

The Consumer Voice in Europe

ACCESS TO CONSUMERS' FINANCIAL DATA

BEUC position paper on the proposed Financial Data Access
Regulation



Contact: Agustin Reyna and Maria Merkou - financialservices@beuc.eu

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND

Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu

EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2023-137 - 31/10/2023

Why it matters to consumers

The sharing and use of data by financial and non-financial institutions could improve consumer conditions in terms of new services and products but it also increases risks of financial exclusion, discrimination and data protection breaches. The proposed Open Finance Regulation enables customers and financial entities to access a wide range of financial data. However, it is important to ensure that sufficient and appropriate safeguards are in place so consumers' personal data is not misused and that consumers can continue having access to affordable and inclusive financial services.

Summary

On 28 June 2023, the European Commission published a proposal for a Regulation to create a framework for financial data access. While third party provider access to customer payment accounts is already a reality due to the Payments Services Directive (PSD2), the proposed Open Finance Regulation widens the possibilities for sharing consumer financial data. This includes new data sources, such as savings accounts, insurance policies, mortgages, investments, and pensions to be accessed by financial and non-financial entities upon the customer's permission. Although Open Finance can boost competition and be an enabler for financial markets, the proposal must be improved regarding consumer protection in order to reduce the risk of exclusion and discrimination. In addition, this new framework should enable the development of simpler financial products for consumers.

The following table summarises the Commission proposal and BEUC's position on the different elements. Where BEUC considers that the approach taken by the Commission is not beneficial to consumers, recommendations to improve the text are provided in the paper itself.

The table assesses the proposals with the following symbols, illustrating whether BEUC:



rejects the proposal



supports in principle but there is room for improvement



supports the Commission proposal



considers that an important point is missing

Commission proposal

BEUC position



Scope: The Regulation excludes from its scope data relating to a person's creditworthiness assessment and data related to health, life and sickness insurance products.



BEUC welcomes that data with a high exclusion risk are not in the scope of the proposal, however, data categories in scope should be further circumscribed, so that these include only financially relevant data. Also, data resulting from profiling activities, should be out of scope, due to their high exclusion risk.



Data Perimeters: Data perimeters are introduced in the form of non-binding guidelines and cover only products and purposes related to a person's



BEUC supports the introduction of data perimeters but urges that they should have a legally binding form. Moreover, the scope of data perimeters is too narrow and should cover

credit rating, and the risk assessment and pricing of life, health & sickness products

more retail banking services and insurance products, due to the high exclusion risk for consumers. The EDPB should be also formally consulted in this process. Furthermore, the legislation should specify that the implementation of data perimeters in line with the Financial Data Access (FiDA) Regulation does not create a presumption of compliance with the GDPR.



Data Users: The proposal introduces the concept of Financial Information Service Providers (FISPs), which will be able to request access to customers' data. They could be active in multiple business lines and bring tailored and innovative solutions to consumers.



BEUC supports that Open Finance can boost competition and deliver for consumers. However, financial data sharing could pose significant risks, if consumers' data is exploited by companies with extensive financial power. Therefore, the role of FISPs should be clearly delineated and entities designated as gatekeepers under the Digital Markets Act should not get access to data under Open Finance.



Alignment with EU data protection & consumer law: The proposal mentions in the Recitals that the GDPR is applicable insofar personal data is being processed.



BEUC welcomes this reference, however, this should be also mirrored in the enacting terms of the proposal. Besides the GDPR, the proposal should be without prejudice to the EU data and consumer protection legislation at large.



Financial Data Sharing Schemes: Data users and data holders, along with consumer organisations will have to form data sharing schemes, whose content and governance will be decided by the members of the scheme themselves.



BEUC welcomes the representation of consumers but urges policymakers to ensure this is balanced and that their presence does not just lend legitimacy to the financial data sharing schemes. Therefore, customer organisations and consumer associations should have full voting rights.



Permission Dashboard: Consumers will be able to manage access to their financial data through a permission dashboard. These will be provided by data holders. Dashboards will inform consumers when their permissions expire.



BEUC supports the mandatory introduction of permission dashboards. To ensure that this tool helps consumers, it is essential that dashboards are easy to find and access, while their design and the information displayed must abide by the data protection and consumer law legislation, such as the GDPR and the Unfair Commercial Practices Directive.



Enforcement: Consumers can seek compensation in case their rights are infringed. Moreover, entities responsible for the infringement are subject to administrative penalties by the Competent Authority, which should also cooperate with the Data Protection Authorities (DPAs).



BEUC welcomes that individuals can seek compensation but urges to include the Open Finance Regulation in the Annex of the Representative Actions Directive. Moreover, the cooperation with the DPAs, and their power to impose penalties insofar as personal data legislation has been infringed should be further clarified. Administrative penalties should be aligned with the stricter ones foreseen under the Payment Services Regulation to ensure the highest level of consumer protection in both frameworks.

1. Introduction

The Commission's proposal for a Regulation to create a framework for Financial Data Access,¹ also known as Open Finance, aims to unleash the full potential of financial data, by enhancing consumers' financial data portability and allowing data sharing amongst financial service providers, in order to boost competition and deliver innovative and tailored financial services and products to consumers. An example would be the development of product comparability and e-switching services, which can be particularly useful for consumers in those fields of financial services where "loyalty penalties" are a common industry practice.

Open Finance builds on the concept of Open Banking introduced under the Payment Services Directive II (PSD II),² which allows third party providers access to consumers' payment accounts (based on the consumer's consent) to offer new services and cheaper payments. The scope of the Open Finance Regulation is, however, considerably broader, covering more categories of personal financial data, establishing data sharing obligations between the holders and users of data, and introducing also a new category of data users known as "Financial Information Service Providers" (FISPs).

Open Finance may be seen as an opportunity to improve European financial systems to benefit consumers, but it also represents the very significant risk of handing out even more market power to the financial industry or already powerful technology companies when dealing with consumers. For example, having data on income, debt and existing assets available to a financial advisor would make financial advice easier to provide and could even increase the quality of services in some cases. On the other hand, there would be very little incentive for the financial industry to share those benefits with consumers instead of booking it as profit. In fact, having access to this information may enable financial salespeople to know exactly how much a specific consumer could be upsold from their needs, making personalised offers which may worsen the already precarious situation of consumers on financial markets. Furthermore, such level of personalisation can be used to deployed unfair practices aiming at increasing consumers' willingness to pay for basic financial services such as insurances.

The direction of dataflow is also an important element to be considered. The availability of income and assets-related data may improve financial advice as outlined above, but the information gathered during the advice process (e.g. sustainability preferences and customer risk profile) may be of interest to other financial institutions. However, it would not be in the benefit of the consumer to share this information as it can be used to identify consumer risk profiles or willingness to pay, therefore, making other financial services, such as insurance, disproportionately priced or inaccessible to consumers.

Therefore, it is important that access to consumers' financial data through the Open Finance framework, delivers for consumers' needs instead of allowing financial service providers to exploit it for a profit. In other words, it would not be in consumers' interests that their data disproportionately empowers salesforces and expands information asymmetry, instead of reducing it. Thus, a certain level of compartmentalisation and restrictions on the access of consumers' data must be maintained. The Open Finance Regulation should be designed to protect consumers' personal data and should explicitly disregard any sales interests: use and sharing of consumer data must be explicitly aimed at increasing consumer benefit and the development of simpler financial products.

¹ Proposal for a Regulation 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, 2023/0205 COD.

² 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.

2. What financial data can be accessed? (Article 2(1))

The scope of the Regulation proposal covers a **wide range of consumer financial data**, notably accounts, payments and transactions of mortgages and loans, savings accounts and investment products, occupational and personal pension products, non-life insurance products and data related to the creditworthiness assessment of firms.³

At the same time, Recitals 9 and 18 of the proposal explicitly **exclude data on life, sickness and health insurance products** as well as **data on the creditworthiness assessment of people**. This was due to the **very high exclusion and discrimination risk** the inclusion of these categories would create for consumers. While article 2(1)(e) makes the same reference, the exclusion of life insurance products is not sufficiently clear. For that purpose, article 2 of the regulation should reflect the text of the Recitals.

The definition of customer data in article 3(3) is broad enough to include data collected from data holders during the pre-sales, onboarding and contractual performance stages. In that sense, this could also include data inferred or derived from data provided by a customer, as a result of profiling. In order to comply with the data minimisation principle of the General Data Protection Regulation (GDPR), the categories of personal data to be made available under the proposal should be clearly delineated, while taking into account the risks their processing poses to individuals and the nature of the financial services to be offered. Thus, data resulting from profiling activities should be explicitly excluded from the scope of customer data in article 3(3).

Regarding investment products, article 2(1)(b) of the proposal expands the scope also to “data collected for the purposes of carrying out a suitability and appropriateness assessment” related to an investment product and advice. Amongst others, when providing investment advice, a firm shall obtain the necessary information regarding an existing or potential client’s knowledge and experience in the investment field, their financial situation and ability to bear losses, and their risk tolerance.⁴ In the Open Finance context, this vague wording can extend to very sensitive personal data. A “person’s experience and knowledge” can include all types of information ranging from those provided from customers themselves, to information not directly related to the purpose a data access permission is granted for, such as their educational background and professional training. Most alarmingly though, one’s risk tolerance and ability to bear losses can be very telling about their creditworthiness assessment, which has been excluded from the scope as a “high-risk” data category.

In a similar fashion, article 2(1)(e) includes “data collected for the purposes of a demands and needs assessment”,⁵ and “data collected for the purposes of an appropriateness and suitability assessment”⁶ in relation to insurance contracts, which can be very telling and allow to draw arbitrary conclusions. This could, for example, be the case regarding theft coverage in motor insurance demands and needs assessment, were a potential policyholder asked to disclose where they live and work, or whether they regularly visit specific neighbourhoods, information that is not related to the provision of financial services.

The ever-increasing deployment of AI systems in the insurance sector amplifies this risk. It is now often the case that insurance companies encourage or even latently oblige policyholders by offering lower premiums, to use telematics as a loss-mitigation insurance tool. This means that policyholders’ location can be tracked in real time, giving detailed

³ *Idem*, article 2.

⁴ 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, article 25(2).

⁵ Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution, article 20.

⁶ *Idem*, article 30.

information about their daily routine and habits. In this context, regularly taken routes to places of prayer, entertainment or even gatherings, could reveal extremely sensitive information about one's religion, sexual orientation or even political beliefs. For that purpose, data falling under article 2(1)(b) and (e) should be narrowly defined and include only financially relevant information related to investment products and non-life insurance products respectively.

BEUC RECOMMENDATIONS:

- Article 2(1)(e) should have an explicit reference excluding data from life insurance products from the scope of the regulation, matching the one made in Recital 9.
- Data collected for the purposes of carrying out an assessment of suitability and appropriateness under article 25 of Directive (EU) 2014/65 and under article 30 of Directive (EU) 2016/97, as well as data collected for the purposes of a demands and needs assessment under article 20 of the latter Directive should be limited to financially relevant data.
- In line with Opinion 38/2023 EDPS, exclude data resulting from profiling activities from the scope of customer data in article 3(3) as they pose a high risk for consumer rights and freedoms.

3. Who can provide and access financial data?

The proposal refers to "data holders", meaning entities that are obliged to make data available to the customer⁷ or to a "data user"⁸ via a permission dashboard.⁹ Data holders listed in Article 2(2)(a)-(n) include traditional financial institutions, such as banks and payment institutions, insurance companies and intermediaries, investment firms and crypto-asset service providers. This does not, however, cover Account Information Service Providers (AISPs),¹⁰ entities introduced under the Payment Services Directive II,¹¹ which aggregate information from a consumer's bank account, to perform a service requested from the consumer, such as money management advice, credit scoring, insurance comparison etc.

Data users on the other hand, i.e. entities that can access customer data pursuant to customer permission, are all the entities listed in article 2(2) of the proposal. This includes all of the aforementioned financial institutions, AISPs and Financial Information Service Providers (FISPs). FISPs, are firms authorised and supervised by competent authorities subject to this regulation but are not defined in the proposal. Article 12 lays down the applicable eligibility criteria necessary to ensure their financial stability, operational resilience and consumer protection, while the aim behind their introduction is to create a level playing field, allowing new entities (such as FinTechs) to enter financial markets, boost competition, and develop new services and data driven products that will support consumers to make informed choices.

However, to provide this kind of services data users can aggregate customer information from different financial sources, such as savings and mortgages accounts, investment, and insurance products, which constitute profiling and would involve automated decision making in the sense of article 22 GDPR. Against this background, it is also important to consider that Big Tech companies may be licensed as AISPs and that the proposal recognises that FISPs can be engaged in other businesses and provide multiple types of

⁷ *Idem*, article 4.

⁸ *Idem*, article 5(1).

⁹ *Idem*, article 8(1).

¹⁰ *Idem*, article 3(5).

¹¹ Consumer Credit Directive, article 33(1).

services and products.¹² In the case of companies whose business model is based on the monetisation of data, there is a clear risk that access to consumers' financial data through the Open Finance Regulation might be abused to generate commercial profit. Based on the rationale of the Data Act, the Regulation should also exclude designated gatekeepers under the Digital Markets Act from the scope of the access right.

BEUC RECOMMENDATIONS:

- Provide a clear and narrow definition for Financial Information Service Providers, that will sufficiently delineate their role and possible data use cases.
- Entities that have been designated as gatekeepers under the Digital Markets Act should be excluded from the scope of access right under this regulation.

4. "Permission" vs GDPR legal bases for processing of personal data

Article 5(1) of the proposal reads that customer data shall be made available from a data holder to a data user, for the purposes a customer has granted permission to. To allow customers to manage their permissions and have effective control over their data, data holders shall provide customers with a permission dashboard,¹³ displaying the permissions granted, including "when personal data are shared based on consent or are necessary for the performance of a contract".¹⁴ In that sense, besides obtaining a permission by a customer, data users need to comply with their obligations under article 6 of the GDPR and obtain a legal basis for processing personal data.¹⁵ This provision could, however, be misinterpreted and understood as any legal basis for processing under the GDPR, which is not the case. Moreover, when personal data processing is based on consent, customers have the right to "withdraw his or her consent at any time, as provided in the Regulation (EU) 2016/679".¹⁶

BEUC considers that the term "permission" in the Open Finance framework should be clarified to avoid any ambiguity related to the legal bases necessary for processing personal data under the GDPR. In this sense, the term "permission" should not be understood as "consent", "explicit consent" or "necessity for the performance of a contract" as per the GDPR, in line with the EDPS Opinion.

Furthermore, where data is being processed on the basis of contract performance, this needs to be interpreted narrowly as recently confirmed by the Court of Justice of the EU¹⁷ meaning that the entities numbered under article 2(2) should take a cautious approach when deciding on the legal basis for the collection and processing of the personal data for the purpose of providing to consumers services facilitated by the FiDA Regulation.

BEUC RECOMMENDATIONS:

- The proposal shall clarify that "permission" within the meaning of the Open Finance proposal is not to be understood as "consent", "explicit consent" and "necessity for the performance of a contract" per the GDPR.
- Recitals 10 and 48 should be amended to reflect the specific GDPR legal bases that can be used to share financial data.
- A recital should indicate that contract performance as a legal basis should be used restrictively, following the interpretation of the CJEU.

¹² Open Finance Regulation Proposal, article 12(4).

¹³ *Idem*, art. 8(1).

¹⁴ *Idem*, Recital 22.

¹⁵ *Idem*, Recital 10 & 48.

¹⁶ *Idem*, Recital 10.

¹⁷ [CJEU ruling in Bundeskartellamt/Meta \(C-252/22\)](#).

4.1. Making sure that consumers know exactly what they are giving their permission for

It is important to ensure that consumers are aware of what they give their permission for. Studies conducted by BEUC members,¹⁸ clearly show that consumers are not giving informed consent when they share their financial data. Most people did not read the terms and conditions and did not understand them even when they had read them. They saw terms and conditions as too long and complicated, full of legal jargon, and “not written with consumers in minds”.

It is essential that consumers know exactly what they are giving their permission for and that their rights under the Open Finance regulation and the GDPR apply. This information should be provided to consumers in clear and understandable language. To allow consumers to effectively stay in control of their data, the regulation must ensure that the deployment of dark patterns¹⁹ and pre-ticked boxes in dashboards are prohibited for the purpose of providing permissions to data sharing.

BEUC RECOMMENDATIONS:

- The use of dark patterns and pre-ticked boxes to obtain consumers’ data sharing permissions should be explicitly prohibited.
- Introduce in Article 6 an obligation for data users to clearly outline to consumers the specific data they seek access to in their access requests.

4.2. Profiling and processing of special categories of personal data

There is little doubt that most of the activities carried out by AISPs and FISPs in the context of Open Finance can constitute profiling under the GDPR and could involve automated decision making in the sense of article 22 GDPR, with the respective data subject rights.

Access to financial data will in many cases reveal sensitive data, that would fall under Article 9 GDPR on special categories of personal data. This can be the case regarding motor or housing insurance products and needs’ assessment, that are in the scope of the Regulation’s proposal, which can reveal sensitive information as mentioned above.

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

BEUC RECOMMENDATIONS:

- The Regulation should explicitly acknowledge that the GDPR rules apply to financial data that falls in the scope of special categories of data and automated decision-making, including profiling and therefore AISPs and FISPs need to develop their respective dashboard accordingly.

¹⁸ BEUC’s Recommendations to the EDPB on the interplay between the GDPR and PSD II, accessible here: https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-021_beuc_recommendations_to_edpb_interplay_gdpr-psd2.pdf.

¹⁹ According to Recital 67 of the Digital Services Act “Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions.”; Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proceedings of the ACM on Human-Computer Interaction, Volume 3, Issue CSCW, Article 81, pp 1–32, define it as: “user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions.”

4.3. Consumers should not be denied access to services for not agreeing to data sharing

While creating opportunities for consumers to receive better and tailored financial services upon sharing their financial data, it is crucial that those who do not wish to share their data under the Open Finance framework, are not excluded from the services listed in article 2(2) of the proposal and are always presented with a fair and reasonable alternative, without having to bear any additional costs. In practice, this should cover both standard products as well as those products requiring additional data to be shared for a risk analysis assessment, by offering consumers the possibility to do so without using the Open Finance system. This could for instance be the case for people with lower digital literacy levels, the denial of services to whom would be unfair and discriminatory.

BEUC RECOMMENDATIONS:

- In line with Opinion 38/2023 of the EDPS, explicitly prohibit the denial of financial services, from providers listed in article 2(2), to consumers who do not avail themselves to the permission dashboard under article 8, or otherwise enable data sharing under the proposal.

5. Obligations of data users & interplay with data protection, privacy and consumer law

BEUC welcomes that the proposal introduces in article 6(4) a minimum set of rules, data users must abide by when accessing personal data pursuant to customer permission, such as the explicit prohibition of processing customer data for purposes other than those explicitly requested by the customer. However, to ensure the maximum level of consumer protection, it is crucial that the interplay of the Open Finance regulation proposal with the EU data protection and consumer protection legislation is further clarified, as the proposal creates unclarity by not making an explicit reference to the existing data and consumer protection frameworks. In particular, the Regulation must be without prejudice to the GDPR, EUDPR the ePrivacy Directive and consumer protection rules, notably the Unfair Commercial Practices Directive, the Unfair Contract Terms Directive and the Consumer Rights Directive (as it has recently incorporated the rules on distance marketing of financial services). This needs to be added in a new article in the proposed Regulation.

In particular to comply with the data minimisation requirement of the GDPR,²⁰ article 6(2) of the proposal should foresee data user access only to data that is “adequate, relevant and necessary” for the purposes intended and the permission granted.

BEUC RECOMMENDATIONS:

- Introduce a provision that the Regulation must be without prejudice to the GDPR, EUDPR the ePrivacy Directive and consumer protection rules, notably the Unfair Commercial Practices Directive, the Unfair Contract Terms Directive and the Consumer Rights Directive.
- In line with Opinion 38/2023 of the EDPS, amend the wording of article 6(2) to read “adequate, relevant and necessary data”.

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, article 5.

5.1. Further Processing

BEUC welcomes that article 6(4)(a) prohibits the processing of customer data for purposes other than those explicitly requested by the customer, however, this provision should also be without prejudice to the GDPR and the purpose limitation and data minimisation principles in particular.²¹ The principle of purpose limitation should be strictly applied in the Open Finance context. This requirement has particular merit especially given the fact that AISPs and FISPs will be undertakings also engaging in other businesses and markets.

5.2. Direct Marketing Activities

While article 6(4)(e) provides that customer data should not be processed for advertising purposes, the proposal leaves an exception for **direct marketing activities**²² in accordance with Union and national law. This creates legal uncertainty in relation to the permissible types of direct marketing activities. This is another example illustrating that the Open Finance proposal needs to make it clear that it applies without prejudice to the EU data protection legal framework. In line with Opinion 38/2023 of the EDPS,²³ and in order to reduce the risks of targeted advertising not expected by the data subject, the provision of article 6(4)(e) should foresee that data users 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.

BEUC RECOMMENDATIONS:

- In article 6(4)(e) introduce a provision foreseeing that data users 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.

6. Data Perimeters

BEUC welcomes the introduction in the Commission's proposal of data perimeters as a way to ensure that the use of consumers' data will not lead to financial exclusion or discriminatory practices. This is the main safeguard for consumers against the misuse of their personal data.

According to article 7(2) the EBA will develop guidelines on how data in the scope of the regulation will be used to assess the credit score of the consumer,²⁴ while EIOPA will develop guidelines relating to financial data use for the risk assessment and pricing in the case of life, health and sickness insurance products, in cooperation with the European Data Protection Board.²⁵

The proposal rightly acknowledges that excluding certain categories of sensitive data from the scope of the Regulation would not suffice to protect individuals' rights and interests and ensure that financial personal data are used in a proper and ethical manner. However, it lacks ambition as to the means used for this purpose and the level of legal certainty this provides, since guidelines are not legally binding. For that purpose, data use perimeters should instead be introduced in the form of Regulatory Technical Standards (RTSs)

²¹ GDPR, article 5(1)(b) and (c).

²² *Idem*, article 6(4)(e).

²³ European Data Protection Supervisor (EDPS), Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, accessible here: https://edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf.

²⁴ Open Finance Regulation Proposal, Recital 19.

²⁵ *Idem*, article 4(4).

developed by the competent ESAs and subject to a formal consultation of the EDPB. In addition, and to ensure the highest level of legal certainty, the Regulation should positively define a minimum set of principles that will be the starting point of the RTSs.

Moreover, in line with Opinion 38/2023 of the EDPS, the legislator should require that the EBA and EIOPA, in consultation with the EDPB, introduce restrictions to combining customer data obtained pursuant to the Open Finance proposal with other types of personal data. This is important since several data combinations may be unlawful and/or present heightened risks for consumers. This could be the case of personal data obtained from third-party sources, such as social media or data brokers, data obtained via tracking technologies such as cookies as well as data obtained by data users under the Data Act.

BEUC RECOMMENDATIONS:

- Data use perimeters should be introduced in the form of Regulatory Technical Standards (RTSs) developed by the competent ESAs and subject to a formal consultation of the EDPB. The regulation should positively define a minimum set of principles that will be the starting point of the RTSs.
- EBA and EIOPA in cooperation with the EDPB should adopt restrictions on the combination of personal data from third-party sources.

6.1. Scope of the services covered by data perimeters: credit scoring

Article 7(2) refers to the use of personal data in the scope of the Open Finance Regulation for products and services related to the credit score of consumers. The scope of this provision is, however, rather narrow and should also cover retail banking services other than an individual's creditworthiness assessment, such as mortgage credit agreements and the provision of payment services. Excluding those services from the scope of this provision would significantly fragment and lower consumer protection in other retail banking services.

Regarding the categories of financial data considered for article 7(2), the Open Finance Regulation should be without prejudice to existing EU sectoral legislation, such as the Consumer Credit Directive²⁶ and the Mortgage Credit Directive.²⁷ While respecting the existing EU legislative framework relating to credit is key to ensure consistency between different pieces of legislation, the Open Finance Regulation will enable extensive financial data sharing, which merits additional protection.

For that purpose, the assessment of an individual's creditworthiness and other credit-related services and products should be based on an exhaustive list of relevant and strictly necessary financial data and relevant evidence, such as evidence of identification, residence, employment, income, and financial assets and liabilities.

BEUC RECOMMENDATIONS:

- Article 7(2) should cover in addition to an individual's creditworthiness assessment also mortgage credit agreements and provision of payment services.
- The Open Finance Regulation should be without prejudice to the existing EU sectoral legislation regarding access to and use of personal data for the provision of financial services and products in scope of the proposal, such as the Consumer and Mortgage Credit Directives.

²⁶ 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, accessible here: [https://www.europarl.europa.eu/RegData/commissions/imco/inag/2023/04-26/IMCO_AG\(2023\)746917_EN.pdf](https://www.europarl.europa.eu/RegData/commissions/imco/inag/2023/04-26/IMCO_AG(2023)746917_EN.pdf).

²⁷ 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.


6.2. Scope of the services covered by data perimeters: Insurance

The risk of exclusion is particularly high regarding insurance products. While risk pooling, has traditionally been the business model of the insurance industry, there is a widely documented shift towards a hyper segmentation and price optimisation model, which is leveraging access to extensive datasets while using sophisticated AI tools.²⁸

Granular risk assessment may on the one hand allow insurance companies to offer coverage to “high-risk” individuals such as diabetics using wearable health devices, or new drivers using telematics tools; however, EIOPA’s Report on AI Governance Principles²⁹ associates this with a higher exclusion risk. This could be the case for both life and non-life insurance products.

For example, DNA data could reveal previously unknown pre-existing medical conditions that could make it difficult for some consumers to access health or life insurance. People living in areas affected by climate change such as those more prone to suffer floods could face difficulties to access flood insurance as a result of increasingly granular risk assessments.

6.2.1. Data & Algorithm Bias



According to the Citizens Advice Annual Report 2022/2023, people of colour still pay on average £250 more for car insurance than white people. As the cost-of-living crisis is ever more challenging for households, data show that people of colour are three times more likely than white people to cancel car insurance as they can no longer afford it.

To ensure fairness to access and affordability of insurance products, we need to ensure sufficient safeguards are installed in the deployment of AI tools in the insurance field. This relates primarily, to an obligation to remove biases from datasets and AI algorithms, as data and algorithmic bias reflect and perpetuate existing inequalities and discrimination in society.³⁰

For that purpose, it is absolutely necessary to comply with EU and

national anti-discriminatory legislation³¹ and also only allow in cases duly justified and absolutely necessary for the policy in question, the processing of protected characteristics and special categories of personal data under article 9 GDPR, such as health data, ethnic origin, religion, political and sexual orientation, as well as proxies that could be correlated with protected characteristics. This could for instance be the case insofar as data from social media were to be used, such as music taste, that could indirectly reveal one’s ethnic origin. As rightly highlighted in EIOPA’s report, “Not all correlations imply causality, and no matter how large the dataset is, it still only remains a snapshot of reality.”³²

²⁸ European Insurance & Occupational Pensions Authority (EIOPA), Artificial Intelligence Governance Principles: Towards ethical and Trustworthy Artificial Intelligence in the European Insurance Sector, page 25, accessible here: <https://www.eiopa.europa.eu/publications/artificial-intelligence-governance-principles-towards-ethical-and-trustworthy-artificial-en>

²⁹ *Idem*, page 25.

³⁰ Citizens Advice, Annual Report 2022/2023, page 24, also accessible here: [https://www.citizensadvice.org.uk/Global/CitizensAdvice/Citizens%20Advice%20consumer%20advice%20ad%20advocacy%20annual%20report%202022_23%20\(2\).pdf](https://www.citizensadvice.org.uk/Global/CitizensAdvice/Citizens%20Advice%20consumer%20advice%20ad%20advocacy%20annual%20report%202022_23%20(2).pdf).

³¹ Such as, Spain’s recent antidiscriminatory legislation: Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, accessible here <https://www.boe.es/buscar/act.php?id=BOE-A-2022-11589>.

³² EIOPA, Artificial Intelligence Governance Principles, page 29.

6.4.2. Privacy or Insurance Coverage?

At the same time, guidance is needed to ensure that the deployment of AI in insurance is steered towards risk prevention, instead of price optimisation. In that sense, the possibility to receive a lower premium or coverage on the condition to share additional data through wearables or telematics should not deprive consumers not willing to share this kind of data from being offered an affordable alternative, as consumers should not have to choose between their privacy and insurance coverage. Insurance companies should provide consumers with incentives to prevent losses and not use such tactics to exclude them from coverage. The urgency of alternatives is ever more obvious in relation to more vulnerable groups, which are already paying higher insurance premiums,³³ such as people with lower digital literacy³⁴ who will not be able to leverage such tools, therefore, amplifying existing barriers.

Harmful price optimisation practices exist across the spectrum of insurance policies and do not solely relate to life, health and sickness products. This has been the case of the so-called “loyalty penalty”. For example, in the UK a recent Financial Conduct Authority (FCA) report into the pricing practices of general insurance contracts, including motor and home insurance, illustrated that longstanding insurance consumers often paid on average more than newer customers. The UK Authority concluded that increasing amounts of customer data accessed by insurers, such as “rating factors” unrelated to risk, lead to price differentiation. These may include data varying from customers’ consumption and media habits to the web browsers they use online. This was also echoed in EIOPA’s recent supervisory statement on differential pricing practices in non-life insurance, illustrating that differential pricing in non-life insurance premiums is based on personal characteristics, such as price elasticity and customer loyalty.³⁵ Given that the Open Finance Regulation will allow access to data from non-life insurance products there is a very high risk of perpetuating and expanding these unfair tactics. Therefore, the non-life insurance products should also be covered in article 7(3), to ensure the highest level of consumer protection across insurance products and policies.

Finally, to ensure maximum transparency and allow consumers to effectively exercise their choice, it is crucial to ensure that insurance companies, in a manner similar to creditors and credit intermediaries,³⁶ are obliged to inform consumers in a clear and comprehensible manner when they are presented with a personalised offer, which is a result of profiling or other types of automated processing of personal data, regardless of the insurance policy in question.

BEUC RECOMMENDATIONS:

- Article 7(3) should cover also non-life insurance products.

³³ Financial Conduct Authority (FCA), General insurance pricing practices market study, accessible here: <https://www.fca.org.uk/publications/market-studies/ms18-1-general-insurance-pricing-practices-market-study>

³⁴ Organisation for Economic Co-operation and Development (OECD), Challenges to consumer policy in the digital age, accessible here: <https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf>.

³⁵ EIOPA, Supervisory statement on differential pricing practices in non-life insurance lines of business, accessible here: https://www.eiopa.europa.eu/system/files/2023-03/EIOPA-BoS-23-076-Supervisory-Statement-on-differential-pricing-practices_0.pdf.

³⁶ Consumer Credit Directive, article 13.

6.5. Right to be forgotten

Data perimeters should aim towards reducing inequalities and lowering the social and economic burden of cancer survivors, in line with the European Parliament's 2020/2267(INI) motion for a resolution,³⁷ which "considers that insurers and banks should not take into account the medical history of people who have been affected by cancer", and "requests that by 2025, at the latest, all Member States should guarantee the right to be forgotten to all European patients 10 years after the end of their treatment, and up to five years after the end of treatment for patients whose diagnosis was made before the age of 18".³⁸ In the EU, cancer survivors are estimated to be over 12 million, including 300,000 children³⁹ a percentage steadily increasing by 3% every year.⁴⁰ Cancer survivors are facing barriers regarding access to financial services, insurance and social protection, even decades after receiving their final treatment, which makes their return to their normal lives much harder than is the case for other people with similar age and socio-demographic characteristics, but no cancer diagnosis.⁴¹

In the area of credit-related insurance, significant progress has been made. According to article 14(4) of the Consumer Credit Directive, personal data concerning consumers' diagnoses of oncological diseases must not be used for the purpose of an insurance policy related to a credit agreement after a maximum of 15 years since there was complete remission. In Belgium, the right to be forgotten applies to cancer survivors who have successfully completed their treatment (without relapse). The Belgian legislator recently adopted a grid, with differentiating time limits per type of cancer and age of diagnosis, where the maximum is eight years and five years for people diagnosed before the age of 21, while periods can drop to just one year for various types of cancer such as melanoma and breast cancer.⁴² Similarly, Portugal has recently passed legislation on the right to be forgotten when taking out mortgage or consumer credit. This covers not only cancer survivors but more generally "people who have overcome or mitigated situations of aggravated health or disability" and starts being effective 10 years after the end of the therapeutic protocol at the latest.⁴³

Taking into account the rapid progress in cancer treatment, the right to be forgotten should also apply to non-credit related insurance products, such as life and health insurance. This has been notably the case in the Netherlands, where the right to be forgotten applies in relation to life and funeral insurance policies. The time periods in this case are 10 years of cancer survivors, and five years for those diagnosed before the age of 21.⁴⁴ These can be even shortened according to a generally accepted and justified medical insight testifying that the recurrence of this type of cancer is slight. Similarly, in Spain, cancer survivors' right to be forgotten is capped at five years.⁴⁵ The same legislation also foresees that discrimination against patients that suffer from HIV or other conditions is illegal,

³⁷ European Parliament 2020/2267(INI), Strengthening Europe in the fight against cancer - towards a comprehensive and coordinated strategy, article 125
accessible here: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0038_EN.html.

³⁸ *Idem*.

³⁹ European Commission, Europe's Cancer Beating Plan, accessible here: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union/cancer-plan-europe_en.

⁴⁰ European Cancer Patient Coalition, accessible here: <https://ecpc.org/policy/the-right-to-be-forgotten/>.

⁴¹ *Idem*.

⁴² Arrêté royal modifiant l'arrêté royal du 26 mai 2019 déterminant une grille de référence relative au droit à l'oubli en certaines assurances de personnes visée à l'article 61/3 de la loi du 4 avril 2014 relative aux assurances, Annexe 1, accessible here: https://www.ejustice.just.fgov.be/mopdf/2023/07/17_1.pdf#Page10.

⁴³ Lei n.º 75/2021, de 18 de novembro, article 3, accessible here: <https://diariodarepublica.pt/dr/detalhe/lei/75-2021-174480833>.

⁴⁴ Besluit van 2 november 2020, houdende regels voor verzekeringskeuringen van ex-kankerpatiënten ten behoeve van het afsluiten van overlijdensrisicoverzekeringen en uitvaartverzekeringen (Besluit verzekeringskeuringen ex-kankerpatiënten), article 1-2, accessible here: <https://zoek.officielebekendmakingen.nl/stb-2020-453.html>.

⁴⁵ [General Law for the Defence of Consumers and Users and other complementary laws](#), article 209.

particularly when taking the form of denial of access to a contract, more deterrent contracting procedures than the ones usually employed by the insurer or the imposition of more onerous conditions.

BEUC RECOMMENDATIONS:

- The right to be forgotten for cancer survivors under the Consumer Credit Directive II art. 14(4), after the end of treatment should be extended to insurance policies not related to credit and cover also chronic diseases.
- Ensure through data perimeters that datasets and algorithms used in relation to insurance products are not biased.
- Insurance companies and institutions offering credit should be obliged to inform consumers in a clear and comprehensible manner when they are presented with a personalised offer that is based on profiling or other types of automated processing of personal data.

7. Permission dashboards

7.1. Dashboard Design

BEUC welcomes article 8 of the proposal introducing permission dashboards, through which consumers will be able to manage their access permissions. As this is going to be a consumer instrument, the proposal must ensure that consumers are made sufficiently aware of these tools and how to use them, while their design and the display of information is indeed steered towards enabling consumers to exercise meaningful control over their financial data.

This has been acknowledged in recital 21 which reads that the dashboard “should not be designed in a way that would encourage or unduly influence the customer to grant or withdraw permissions”. For the sake of clarity, we recommend this to be reflected in article 8 of the proposal and that it is made it clear that interface design should be designed in a fair manner. As consumers will have to provide their permission, regardless of whether data will be shared under “consent” or “necessity to perform a contract”, it is crucial that the minimum requirements to obtain valid consent are always applicable when obtaining permission as well. This will ensure that the permission obtained is meaningful and not just a tick-the-box exercise, allowing consumers to effectively manage which data they want to share with whom and for what purpose. It is also essential that the dashboard design is subject to the GDPR principle of data protection by design and by default and is compliant with consumer law, notably the Unfair Commercial Practices Directive. This means, for example, that dashboards should not allow pre-ticked boxes and explicitly enable consumers to stop sharing their data at any point in time.

Moreover, recital 22 reads “a permission dashboard should warn a customer in a standard way of the risk of possible contractual consequences of the withdrawal of a permission, but the customer should remain responsible for managing such risk...”. Data holders should inform data users in real-time of any withdrawal of a permission”. In order to empower consumers to adjust their permissions according to their wishes and in an impartial manner, the dashboard design shall not steer consumers to provide again their permission and influence their decisions.

7.2. Obligations of data users to data holders

In order to verify access requests, the proposal must require data users to display to data holders with information necessary to validate their request.

In line with the EDPS opinion on the proposal, data users should be also required under article 8(4)(b) to inform data holders about the legal basis under the GDPR they would rely on to access personal customer data. This would also be in line with the controllers' duty to ensure that personal data is not further processed in a manner incompatible with the purposes for which it was originally collected.

This obligation should also extend to the customers' permission that data users have obtained in order to access data held by the data holder. While article 5(3)(c) obliges data holders to request a demonstration of obtained permissions, the corresponding requirement for data users to provide such proof is missing from the proposal.

Finally, recital 10 foresees the ability for data users to submit a request on behalf of a customer, a provision that is not included in the enacting terms of the proposal. To ensure that consumers remain effectively in control of their financial data, it is important that access requests are handled solely by customers themselves. Such a provision would also place a disproportionate burden on data holders to verify the legitimacy of the requests placed from data users on behalf of consumers, turning them into gatekeepers.

BEUC RECOMMENDATIONS:

- The design of permission dashboards should be compliant with the GDPR principles of data protection by design and by default and the use of dark patterns, such as pre-ticked boxes, must be prohibited.
- The principles of recital 21, that permission dashboards shall not unduly influence how consumers manage and grant their permissions should be reflected in an article of the Regulation.
- The design of the dashboard must optimise consumer empowerment and not encourage consumers to provide again expired permissions and does not influence their decisions.
- Oblige data users to demonstrate to data holders the customer permissions obtained, as well as the legal basis under the GDPR based on which they request access to the data in question.
- Delete the provision of recital 10, which allows data users to place a data access request on their behalf.

8. Data sharing for sustainability purposes

Data sharing can play a role for the development of more sustainable financial services. BEUC therefore welcomes the inclusion of sustainability-related information to enable consumers access financial services aligned with their sustainability preferences and financial needs. BEUC considers that the open finance framework can provide opportunities for consumers to access green loans and mortgages, have a meaningful choice of sustainable investment products and access insurance services that can cover climate-related risks based on actual and complete climate data.

To achieve these objectives and considering that climate-related data or data concerning energy efficiency of buildings is not easily accessible to consumers or financial entities, it would be important to establish clear synergies between the proposal and other EU legislation such as the Data Governance Act, the Energy Performance of Buildings Directive and the Energy Efficiency Directive. This also means that we need an assessment of how the private sector could use the information gathered under the Open Finance framework to its advantage, for example, if insurance companies obtain information on flood risks in certain areas, how would that impact home insurance policies? Therefore, it is extremely important that access to financial services is facilitated and not hampered by the new framework.

BEUC RECOMMENDATIONS:

- The Regulation should require the Commission to provide an assessment on how the Open Finance Framework is used to enhance sustainable finance.

9. Governance of Financial Data Sharing Schemes

The way the proposal currently stands, data holders and users should participate in financial data sharing schemes.⁴⁶ These schemes will essentially operate as “open finance ecosystems”, allowing data holders and users to voluntarily join multiple schemes, whose content and governance are decided by the members of the scheme itself “with each side having equal representation in the internal decision-making process”⁴⁷. Except for data holders and users, customer organisations and consumer associations should also be members of the scheme. In the case that no schemes in the sense of article 9 of the proposal are developed, the Commission is empowered to adopt a delegated act, specifying under which terms data holders shall make available customer data.⁴⁸ In line with the EDPS Opinion on the proposal, under article 42(1) of the EUDPR the Commission should be obliged to consult the EDPS when preparing implementing acts affecting the protection of individuals’ personal data.

Article 10(1)(e) foresees that the rules of the scheme can be amended subject to “the agreement of the majority of each community of data holders and data users respectively”. This includes transparency and reporting to members obligations, governance rules and applicable data and technical interface standards. While excluding customer organisations and consumer associations from participating in the amendment process, the proposed governance model leaves room for self-regulation, creating legal uncertainty as to the content and the governance of the schemes.

BEUC RECOMMENDATIONS:

- Give consumer associations and customer organisations the right to participate in amending the rules of a financial data sharing scheme.
- Clarify in article 11 that the Commission should consult the EDPS when preparing the implementing acts provided for in the proposal.

10. Enforcement

10.1. Right to lodge a complaint and bring collective actions

Article 24 of the proposal foresees a right of appeal before the courts for decisions taken by the competent authorities, pursuant to Chapter VI. Pursuant to article 18(1), competent authorities also have investigatory powers necessary to exercise their functions in enforcing the regulation, however, the proposal does not foresee the possibility for individuals to lodge a complaint with the competent authority, disproportionately limiting consumers’ access to redress mechanisms in case the Regulation is infringed.

To guarantee sufficient consumer protection, the Regulation should allow consumers to lodge a complaint with the competent authority individually and collectively, while also annexing the Open Finance Regulation to the Representative Actions Directive,⁴⁹ so that

⁴⁶ Open Finance Regulation Proposal, articles 9 & 10.

⁴⁷ *Idem*, article 10 (1)(a)(i).

⁴⁸ *Idem*, article 11.

⁴⁹ Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC.

qualified entities can represent consumers in case of infringements of the Regulation and for redress claims. Given the complex set of requirements and measures that data holders and users will have to comply with under the Open Finance proposal, there is a substantial power imbalance and information asymmetry, which leaves consumers extremely vulnerable. Only representative actions can effectively bridge this gap and offer consumers the realistic possibility to seek redress and bring cases to court.

BEUC RECOMMENDATIONS:

- Introduce a right allowing consumers individually and collectively to lodge a complaint with the competent authorities, in case of infringement of the Regulation.
- Introduce a new article which amends the Annex of the Representative Actions Directive to include the Open Finance Regulation:
"In the Annex of Directive (EU) 2020/1828 the following point is added: Regulation (EU) XXX of the European Parliament and of the Council a framework for Financial Data Access".

10.2. Enforcement of data protection legislation & cooperation between competent authorities

To ensure the effective enforcement of the EU data protection legal framework in the products covered by the Regulation, the proposal should clarify the remit and powers of competent authorities involved. In that context, article 26(5) should include an explicit reference, stating that Data Protection Authorities should remain competent, particularly in relation to the processing of personal data and to address complaints lodged by the consumers in this regard.

In a similar manner, Data Protection Authorities should be explicitly mentioned in article 10(6) regarding the assessment of compliance of financial data sharing schemes, article 14(1) regarding the authorisation of FISPs and in article 18(3) regarding the cooperation between competent authorities.

Finally, to effectively enforce the EU data protection legal framework, competent authorities under the Open Finance Proposal should be able to withdraw the authorisation granted to FISPs, insofar Data Protection Authorities have established that a FISP breached its obligations under EU data protection law. In line with Opinion 39/2023 of the EDPS, the wording of article 14(7) should be amended to reflect this possibility.

BEUC RECOMMENDATIONS:

- The proposal should include explicit references to the Data Protection Authorities under the GDPR, in articles 10(6), 14(1), 18(3).
- Competent authorities under the proposal should be able to withdraw an authorisation granted to a FISP, consequent to an infringement of data protection legislation established by a Data Protection Authority.
- The proposal should clarify that Data Protection Authorities remain competent to monitor and enforce the EU data protection legal framework.

10.3 Penalties for Infringement

The penalties foreseen in case of consumers' rights infringement under the Open Finance framework must be strong enough to ensure that the interests of individuals are respected and safeguarded.

We regret to see that the penalties provisions in the FiDA proposal are significantly weaker than the penalties provisions foreseen in the Payment Services Regulation (PSR),⁵⁰ which provides the rules for Open Banking. The administrative fines for natural persons set out

⁵⁰ 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.

in the PSR proposal can reach a maximum of €5m,⁵¹ whereas the corresponding provision in the Open Finance proposal does not exceed €250,000.⁵² Similarly, the administrative fines foreseen for legal persons in Open Banking, may reach a maximum of 10% of the total annual turnover of the legal person,⁵³ which is limited to just 2% of the annual turnover for infringements of the Open Finance Regulation.⁵⁴

Considering the implications consumers would be faced with, were their rights set out in the Open Banking and Open Finance frameworks to be infringed, it is crucial for co-legislators to ensure that consumers enjoy an equal level of protection in both Regulations.

BEUC RECOMMENDATIONS:

- Align the penalties provisions of the Open Finance Proposal with those foreseen in the Payment Services Regulation Proposal, to ensure consumers are offered the same level of protection.

11. Review clause

Because of the consumer risks associated to the sharing of data and information under the open finance framework, the report of the Commission under article 31(1) of the proposal should explicitly include an assessment of the impact of the Regulation on financial inclusion and how it has contributed to the development of simpler financial products.

BEUC RECOMMENDATIONS:

- Add in Article 31(1) an assessment by the Commission of the impact of the Regulation on financial inclusion and product simplicity.

[END]

⁵¹ *Idem*, article 97(2)(a)(ii).

⁵² Open Finance Regulation Proposal, article 20(3)(f).

⁵³ Open Finance Regulation Proposal, article 20(3)(f).

⁵⁴ Open Finance Regulation Proposal, article 20(3)(f).



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.

BEUC would like to thank the Adessium Foundation and the Kristian Gerhard Jebsen Foundation for providing funding for the development of this publication.