees of members and beneficiaries of occupational pension schemes.*"

d. The provision of non-life insurance products (e.g. insurance covering homes, vehicles and other property) in accordance with Solvency II, with the exception of sickness and health insurance products[38]. Recital (14) of the Proposal clarifies that such data should include both insurance product information - such as detail on an insurance coverage - and data specific to the consumers' insured assets. This would include data collected for the purposes of a demands and needs assessment and data collected for the purposes of an appropriateness and suitability assessment in accordance with (respectively) Article 20 and 30 of Directive (EU) 2016/97[39] ('IDD').

e. Data which forms part of a creditworthiness assessment of a firm which is collected as part of a loan application process or a request for a credit rating. According to recital (16) of the Proposal, this may include "*financial statements and projections, information on financial liabilities and arrears in payment, evidence of ownership of the collateral, evidence of insurance of the collateral and information on guarantees.*"

12. Personal financial data processed by payment service providers, insurance undertakings, providers of pension products and other financial institutions are inherently sensitive[40]. Therefore, the EDPS welcomes that certain categories of data have been excluded from the scope of the Proposal under Article 2(1)(a), (e) and (f), in particular customer data related to: payment accounts[41]; the provision of life, sickness and health insurance products; and data which forms part of a creditworthiness assessment of natural persons.

13. Notwithstanding the exclusion of certain categories of data, customer data within scope of Article 2(1) may still be highly sensitive in nature. According to the Commission's impact

---

[35] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (recast) (Text with EEA relevance) OJ L 335, 17.12.2009, p. 1–155.
[36] Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (recast) (Text with EEA relevance) OJ L 354, 23.12.2016, p. 37–85.
[37] Regulation (EU) 2019/1238 of the European Parliament and of the Council of 20 June 2019 on a pan-European Personal Pension Product (PEPP) (Text with EEA relevance) PE/24/2019/REV/1 OJ L 198, 25.7.2019, p. 1–63.
[38] See also SWD(2023) 224 final, p. 104 (underlining that "*Particular attention needs to be paid to services with inherent risk mutualisation of insurance, and how the personalisation of products may affect this model. Given the nature of sensitive personal data, overall risks around health data, for example, would be more severe.*")
[39] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast) Text with EEA relevance OJ L 26, 2.2.2016, p. 19–59.
[40] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, as last revised and adopted on 4 October 2017, p. 10: "*These personal data are considered as sensitive (as this term is commonly understood) because* (...) *their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud).*"
[41] European Data Protection Board (EDPB), Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 2.0, adopted on 15 December 2020, paragraph 52: "*financial transactions can reveal sensitive information about an individual data subject, including those related to special categories of personal data. For example, depending on the transaction details, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes. (...) Personal data concerning health may be gathered from analysing medical bills paid by a data subject to a medical professional (for instance a psychiatrist).*"

assessment, certain customer data may even include special categories of personal data related to the customer, such as health-related data[42]. By way of example, according to the IORP II Directive, pension rights may include retirement benefits that are *"in the form of payments on death, disability, or cessation of employment or in the form of support payments or services in case of sickness, indigence or death."*[43] In the same vein, contracts concerning pan-European personal pension products can cover 'biometric risks', i.e., risks linked to death, disability and/or longevity, and can thus involve the collection of special categories of data about the customers[44]. Yet another example concerns mortgage credits. In this regard, the Commission's impact assessment notes that standard mortgage credits for a consumer may contain sensitive personal data[45]. As a result, the combination of mortgage credit with other financial services (such as insurance products and payment accounts) could lead to unfair discrimination[46].

14. The EDPS notes that allowing financial institutions to access highly sensitive personal data through the Proposal's data sharing, access and use provisions not only constitutes an interference with their fundamental rights to privacy and protection of personal data, but could also entail significant risks to the rights and freedoms of individuals , such as risks of financial exclusion via price discrimination, or refusal to supply financial products. This outcome would run counter to one of the stated objectives of the Proposal in Recital (18), namely to ensure that the categories of personal within scope of the Proposal "*allow for innovative products to the benefit of consumers to be developed, while being least intrusive for data subjects in terms of limiting fundamental rights, notably the right to privacy and the protection of personal data*[47]".

15. The EDPS calls on the co-legislators to clarify and to clearly circumscribe the categories of personal data listed in Article 2(1). In this regard, the EDPS alerts that the current definition of 'customer data' is particularly broad. Article 3(3) of the Proposal defines 'customer data' as *"personal and non-personal data that is collected, stored and otherwise processed by a financial institution as part of their normal course of business with customers which covers both data provided by a customer and data generated as a result of customer interaction with the financial institution*." In line with the principle of data minimisation[48], the categories of personal data to be made available under the Proposal should be clearly circumscribed, taking into account the nature of the financial services and products offered by eligible entities listed in Article 2(2) of the Proposal and the risks for individuals whose personal data would be accessed and used.

16. As it is currently drafted, Article 3(3) of the Proposal could be interpreted as including data collected by data holders both at the pre-sales, on-boarding and contractual performance stages of their relationship with customers, including data collected based on legal

[42] SWD(2023) 224 final, p. 107 (stating that "*Pensions data can contain sensitive personal data of consumers*" and that financial institutions may need to rely on the explicit consent of the data subject as per Article 9(2)(a) GDPR to process such personal data.)
[43] Article 6(4) of the IORP II Directive.
[44] Articles 2(29) and 49 of Regulation (EU) 2019/1238 of the European Parliament and of the Council of 20 June 2019 on a pan-European Personal Pension Product (PEPP) (Text with EEA relevance) PE/24/2019/REV/1 OJ L 198, 25.7.2019, p. 1–63.
[45] SWD(2023) 224, p. 101.
[46] SWD(2023) 224, p. 101.
[47] SWD(2023) 224 final, p. 98.
[48] Article 5(1)(c) GDPR.

obligations[49]. However, parts of the Proposal's Impact Assessment suggest[50] that data that the data holder *derives* or *infers*[51] from data provided by a customer as a result of profiling[52] is not intended to be in scope of the Proposal. The EDPS therefore also calls for the explicit exclusion of data created as a result of profiling from the definition of 'customer data', as a way to minimise the risks to the rights and freedoms of individuals[53].

3.2. The role of 'permissions'

17. According to the Proposal, eligible entities acting as data users may only obtain lawful access to customer data held by other eligible entities acting as data holders following the 'permission' of the customer. The EDPS notes that the term 'permission' is not defined under Article 3 of the Proposal, which could generate legal uncertainty for data holders, users and customers alike. Moreover, the use of the term 'permission' in Article 6(3) and Recitals (10) and (22) of the Proposal could be understood as referring to consent as defined under Article 4(11) GDPR or as a contractual legal basis as per Article 6(1)(b) GDPR[54].

18. In this regard, the EDPS positively notes that the Proposal stresses the need for data users to secure a lawful ground under the GDPR to process personal data[55], and that "*[t]he granting of permission by a customer is without prejudice to the obligations of data users under Article 6*" of the GDPR[56]. However, the EDPS is of the opinion that an ambiguity remains in the Proposal between the term 'permission' and the legal basis for processing under the GDPR, namely 'consent' or 'explicit consent' or 'necessity for the performance of a contract'. Thus the EDPS recommends additionally clarifying in Recital (48) 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*".

3.3. Obligations of data holders and data users

19. Articles 5 and 6 of the Proposal outline obligations that would apply to eligible entities acting as data holders or data users in relation to customer data that they are required to share or that they are entitled to access pursuant to the Proposal. The EDPS welcomes that several of these obligations could have a positive effect on the level of protection of the

[49] Such as enhanced customer due diligence requirements under Article 18a of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) PE/72/2017/REV/1 OJ L 156, 19.6.2018, p. 43–74.
[50] In its Impact Assessment, the Commission states that pension risk assessments and other enriched data in relation to personal pensions related to consumers should remain out of scope of the Proposal, as these data may involve financial exclusion risks (SWD(2023) 224 final, p. 108).
[51] On the definition of 'derived and inferred data', see Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, as last revised and adopted on 5 April 2017, p. 10 and 11.
[52] Article 4(4) GDPR and Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, as last revised and adopted on 6 February 2018, page 7.
[53] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, as last revised and adopted on 6 February 2018, page 8.
[54] Having regard to Article 6(1)(b) GDPR, we recall the EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, adopted on 8 October 2019, paragraphs 23 and 30. On the conditions and limits of possible reliance on Article 6(1)(b) GDPR, see also Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others (Conditions générales d'utilisation d'un réseau social) (C-252/21) ECLI:EU:C:2023:537, paragraphs 98 to 100.
[55] Recital (10) of the Proposal.
[56] Recital (48) of the Proposal.

personal data that data holders and data users would process under the Proposal. For example, the requirement for data holders under Articles 5(3)(d) of the Proposal to provide the customer with a permission dashboard to monitor and manage their permissions could increase transparency and control for individuals[57]. Another example is the obligation for data users under Article 6(4)(f) of the Proposal not to share customer data with other entities of the corporate group that they might be a part of.

20. Nonetheless, the EDPS believes that further safeguards and limitations should be included concerning the processing of customer data by data users under Article 6, in order to protect individuals against risks to their fundamental rights to privacy and data protection arising from the increased sharing of sensitive financial data under the scope of the Proposal.

21. The EDPS welcomes the declared objective of the Proposal of preventing risks of financial exclusion of customers having regard to both eligibility for and pricing of financial products and services[58]. He also raises attention to the foreseeable impacts on the fundamental rights to privacy and data protection of the sharing of and access to 'customer data' as currently provided by the Proposal.

22. To ensure the achievement of said objective, the EDPS recommends to insert in the enacting terms of the Proposal a provision that would prohibit the denial of financial services listed in Article 2(2) of the Proposal to customers who do not install and avail themselves of the permission dashboard under Article 8 of the Proposal or otherwise enable data sharing by data holders with data users under the Proposal[59].

23. Additionally, the EDPS recommends including a requirement for data users to clearly outline, in their access requests to customers, the specific types of customer data they seek access to. This would ensure that customers are able to selectively allow access to certain types of customer data under the scope of Article 2(1), but not all. For instance, a customer may wish to share savings account information with a specific data user but not pensions- or investment-related data[60]. This requirement, in addition to the transparency requirements under the GDPR, would help to avoid the risk of broadly-worded and generic requests for access to personal data, regardless of the eligible entities holding it or the sensitivity of specific datasets.

24. The EDPS also recommends amending the wording of Article 6(2) of the Proposal as follows [additional words underlined]: "*A data user shall only request and access customer data under Article 5(1) that is adequate, relevant and necessary for the purposes and under the conditions for which the customer has granted its permission. A data user shall delete customer data when it is no longer necessary for the purposes for which the permission has been granted by a customer.*"

---

[57] See also Article 8 of the Proposal.
[58] Recital (18) of the Proposal.
[59] Expert Group on the European Financial Data Space, Report on Open Finance, 24 October 2022, p. 22: "*from a financial inclusion perspective, it is important that data which consumers are required to provide to access services deemed essential to daily life (e.g., payment accounts, saving accounts, certain insurance and pension products) are focused on data sets which all consumers are fully able to provide.*"
[60] CGAP Technical Note 'Combining Open Finance and Data Protection for Low-Income Consumers', of February 2023, provides another example at p. 22: "*if a fintech offers a payment initiation service, it likely would not be necessary to collect a decade's worth of loan repayment history from the consumer's current bank.*"

25. Furthermore, the EDPS welcomes the exclusion of processing of customer data for advertising purposes in Article 6(4)(e) of the Proposal. At the same time, the exception provided for "*direct marketing in accordance with Union and national law*" would create legal uncertainty, in particular in relation to which types of direct marketing activities would be permissible. In order to increase legal certainty, as well as to reduce the risks of targeted advertising which is not expected by the data subject, the EDPS recommends replacing the reference to Union and national law by specifying that a data user may only contact customers for direct marketing purposes subject to their prior consent or with offers for products or services similar to the ones for which they have accessed customer data and under the conditions provided by Article 13(2) of the ePrivacy Directive.

3.4. Data use perimeter

26. Article 7 of the Proposal refers to a 'data use perimeter' for customer data and explicitly reminds that the processing of personal data referred to in Article 2(1) must be limited to what is necessary in relation to the purposes for which they are processed[61].

27. Access to services, notably services which are necessary for the daily life, such as consumer credit or insurance or pension services, should not be made conditional on excessive data processing. This is particularly important in the financial sector, where asymmetries of information and power might also weaken data subjects' freedom to refuse granting financial institutions disproportionate access to their personal data. Moreover, risks of financial exclusion increase when reliance on in-depth profiling for financial products or services becomes the 'standard option', or where the option not based on such profiling becomes no longer affordable to the consumer.

28. The EDPS notes that Article 7(2) and (3) of the Proposal, as motivated by Recital (19)[62], provides that the EBA and the EIOPA, in close cooperation with the EDPB, will develop guidelines on the processing of customer data pursuant to Article 7(1) in the context of products and services related to the credit score of the consumer and to risk assessment and pricing of a consumer in the case of life, health and sickness insurance products[63].

29. The EDPS underlines the importance of ensuring compliance with the principles of fairness, proportionality and data minimisation[64]. In this regard, the EDPS understands that it may be impossible to exhaustively outline in the Proposal what categories of personal data could reasonably be used for each possible financial product or service. At the same time, it is worth recalling the existence of sector-specific legislation and guidelines applicable to the eligible entities listed in Article 2(2), including legislation that applies to consumer credits

---

[61] Article 5(1)(c) GDPR.
[62] Recital (19) states that such guidelines would *"provide a proportionate framework on how personal data related to a consumer that falls within the scope of this Regulation should be used", and "should be developed in a manner that is aligned to the needs of the consumer and proportionate to the provision of such products and services."* In this respect, the Impact Assessment notes that "*Guidelines have been effective in specifying data requirements to be used in financial products and services, whilst their non-binding nature would provide the market with a flexible framework in which to use and combine data sets in scope an innovative manner and offer such services to customers. A guideline-based approach would also follow existing regulatory practice.*" (SWD(2023) 224 final, p. 49).
[63] As stated in Recital (20) and Article 7(4) of the Proposal.
[64] Article 5(1)(a) and (c) GDPR. See also EDPS Opinion 11/2021 on the Proposal for a Directive on consumer credits, issued on 26 August 2021, paragraph 15: "*data for the creditworthiness assessment should have a clear relationship with the borrower's ability to repay the loan and not have a disproportionate or unexpected impact on the fundamental rights to privacy and to the protection of personal data of the person concerned.*" (emphasis added)

and mortgages[65]. The EDPS recommends amending Article 7 of the Proposal in order to make explicit reference to compliance by data users with the existing EU rules and guidelines regarding the access to and use of personal data for the purpose of the provision of the financial services and products in scope of the Proposal. This would include, for example, the rules applicable to carrying out consumer creditworthiness assessments as laid out in the agreed text of the Consumer Credits Directive[66] ('CDD') and the Mortgage Credit Directive[67], or the duty of investment firms to act in the best interests of the client when carrying out suitability assessments[68].

30. The EDPS welcomes that the Proposal provides for the development of guidelines by the EBA and the EIOPA, in cooperation with the EDPB, on the implementation of the key principle of data minimisation for specific financial products and services. The EDPS notes that the guidelines, despite their non-binding character, would likely gain authoritative value to define the 'perimeter' of data considered necessary to provide specific financial products and services. In light of this, to ensure that these guidelines under Articles 7(2) and (3) of the Proposal are fully aligned with data protection law, the EDPS strongly recommends providing for a formal consultation of the EDPB by the EBA and EIOPA respectively when developing the guidelines. Specifically, the EDPS recommends adding to Article 7(4), after "*in close cooperation with*", the wording "*and subject to a formal consultation of*". In addition to Proposal should clarify that the formal consultation of the EDPB, the issuance of the EDPB's opinion, and the adoption of the guidelines should occur at the earliest possible moment considering the date of applicability of the Proposal, to enable data users to implement the guidelines in a timely manner.

31. The EDPS welcomes that Article 7(2) and (3) of the Proposal makes specific reference to certain products and services that are prone to risks of excessive data collection and/or financial exclusion, such as products and services related to the credit score of the consumer and products and services related to risk assessment and pricing of a consumer in the case of life, health and sickness insurance products. The EDPS recommends extending the scope of Article 7(2) and Article 7(3) of the Proposal to other important financial products and services that would be within the scope of the Proposal, such as mortgage credit agreements[69], provision of payment services, investment products, insurance products other than the ones listed in Article 7(3), and pension products.

32. Finally, the EDPS considers that the guidelines pursuant to Articles 7(2) and (3) of the Proposal should not be strictly limited to the use of data referred to in Article 2(1) of the

---

[65] EBA's Final Report - Guidelines on loan origination and monitoring (EBA/GL/2020/06), of 29 May 2020.
[66] Proposal for a directive of the European Parliament and of the Council on consumer credits (COM(2021)0347 – C9-0244/2021 – 2021/0171(COD)), provisional agreement resulting from interinstitutional negotiations.
[67] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 ('Mortgage Credit Directive') Text with EEA relevance OJ L 60, 28.2.2014, p. 34–85, Articles 18 ('Obligation to assess the creditworthiness of the consumer') and 20 ('Disclosure and verification of consumer information'). Sections 5.1, 5.2 and Annex 2 of the EBA's Final Report - Guidelines on loan origination and monitoring (EBA/GL/2020/06), of 29 May 2020, lay out in detail the types of information that credit institutions should collect from consumers in the context of such creditworthiness assessments.
[68] Article 24 of MiFiD II and Article 54 of Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (Text with EEA relevance) C/2016/2398 OJ L 87, 31.3.2017, p. 1–83.
[69] SWD(2023) 224 final further specifies in p. 101 that "*Clear safeguards, such as personal data use perimeters that specify when mortgage-related data should be used for the different types of use cases, would delineate appropriate use of data*".

Proposal. As acknowledged by recital (18) of the Proposal, data users may in practice choose to combine traditional data sources with 'new' data sources, which can lead to a more sophisticated or comprehensive analysis of certain vulnerable segments of consumers, such as persons with a low income, or may increase the risk of unfair conditions or differential pricing practices like the charging of differential premiums.

33. In this respect, the EDPS underlines that such combinations of personal data are already subject to the requirements of the GDPR, notably in what concerns the principles of lawfulness, fairness, purpose limitation, data minimisation, and adequacy[70]. He also notes that certain data combinations may already be explicitly prohibited under applicable EU or national law, which is the case of processing special categories of data and personal data obtained from social media networks in the context of consumer creditworthiness assessments[71].

34. The EDPS considers that the legislator should provide for the guidelines to be developed by EBA and EIOPA, in consultation with the EDPB, to elaborate, where appropriate, on the limits for combining 'customer data' obtained pursuant to the Proposal with other types of personal data. Such guidance may be particularly relevant in relation to data combinations which may be unlawful and/or present heightened risks for individuals, such as personal data obtained from third party sources (e.g., social media networks or data brokers), data obtained via cookies and other tracking technologies[72], as well as personal data obtained by data users under the Data Act[73], given its potential to reveal highly sensitive personal data concerning customers[74].

3.5. Financial Data Access permission dashboards

35. According to Article 8 of the Proposal, data holders would be required to provide the customer with a financial data access permission dashboard to monitor and manage the permissions they have provided to data users. The dashboard should allow the customer "*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.*[75]" Article 8(3) of the

[70] Article 5(1)(a), (b), (c) and (d) GDPR.
[71] See the final agreed text of the Consumer Credits Directive, Article 19(3a), providing that "*Creditors and credit intermediaries shall not process special categories of data as referred to in Article 9(1) of the Regulation (EU) 2016/679 and personal data processed from social networks that may be contained in databases referred to in paragraph 1.*"
[72] See EDPS Opinion 11/2021 on the Proposal for a Directive on consumer credits, issued on 26 August 2021, paragraph 17.
[73] As the Impact Assessment notes: "*The Data Act proposal introduces an obligation on data holders to make available to the user, or to third parties at the request of the user, Internet of Things (IoT) data generated by the use of products or related services (Article 3, 4 and 5 of the Data Act proposal). While such data are typically outside the scope of the open finance framework, financial institutions may be potential beneficiaries of this access right, e.g. financial institutions that are active in aftermarket data-driven services related to IoT products.*" (SWD(2023) 224 final, p. 110).
[74] See also EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted on 4 May 2022, at paragraph 13 and at paragraphs 54 and 55 ("*Therefore EDPB and the EDPS recommend to include in the proposal clear limitations or restrictions on the use of personal data generated by the use of a product or service by any entity other than the data subject (either as "user", "data holder" or "third party"), in particular where the data at issue is likely to allow precise conclusions to be drawn concerning their private lives or would otherwise entail high risks for the rights and freedoms of the individuals concerned. In particular, the EDPS and EDPB recommend to introduce limitations regarding use of personal data generated by the use of a product or related services for purposes of direct marketing or advertising, employee monitoring, credit scoring or to determine eligibility to health insurance, to calculate or modify insurance premiums.*" (emphasis added)).
[75] Recital (21) of the Proposal.

Proposal states that "*the permission dashboard should be easy to find in its user interface and information displayed should be clear, accurate and easily understandable for the customer.*"

36. The EDPS takes positive note of the requirements in Article 8(2) of the Proposal for data holders to provide customers with a permission dashboard with an overview of each ongoing permission given by him or her to data users, including: the names of data users to whom access has been granted; the customer account, financial product or financial service 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[76]. To ensure that data holders are able to convey all elements of information under Article 8(2) to customers, the EDPS recommends that data users are required under Article 8(4)(b) to also inform data holders about the customer account, financial product or financial service to which access is being sought.

37. Additionally, the EDPS recommends that Article 8(4)(b) requires 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 would rely on to access personal data contained in the customer dataset. This would help prevent data holders from granting access to personal data in the absence of an appropriate GDPR legal basis[77]. As clarified by the EDPB, 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[78].

38. The EDPS also welcomes the reference in Recital (21) to the fact that the permission dashboard "*should empower the customer to manage their permissions in an informed and impartial manner*" and that it "*should not be designed in a way that would encourage or unduly influence the customer to grant or withdraw permissions*". Indeed, in a sensitive area such as personal finance, consumers may be particularly unaware of the consequences of agreeing to share large amounts of their personal data with financial institutions[79]. The EDPS therefore recommends reflecting Recital (21) in the enacting terms of the Proposal, notably in Article 8.

39. The EDPS also notes that Article 8(4) of the Proposal would establish a duty for data holders and data users to cooperate to make information available to the customer via the dashboard in real-time. In this regard, the EDPS welcomes the exchange of this information between data holders and users regarding the permissions given, withdrawn or modified by customers under the Proposal. Nonetheless, the EDPS recommends obliging data users to demonstrate to data holders in an appropriate manner that they have obtained the

---

[76] Article 8(2)(a) of the Proposal.
[77] Recital (48) of the Proposal: "*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 me.*"
[78] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 7 July 2021, p. 45 (paragraph 167 and footnote 76).
[79] The Finance Innovation Lab, 'Open Finance and Vulnerability - A Policy Discussion Paper', July 2021, p. 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.*"

customer's permission to access the customer data held by the data holder. While it is true that the Proposal would oblige data holders to "*request data users to demonstrate that they have obtained the permission of the customer to access the customer data held by the data holder*" [80], there is currently no corresponding obligation under the Proposal for data users to make such demonstration before they obtain the right to access customer data.

40. On a related note, Recital (10) provides that a customer data sharing request "*can be submitted to the data holder by a data user on behalf of the customer*". Even if this part of Recital (10) is not mirrored in the enacting terms of the Proposal, this possibility could open the door to abuse if the data holder cannot verify the representation powers purportedly given to the data user by the customer. Therefore, the EDPS recommends either to delete the relevant part of Recital (10) or, if Recital (10) is kept, amend Article 5 to specify that the data holder shall request proof of the representation powers obtained from the customer. Article 6 should in turn provide for the obligation of the data user to provide proof of its powers of representation.

4. Financial Information Service Providers ('FISPs')

41. The Proposal lists Financial Information Service Providers ('FISPs') as one of the entities that may act as either data holders or data users[81]. FISPs require prior authorisation delivered by a competent authority before becoming eligible to access customer data[82]. If authorised by competent authorities under Article 14 of the Proposal, FISPs would be allowed to leverage the Proposal's customer data access mechanisms 'for the provision of financial information services'[83]. The competent authority would be able to withdraw the authorisation if the FISP would constitute a risk to consumer protection and the security of data[84].

42. The EDPS recommends the inclusion of a possibility under Article 14(7) of the Proposal for competent authorities to withdraw the authorisation in cases where supervisory authorities under the GDPR establish that a FISP has breached its obligations under EU data protection law. This might be particularly important in what concerns FISPs' potential failures to implement appropriate technical and organisational measures to ensure that customers' personal data is adequately protected in the context of the data access and sharing mechanisms created by the Proposal[85]. The withdrawal of an authorisation for the reason recommended by the EDPS could be facilitated by the exchange of information between supervisory authorities under the GDPR and competent authorities under the Proposal, which the EDPS recommends to foster in Section 6 of this Opinion.

---

[80] According to which data holders shall "*request data users to demonstrate that they have obtained the permission of the customer to access the customer data held by the data holder*". This is also in line with the recommendations made by the Expert Group on the European Financial Data Space's Report on Open Finance, in p. 17 and 18: "*the data holder should be able to check the validity of the consent given by the data subject*".
[81] Article 2(2)(o) of the Proposal.
[82] Article 12(1) of the Proposal.
[83] Article 3(7) of the Proposal.
[84] Article 14(7)(d) of the Proposal.
[85] Article 32(1) GDPR.

43. The EDPS notes that the Proposal does not further define what constitutes a 'financial information service'. To ensure that the role of FISPs is clear to data holders and customers alike, the EDPS recommends providing a definition of 'financial information services' in the Proposal[86].

5. Financial Data Sharing Schemes ('FDSS')

44. Article 9 of the Proposal would require data holders and data users to become part of one or more Financial Data Sharing Schemes ('FDSS') within 18 months from the entry into force of the Proposal, and to make customer data available to data users under the Proposal only in accordance with the FDSS's rules and modalities.

45. The EDPS takes positive note that Article 10(g) of the Proposal would require FDSS to establish common standards for customer data and the technical interfaces to allow customers to request data sharing in accordance with Article 5(1) of the Proposal. The EDPS recommends requiring FDSS to also lay down the minimum technical and organisational measures that FDSS members should implement to ensure an appropriate level of security for exchanged personal data.

46. Furthermore, the EDPS observes that Article 11 of the Proposal would empower the Commission to adopt a delegated act to specify the "*modalities under which a data holder shall make available customer data*", in the absence of a FDSS. Such modalities would also include "*common standards for the data and, where appropriate, the technical interfaces to allow customers to request data sharing under Article 5(1)*". In this regard, the EDPS reminds the Commission of its obligation pursuant to Article 42(1) of the EUDPR to consult the EDPS when preparing implementing acts that would affect the protection of individuals' rights and freedoms with regard to the processing of personal data.

47. The EDPS welcomes that Recital (25) of the Proposal mentions that FDSSs must comply with Union rules in the area of competition, consumer protection and data protection and privacy, and that they are encouraged to draw up codes of conduct similar to those prepared by controllers and processors under Article 40 of the GDPR to clarify the obligations of controllers and processors involved in the FDSS. However, for the sake of clarity and consistency, the EDPS recommends replacing the word "similar" after "to draw up codes of conduct" with "*in accordance with Article 40 GDPR*".

6. Competent authorities and cooperation

48. Cooperation between financial regulators and data protection supervisory authorities has been explicitly acknowledged as an objective in EU law. For example, the EBA is currently

[86] For comparison, the EDPS notes that 'account information service' is defined in Article 4(16) of PSD2 as "*an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider*".

mandated to closely cooperate with the EDPB "*to avoid duplication, inconsistencies and legal uncertainty in the sphere of data protection*". The EBA may also invite national data protection supervisory authorities to participate as observers in its committee on consumer protection and financial innovation[87]. As exchange of personal data in the financial sector is likely to increase significantly under the Proposal, the EDPS considers that there is a commensurate need for increased cooperation between competent authorities in finance and data protection authorities, both at national and EU level.

49. The EDPS notes that, pursuant to Article 14(1) of the Proposal, when assessing compliance of an applicant for a FISP authorisation with the requirements under Article 12(1) and before granting an authorisation, competent authorities may consult "other relevant public authorities". The same possibility would exist in relation to "other competent authorities" where competent authorities would be called to assess whether a notified FDSS's governance modalities and characteristics comply with the requirements under Article 10(1) of the Proposal[88]. Given the foreseeable data protection implications of both FISPs' services and FDSS's rules and modalities, the EDPS recommends expressly specifying that supervisory authorities under the GDPR are among the 'other relevant public authorities' or 'other competent authorities' who may be consulted pursuant to those provisions.

50. The EDPS further notes that Articles 18(3) and 26(2) of the Proposal provide for the exchange of information among competent authorities in different Member States in the context of the exercise of their investigatory and sanctioning powers. Article 26(5) provides that competent authorities must also cooperate with supervisory authorities under the GDPR where obligations under the Proposal concern the processing of personal data[89]. In order to ensure a clear legal basis for the exchange of relevant information, the EDPS recommends making explicit reference to the supervisory authorities under the GDPR in Article 18(3) of the Proposal (which currently refers to "authorities from any sector concerned").

7. Publication of administrative decisions

51. Article 25(1) of the Proposal provides that, as a rule, the identity of the natural person subject to a decision from a competent authority imposing an administrative penalty or administrative measure shall not be published. This rule is subject to a derogation under Article 25(2), in cases "*where the publication of the identity or other personal data of natural persons is deemed necessary by the national competent authority to protect the stability of the financial markets or to ensure the effective enforcement of this Regulation*", provided that the

[87] Article 3(6)(c) of Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority), Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) No 600/2014 on markets in financial instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) 2015/847 on information accompanying transfers of funds (Text with EEA relevance) (Text with EEA relevance) PE/75/2019/REV/1 OJ L 334, 27.12.2019, p. 1–145.
[88] Article 10(6) of the Proposal.
[89] See also Recital (36) of the Proposal.

publication is limited to what is strictly necessary to ensure those objectives and properly justified[90].

52. The EDPS considers that the publication of personal data in the context of the publication of the decisions by competent authorities should indeed be the exception, following the case-by-case assessment prescribed in Article 25(2) of the Proposal. The EDPS notes that the publication of personal data related to persons who have been sanctioned for an infringement under the Proposal 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.

53. The EDPS welcomes that Article 25(4) of the Proposal states that "*Personal data contained in the publication shall 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 this Regulation and in any event for no more than 5 years*", as this rule is in accordance with the principle of storage limitation under Article 5(1)(e) of the GDPR.

8. Conclusions

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

(1) to clarify in Recital (48) that processing of personal data in the context of the Proposal Regulation should be carried out in accordance with the GDPR, the EUDPR and the ePrivacy Directive;

(2) to clearly circumscribe the categories of personal data included in Article 2(1) of the Proposal, taking into account the nature of the financial services and products offered by eligible entities listed in Article 2(2) of the Proposal and the risks for individuals whose personal data would be accessed and used by data users;

(3) to explicitly exclude data created as a result of profiling from the definition of 'customer data' in Article 3(3) of the Proposal;

(4) to avoid any ambiguity between the term 'permission' within the meaning of the Proposal and the legal basis for processing under the GDPR, by additionally clarifying in Recital (48) that permission should not be construed as 'consent' or 'explicit consent' or 'necessity for the performance of a contract' as defined in the GDPR;

(5) to insert in the enacting terms of the Proposal a provision that would prohibit the denial of financial services listed in Article 2(2) of the Proposal to customers who do not install and

[90] In addition, Recital (43) of the Proposal states that "*Publication should occur in an anonymised way unless the competent authority deems it necessary to publish decisions containing personal data for the effective enforcement of this Regulation, including in the case of public statements or temporary bans. In such cases the competent authority should justify its decision.*"

avail themselves of the permission dashboard under Article 8 of the Proposal or otherwise enable data sharing by data holders with data users under the Proposal;

(6) to include a requirement in Article 6 of the Proposal for data users to clearly outline in their access requests to customers the specific types of customer data they seek access to;

(7) to amend the wording of Article 6(2) of the Proposal as follows: "A data user shall only request and access customer data under Article 5(1) that is adequate, relevant and necessary for the purposes and under the conditions for which the customer has granted its permission";

(8) to specify that a data user may only contact customers for direct marketing purposes subject to their prior consent or with offers for products or services similar to the ones for which they have accessed customer data and under the conditions provided by Article 13(2) of the ePrivacy Directive;

(9) to include an explicit reference, in Article 7 of the Proposal, to the need to comply with the existing EU sectoral rules and guidelines regarding the access to and use of personal data for the purpose of the provision of the financial services and products in scope of the Proposal;

(10) to provide for a formal consultation of the EDPB by both EBA and EIOPA when developing the proposed data use perimeter guidelines, by adding to Article 7(4), after "in close cooperation with", the wording "and subject to a formal consultation of";

(11) to provide for the adoption of the guidelines under Article 7, subject to the formal consultation of the EDPB, at the earliest possible moment considering the date of applicability of the Proposal;

(12) to extend the scope of the guidelines under Article 7 to other important financial products and services in scope of the Proposal;

(13) to specify that the guidelines under Article 7 should also address, where appropriate, the limits of the combination for combining 'customer data' obtained pursuant to the Proposal with other types of personal data;

(14) to require data users under Article 8(4)(b) to also inform data holders about the customer account, financial product or financial service to which access is being sought;

(15) to require data users under Article 8(4)(b) 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 would rely on to access personal data contained in the customer dataset;

(16) to specify in Article 8 of the Proposal that the permissions dashboard should not be designed in a way that would encourage or unduly influence the customer to grant or withdraw permissions;

(17) to require data users to demonstrate to data holders in an appropriate manner that they have obtained the customer's permission to access the customer data held by the data holder;

(18) if data users may request access to customer data on behalf of a customer, to require data holders to request (and data users to provide) proof of the representation powers obtained from the customer;

(19) *to amend Article 14(7) of the Proposal to clarify that competent authorities may withdraw the authorisation they have granted to a FISP in cases where supervisory authorities under the GDPR establish that a FISP has breached its obligations under EU data protection law;*

(20) *to provide for a definition of 'financial information services' in Article 3 of the Proposal;*

(21) *to require FDSS to lay down the minimum technical and organisational measures that FDSS members should implement to ensure an appropriate level of security for exchanged personal data;*

(22) *to replace the word "similar" after "to draw up codes of conduct" in Recital (25) of the Proposal with "in accordance with Article 40 GDPR";*

(23) *to specify that supervisory authorities under the GDPR are among the 'other relevant public authorities' or 'other competent authorities' to be consulted by competent authorities pursuant to Articles 14(1) and 10(6) of the Proposal; and*

(24) *to make explicit reference to supervisory authorities under the GDPR in Article 18(3) of the Proposal.*

Brussels, 22 August 2023

Wojciech Rafał WIEWIÓROWSKI

p.o. Leonardo CERVERA NAVAS
Secretary-General