REPORT ON OPEN FINANCE

Report of the Expert Group on European financial data space

Disclaimer

This report is prepared by the Expert Group on European financial data space set up by the European Commission. The views reflected in this Report are the views of the members of the Expert Group only. They do not constitute the views of the European Commission or its services, nor provide an indication to the policy approach that the European Commission may take in its future work.

Report on open finance

October 2022

CREDITS

All images © European Union, except:

cover: © Murrstock - stock.adobe.com

CONTENTS

List of Expert Group Members

Members of the Expert Group on European financial data space are listed below, in alphabetical order. Open Finance Subgroup members are in bold.

Name	Organisation[1]
Jean Allix	Bureau Européen des Unions de Consommateurs
Davide Corda	Banca Intesa Sanpaolo and Association for Financial Markets in Europe (AFME)
Que-Phuong Dufournet,	Société Générale
Jens-Daniel Florian	Marsh McLennan
Jens Gammelmark	PFA
Catalina Hernandez Serra	Banco Santander, Asociación Española de Banca (AEB)
Sanda Ivankovic	Allianz
Olivier Jérusalmy *	Financial Inclusion Europe
Krzysztof Korus	European Payment Institutions Federation
Zornitsa Manolova	Global Legal Entity Identifier Foundation
Nicolas Marescaux	AEMA Groupe
Anne-Sophie Morvan	The Open Innovation Lab
Ralf Ohlhausen	European Third Party Providers Association
Carlos Ollero *	Equifax
Juliana Pichler	Raiffeisen Bank International
Gilles Saint-Romain	Groupe BPCE
Mladen Sancanin	PGGM
Rudolf Siebel	Bundesverband Investment und Asset Management e.V.
Konrad Sippel	Solactive AG
Maria Staszkiewicz	European Digital Finance Association
Mirek Sopek	MakoLab SA
Emanuel van Praag	Erasmus School of Law Erasmus University Rotterdam
Polyxeni Vasilakopoulou	University of Agder
Michael Zimonyi	European Financial Reporting Advisory Group

*Asterisk denotes members who contributed to the open finance report but left the Expert Group before the finalisation of the report following a change in professional situations.

[1] Company affiliation has been added for information purposes only. The Expert Group consists of Type A (Individual expert appointed in his/her personal capacity) and Type B members (Individual expert appointed as representative of a common interest). For more information, see European Financial Data Space. Register of Commission expert groups and other similar entities (europa.eu)

PART A: Introduction

1. Mandate of the expert group and structure of the report

This report is a key outcome of the Expert Group on the European financial data space. The Expert Group was set up by the Commission in June 2021 with a mandate to provide advice and expertise to DG Financial Stability, Financial Services and Capital Markets Union (FISMA) in relation to the preparation of legislative proposals and policy initiatives in the field of data sharing in the financial sector, to further the establishment of a common financial data space in the EU, and to assess the need for any interaction with other data spaces and data-sharing beyond the financial sector.[2] The Expert Group was asked in particular to examine matters related to open finance. For these purposes, a dedicated subgroup on open finance was set up with the mandate to establish the modalities for data sharing and reuse based on a specific number of illustrative use cases and to describe the key components of an open finance ecosystem in the EU.[3] This report also gathered some contributions from members outside the subgroup on open finance.

Based on the discussion of the Expert Group, this report is structured as follows: Part B describes the key elements of an open finance ecosystem as seen by the expert group and sets out some findings in that respect. To inform this analysis and illustrate the challenges and opportunities of open finance, the group has carried out an assessment of several specific use cases which is detailed in Part C of this report. The selection of these use cases was carried out to ensure a sample of use cases illustrating the diversity of such cases and should in no way seen as an endorsement by the group members of the business case or merits of individual use cases, as compared to other use cases.

The Expert Group will continue to work on certain policy areas identified in this report, with a view to further developing and discussing more detailed technical issues related to the implementation of this report and open finance in general.

2. Objectives of open finance

Open finance refers to the sharing, access and reuse of personal and non-personal data for the purposes of providing a wide range of financial services. The objective of open finance is to promote innovative financial products and services to the direct benefit of consumers and firms. A key condition for open finance is strong consumer trust and confidence. Further steps towards enhanced data openness across and within sectors will increase opportunities for data-driven innovation and support the creation of a broader single market for data.

[2] Expert group on the European financial data space, Register of Commission expert groups and other similar entities (europa.eu)

[3] Subgroup on open finance, Register of Commission expert groups and other similar entities (europa.eu)

A **core focus** of open finance should be to improve financial products and services and to create opportunities for consumer and firms to obtain better targeted advice and personalised services. This includes:

- Customer[4] experience – a broader choice for customers and easier identification of the best options through access to a more tailored and personalised range of services and products; as well as an easier ability to access and use those products;
- Financial inclusion - improving access and use of financial services for all segments of consumers and firms, including SMEs and access for financially excluded people;
- Customer control - giving customers meaningful control over how their data is shared and reused, in line with data protection rules; providing consumers and firms with greater transparency about how their data is used and accessed;
- Innovation - facilitating the interoperability of data in open finance; as well as supporting the development of Artificial Intelligence / Machine Learning models to build services and products for consumers and firms including more accurate prudential risk management.
- Horizontal approach – embed the open finance approach of customer-centric services in a general cross-sectoral framework.

Open finance must therefore envisage use cases with high potential and benefit for consumers and firms, as well as clear industry incentive (see Part C: Use Cases)[5]. It should also complement what exists and works well in the market today: it should add value to existing markets and systems through the sharing and reuse of data and provide a basis for innovation. Open finance is best achieved in a controlled manner, where there is *opening of data with a purpose*.

To **achieve its objective**, open finance can only work based on strong customer trust and confidence in the sharing and reuse of data – including personal data. In this respect, a condition for open finance is to protect consumers and firms by addressing risks related to data access and use and reducing use issues, e.g.:

- Risks related to consumers and firms – risks related to unfair use of data, mis-selling, fraud or a lack of expected protection from a service or product due to incorrect advice or incomplete information;
- Exclusion risks - risks related to exclusion, discrimination or overcharging because of a customer's risk profile;
- Operational risks – risks related to complex data control & management because of increasing data sharing and reuse; cybersecurity risks that could affect the customer, the data holder, or the underlying open finance infrastructure; Including with regards to the protection of personal and non-personal data, trade secrets, intellectual property theft or industrial espionage.

[4] A customer in this report refers to consumers and firms, including SMEs.

[5] As explained in Part C of this report, the selection of the use cases in this report was carried out to ensure a sample illustrating the diversity of such cases and therefore should in no way seen as an endorsement by the entire group members or merits of individual use cases, as compared to other use cases.

Moreover, open finance must be based on a level playing field, including fair competition as well as equal and fair access to data.

When discussing open finance, this report uses the terms of "data sharing", or of "data access and "reuse". While certain members stress that data openness in open finance should be framed either in terms of "data sharing", or of "data access and reuse"[6], this report refers to both *data sharing and data access/reuse* as a collective term to ensure consensus. The use of these terms does not prejudge the different models of open finance, as set out in the subsection below.

Models for open finance

How an integrated market for open finance operates in practice depends on the data sharing model used. An integrated market could be organised based on different models for data sharing, access and reuse.

Open finance could be determined based on either a voluntary framework based on contractual schemes, or a mandatory framework. Both frameworks exist in the market today in certain sectors: there are market-driven examples of financial firms sharing data voluntarily[7], while certain relevant regulatory requirements such as access to payments account data under the revised Payment Services Directive (PSD2) as well as the right to data portability under the General Data Protection Regulation (GDPR) create obligations to make specific data available[8]. However, this Report does not commend a particular model.

Second, an open finance model is dependent on the data flow between actors in the data chain. This is discussed at length in this report (see Section 1: Definitions; Section 5: Data protection and consumer protection; Section 9: Key actors and Success Criteria). Data sharing models depend on several conditions:

1. Who initiates the data sharing (e.g., the data user, the data holder or the data subject). Under this condition, open finance models can differ depending on the actors involved in data sharing: data sharing between financial institutions; data sharing from financial institutions to non-financial institutions (where the data holder is a financial institution); and data sharing from non-financial institutions to financial institutions (where the data holder is a nonfinancial institution). Irrespective of the data sharing scenario, personal data must be shared in a manner fully consistent with the rights and obligations under the GDPR.

[6] In general terms, 'data access and reuse' means the processing of data by a data user for a specific purpose other than that for which the data was collected, based on a GDPR lawful ground of processing. Some members argue that data reuse is the most appropriate term to describe data processing in open finance.
[7] Market-driven initiatives include, for example, the SEPA API Access Scheme of the European Retail Payments Board. See: Development of the EPC SEPA credit transfer and direct debit schemes | European Payments Council
[8] GDPR Article 20. See : EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

2. What legal basis is used for the processing of data (e.g., processing based on consent, contract or legitimate interest[9])
3. What are the conditions in which the data shared (e.g., via a contract, or an obligation described above).
4. How the data is shared (e.g., directly or indirectly between the data holder and the data user). Here as well, an open finance model needs to consider national differences (e.g., in tax, welfare or pension systems) that must be respected.

3. Definitions used within the Report

3.1. Principles facilitating chosen definitions

This section defines certain open finance concepts used in this Report, including main data actors and other broader concepts of relevance.

The definitions used for the purpose of the Report are based on the roles, which each of the open finance parties have been assigned in the data chain according to their function. Where appropriate, they reflect use in EU legislation, such as in the Data Governance Act. Open finance data definitions were also tailored to highlight specific rights attaching to data (e.g., people's rights to data protection and private life, rights to protect intellectual property, etc.).

The provided definitions come as far as possible from existing legislative texts. However, they are not meant to have a legal character and are confined to their use within the Report. The definitions do not always reflect the way different members of the group in their own capacities use different definitions. In particular, some of the members expressed a view that use of the data 'ownership' concept would be more appropriate to define open finance actors/data. Nonetheless, the discussions identified conceptual issues related to the idea of data ownership and noted that data ownership is not a term used or defined in EU law. Accordingly, definitions were chosen due to their ability to facilitate discussion on open finance and provide operational terms for concepts used in this Report.

3.2. Definitions of the key data actors

The following definitions of the data actors are proposed:

Data Subject – an identified or identifiable natural person to whom the data relates, as established within the GDPR (Article 4.1 GDPR).

In relation to non-personal data, Data Subject would include all legal entities whose data is held (e.g. SMEs in SME use case). This is without prejudice to the scope of the GDPR.

Data Rights Owner – a legal or natural person who, in accordance with applicable law, has produced the relevant data and/or has intellectual property rights over such data (including

[9] GDPR Article 6. See : EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

where the data is considered as a trade secret of such person). There may be several Data Property Rights Owners in case of joint intellectual property rights.

Data Holder – a legal person, public body, international organisation or a natural person who is not a Data Subject with respect to the specific data in question, which, in accordance with applicable law, has the ability to grant access to or to share certain personal or non-personal data (Article 2.8 Data Governance Act)

Data User – a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non-commercial purposes;

Data Intermediary – a provider of data intermediation services as established within the Data Governance Act (Article 2.11 Data Governance Act)

Data Broker – a legal or natural person which provides adjacent value-added services based on the Data Subject's data and makes them available to Data Users, which are often the Data Subjects themselves.

Third Party – parties other than the Data Subject, Data Rights Owner or Data Holder who facilitates the provision, movement and/or use of data.[10]

3.3. Other definitions used within the report

Intellectual property rights – intellectual property generally refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.[11] For the purposes of the Report, the most relevant intellectual property rights include patents, trademarks, designs, copyright (e.g., copyright protection of databases provided within the Database Directive), sui generis database rights and trade secrets. Intellectual property rights allow companies to safeguard and, where relevant, valorise their rights within intangible assets such as data.

Machine-Readable Format – a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure (Article 2.13 Open Data Directive).

[10] The definition of 'Third Party' used in this report is without prejudice to Article 4(10) GDPR.
[11] https://euipo.europa.eu/ohimportal/en/web/observatory/understanding-ip

PART B: Key elements of an open finance ecosystem

Part B describes the key elements of an open finance ecosystem as seen by the expert group and sets out some findings and recommendations on each. The findings in Part B reflect the collective discussions which took part in the expert group, and draw from the use cases in Part C. The following elements are covered:

- Data accessibility and data availability
- Data protection and consumer protection issues
- Data standardisation
- Liability issues
- Level playing field and cost of data access
- Key actors and success criteria for open finance

4. Data accessibility and availability

An efficient open finance framework should be based on appropriate data availability and access, which is fair, transparent and proportionate. Therefore, the need for a list of customer data fields, mandatory available data and data access specifics (including question of costs) should be assessed.

Summary of views on data accessibility and availability:

1. While views diverge, some members recommend that publishing lists of customer data fields would also be one way of ensuring transparent processing, in line with the GDPR. These lists could provide a general overview of what type of data is stored by the data holders and could apply irrespective of the data model (voluntary or mandatory). Other members however disagree with this recommendation, and outline that the GDPR already ensures the transparent processing of categories of personal data and they highlight that the concept of publishing lists of customer data fields may be technically challenging to implement.

4.1. Organising access to data

Technical access to both personal and non-personal data could be organized similarly to facilitate business operations, e.g., as regards the development and maintenance of the relevant systems and procedures. However, such approach would bring different regulatory frameworks together. Therefore, differences in access to personal and non-personal data depending on the intended use case should be considered (e.g., different lawful grounds of access as well as other applicable national and supranational laws).

There was also a consensus that an open data economy should be multilateral and cross-sectoral. Taking considerations of the whole data value chain as well as cross-sectorial (including non-financial) data will also allow to improve performance of the financial sector. Sectorial differences are particularly relevant to address varying risks within the sectors.

For open finance to grow, it is also important to maintain incentives for data holders to continue investing in high-quality data collection and processing. To address this issue, some participants suggested to consider principles introduced within the proposed Data Act – e.g. compensation for the costs of granting access to data and the prevention of any negative impact on data holder's business opportunities.

While views among members diverge, specific tools that may be used to promote transparency and easier access include establishment of data perimeter and the publication of lists of customer data fields. Lists of customer data fields are to be understood as the publication of general data fields stored by data holders (see Section 4.2). Data perimeters are to be understood as a framework defining the categories of personal data normally used for specific open finance products or services (see Section 5).

The Data Act proposal addresses some of these requests and recommendations above. The proposed Data Act proposes new horizontal rules to clarify who can use and access data generated in the EU across all economic sectors, including the financial sector. Moreover, the Data Act introduces a new access right that allows users of connected devices to gain access to data generated by them (industrial and IoT data); and allows users to share such data with third parties to provider data-driven innovate services. In addition, the Data Act proposal seeks to rebalance negotiation power for SMEs by preventing abuse of contractual imbalances in data sharing contracts. The Commission will also develop model contractual terms to help such companies to draft and negotiate fair data-sharing contracts.

4.2. Publishing lists of customer data fields

While views among members diverge, some members argue that there is merit in publishing lists of customer data fields stored by financial service providers to raise awareness among both customers and third-party service providers as to what data is collected and processed by financial service providers (as, for example, a consumer many wish to know which personal data sets are processed by a wallet provider each time a payment is transacted). Members supporting publishing lists of customer data fields state that they would not contain any specific data sets but would provide general information on what data fields and type of data is stored by the data holders. This could ensure transparency for third-party access to customer data on a commercial basis. In some instances the existing transparency obligations under the GDPR[12] could be used as a basis for the publication of customer data fields, while other cases would go beyond an existing GDPR legislation. For instance, the GDPR establishes an obligation to provide Data Subjects with information about categories of his/ her personal data being

[12] GDPR Articles 13, 14 and 15 obliges firms to provide the categories of personal data that they hold on customers.

processed by the relevant Data Holder. Publishing lists of customer data fields, on the other hand, is more specific than provision of overall data categories and is also not restricted to being provided solely to the Data Subject himself/herself. The lists of customer data fields would also address situations where customers/Data Subjects are SMEs or firms more generally, which are not covered under the GDPR. The Expert Group agrees that further work may be necessary on the concept of publishing lists of customer data fields, for example to assess its potential impacts and to address situations where customers are SMEs or firms.

Other members however disagree with this recommendation and outline that the GDPR already ensures transparent processing of personal data. Therefore, these members argue that the concept of publishing lists of customer data fields, additionally to already implemented GDPR requirements, would, if at all, likely generate little added value compared to the costs and risks that may arise. Indeed, the publication of those lists would not help a lot the potentials data users. First, the sources of any data are usually easy to determine. Secondly during the development of an innovative service, the necessary data is not chosen from a list but determined following iterative exchanges between the data holder and the data user on the purpose of the sharing. There are often cultural differences to consider beyond the choice of the data themselves, when the usages envisaged by the data user are new.

While the GDPR request transparency for the data subject on the categories of personal data concerned by a processing (Article 15 GDPR), a one-to-one approach with a consumer protection goal, the publication of list of customer data fields, a one-to-many approach, has the objective to raise awareness among TPPs on the data available from each data holder which falls within the scope of competition.

Assessing the merit in publishing lists of customer data fields requests a proof of a real market need and a careful assessment of its potential impacts. It will be important to precisely determine the scope of these list (vs the data categories / type of personal data under GDPR Article 15), who will bear the implementation cost, and the potential privacy issues (and bank secrecy and trade secret) and on the level of legislation (horizontal vs sectorial).

Moreover, these lists could place additional financial burden on the individual Data Holders. Some members therefore expressed opposition to any obligations on a sectoral level, going beyond the GDPR scope, since they argue that this could impose excessive burden and impinge on the level playing field across sectors. Moreover, some members argue that these lists should not contain mandatory data fields that are not relevant to the individual service provider's specific service offerings. Specifically: the service provider should not be obliged to collect and disclose of data that it does not need for the specific range of services it offers. Additionally, some members are concerned that disclosing customer data fields may be determinantal for innovation. Firms must be free to create company-specific data fields that can serve as the factual base to provide additional services for the service provider.

If implemented, such lists could be published gradually to promote specific use cases with benefits for customers and extended to other use cases over time. There were some suggestions to publish such lists of data fields on a voluntary basis, especially if those are

related to inferred data covered by intellectual property rights, possible trade secrets or other proprietary data that data providers have generated and analysed/enriched themselves.

Standardised data identification and aggregation methodology could allow for Data Subjects to clearly identify with whom the data is shared and for API providers to track sharing of data.

It was suggested that existing market tools may be used to advance data/ entity identification by users and provide an ability to further connect to other information sources (e.g., use of global data standards for identification, links with global registers that follow common data formats, etc.).

For the sake of clarity, it is worth noting that transparency and processing of personal data is addressed under the GDPR. Principles of data minimisation – limiting processing of data to what is necessary – must also be adhered to.

5. Data protection, and consumer protection issues

Summary of views on data protection

1. Data sharing should be limited to the specific purpose of processing, as agreed with the data subject. Processing should be based on the nature, scope, context and purposes of the data subject's agreement.
2. Data subjects must remain in control of the data they wish to share and be able to keep track of who they have granted access to. Transparency must be maintained in the data chain. Data subjects should be provided with clear information on the type of personal data processed, the reason and the type of use. The data subject should be informed of the different personal data sources used to deliver a product.
3. Some members recommend that the introduction of data perimeters for use cases – clearly delineating the categories of personal data which is expected to be used for a specific financial products or services – could be an approach to strengthen control over data use and enhance transparency as well as explainability of decision processes. Other members however disagree with this recommendation and argue that the concept of data perimeters would not serve the purpose of offering innovative services to customers and limit the opportunity for promoting financial inclusion. Moreover, perimeters would be technically challenging to implement to the extent that it negatively impacts transparency, competitiveness and the control the data subject has over their personal data.

5.1. Lawful grounds for processing personal data

The sharing of and access to personal data in an open finance context must take place in a safe and ethical environment, in full respect of all EU data protection requirements. The processing of personal data is regulated by the General Data Protection Regulation (GDPR). When personal data is processed as part of activities related to open finance, all controller(s) involved must ensure that processing is based on at least one of the six lawful grounds under Article 6 GDPR.

All GDPR-defined lawful grounds are allowed for the processing of finance data that contains personal data. All processing must abide to the following obligations:

- strict respect of GDPR Article 5 principles on the processing of personal data, including the principle of necessity and the principle of minimisation.
- ensuring that transparency is maintained in the data chain (e.g., the data subject should be informed of the different personal data sources used to deliver a product) in line with the responsibilities of individual controllers and the rights of data subjects.

While data subjects should remain in control of the data they wish to share, it is important to acknowledge that processing of personal data may be processed on lawful grounds other than consent. To give one

example, processing of personal data may be necessary for compliance with a legal obligation to which a financial institutor as a controller is subject to, as per GDPR Article 6(1)(c). This could include, for example, customer due diligence checks which financial institutions as obliged entities **must** carry out. In this respect, the rights of the data subjects to withdraw data are reduced, since access to these data is a legal necessity.

5.2. Processing based on the performance of a contract

Financial services are often contract-based. In most instances, therefore, processing based on a performance of a contract may be the most appropriate lawful ground for processing as personal data is processed to provide a *specific service* for the data subject (consumer). The performance of a contract may also be preferred in open finance for a number of other reasons:

- Processing based on a contract may be more stable for those involved in the data chain compared to processing based on consent, given that 'consent' for personal data processing can be withdrawn at any point by data subjects with the data controllers needing to stop the data processing.
- Processing based on consent is often not achievable as a lawful ground for processing, as consent must be *freely given* (see more on the requirements for consent in Section 6.3 below). This criterion is challenging to achieve for market participants as financial services are contract-based (if the data is not provided, a contract cannot be performed). Naturally, controllers must evaluate to what extent personal data are in fact needed to perform the contract.

5.3. Processing based on consent

Consent under Article 4 GDPR

"Consent' as defined in the GDPR means any *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*" (Article 4(11) GDPR). According to the EDPB[13], all four requirements (freely given, specific, informed, unambiguous) are required for consent to be meaningful. Market participants mention that achieving this in practice, however, can be challenging, in particular the 'informed' condition (combing the ability of a data holder to explain and the data subject to understand). In addition, where processing is based on consent, a data subject has the right to '*withdraw his or her consent at any time*', as per Article 7 GDPR.

As outlined in Section 5.2 above, it is also important to highlight that data to which access is requested is necessary for the provision of services and, therefore, financial service providers have a lawful ground to have access to these necessary data. Therefore, the consumer would be able to provide the necessary data and receive services. This condition means that consumer who would like to access a financial product or service should have the possibility to provide the necessary data for the performance of a contract. However, the data subject

[13] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 (May 2020)

should still have an option to limit access to the provided necessary data by parties that are not a service provider. Additionally, access to any additional data by the service provider would require a more specific and explicit consent to access/process the particular data.

'Explicit' consent under Article 9, Article 22 and Article 49 GDPR

Certain open finance activities that process personal data may need to rely on explicit consent where serious data protection risk may emerge and, hence, where a high level of individual control over personal data is deemed appropriate. As outlined above, market participants note that the granularity in consent makes it challenging to achieve in practice. Under the GDPR, explicit consent is can be relevant when:

- Processing of special categories of data (Article 9 GDPR): according to the EDPB, financial transaction data[14] could be considered sensitive categories of data as it could disclose a data subject's political, religious, sexual and/or health status.[15] When processing certain types of financial data that contains personal data, GDPR Article 9 may apply. This would either require explicit consent by the data subject, which in financial services context is challenging given that the GDPR criteria for 'freely given' is difficult to obtain and would require another condition as set out in Article 9(2) to be met.
- Automated individual decision-making, including profiling (Article 22 GDPR): a data subject's explicit consent is required in these circumstances[16], unless automated processing is necessary for entering into, or performance of, a contract between the data subject and a data controller, or is authorised by Union or member states law to which the controller is subject.
- Data transfers to third countries: third country transfers or transfers to international organisations in the absence of adequate safeguards in Article 49 could require a data subject's explicit consent[17].

PSD2 consent:

The revised Payment Services Directive (PSD2) provides third-party service providers' access rights to payment accounts upon customer request. PSD2 requires the payment service provider to collect a user's 'explicit consent' as defined in Article 67(2) PSD2 for a PISP, and

[14] Transaction data includes information about the customer's past and present transactions, including the amount spent, time of the transaction, payment methods used, location of the transaction and other aspects associated with the transaction.

[15] According to the EDPB, "financial transactions can reveal sensitive information about an individual data subject, including those related to special categories of personal data". See EDPB, Guidelines 06/2020 on the interplay of the Second Payment, Services Directive and the GDPR Version 2.0 (December 2020). To note however that the EDPB opinion has been disputed by joint industry letters, European Payment Service Providers' comments on the EDPB Guidelines 06/2020 on the interplay (ebf.eu) (October 2020)

[16] GDPR Article 22(1) states that explicit consent is required when automated decision-making produces 'legal effects' on data subjects or 'similar significantly affects' the data subject.

[17] To note that GDPR Article 49 provides seven derogations for transfer, of which explicit consent is one.

Article 67(2)(b) for an AISP. According to the EDPB, PSD2 explicit consent is of a different nature to the GDPR's explicit consent.[18]

Data Governance Act:

The Data Governance Act (DGA) defines "data altruism" as 'the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services' (Article 2(10) DGA). It remains to be considered to what extent data altruism consent could be used for open finance. Indeed, consumer protection representatives have expressed their doubts about this and argue that in all cases the data should be anonymised.

5.4. Examples & elements of useful consent management tools

Open finance should provide the necessary tools to enable consumers as data subjects to control the use of their personal data and keep track of whom they have granted access to. In this respect, the operationalisation of consent management tools could be important to strengthen the sharing of personal data based one of the GDPR lawful grounds for processing. If designed effectively, these tools could also combat issues specific to the lawful ground for processing based on consent, notably 'consent fatigue'.[19] Ideally, these tools should grant a holistic consumer view considering a cross-sectoral perspective to ensure consumer consent understanding and control, given that financial sector is only one of the many different players involved in data sharing. Once consent is given, the consumer could have the following rights:

- keep control over what type of data is being shared (for instance, a consumer may wish to share their savings account information, but refuse to share payment account information). For example, some members argue that a significant amount of data available on payment accounts are not necessary for a creditworthiness assessment.[20] This could include: the granularity in the expenditures (shops, internet…), data on the type of payment tool used and on the time of purchase – and, on top of this, the expenditures which refer to sensitive personal data (e.g. religious affiliation, trade-union status).
- track and control who they have granted consent to, including for revoking consent. Consumers should have a right to instruct financial services providers (the data holder) not to share their data with third parties., and the data holder should be able to check

[18] Indeed, the EDPB argues that 'explicit consent under Article 94 (2) of the PSD2 is an additional requirement of a contractual nature'. From a GDPR point of view, PSD2 customer request does not rely on "consent" legal basis for processing but the "performance of a contract". See EDPB, Guidelines 06/2020 on the interplay of the Second Payment, Services Directive and the GDPR Version 2.0 (December 2020)

[19] When encountered too many times, the actual warning effect of consent is diminishing. This results in 'click' or 'consent' fatigue. See EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 | European Data Protection Board (europa.eu) (May 2020)

[20] Finance-Watch, October 2020, Responsible lending and privacy protection: A consumer perspective, Discussion paper, See: https://www.finance-watch.org/wp-content/uploads/2020/10/FW-paper_Responsible-lending-and-privacy-protection_Oct2020.pdf, pp 10-13

the validity of the consent given by the data subject[21] The consumer should be able to establish a 'white' list (e.g. intermediaries who can have access) or a 'red' list (intermediaries which are not accepted) for data use. This could be useful for certain cases, such as for direct debits. Some members argue that only red lists would be feasible, because permission must be given directly to the data broker. Other members however argue that these lists would be technically challenging to implement and it should be considered in a cost benefit assessment.

- keep track of the insights into what types of actors have access to this data, and how this data has been used.

Operationally, consumer management tools could include:

- Privacy dashboards: Dashboards are being developed by the market, such as by Groupe BPCE's *Privacy Centre*. Developing dashboards however comes with challenges that may need to be looked into. Some members have argued that dashboards must be 'read-only', to avoid a situation where one party interferes with the legal basis of another party's data processing (i.e. a data subject cannot grant or remove consent for one party on another party's website).
- European Digital Identity Wallet proposed by the Commission's revision of the eIDAS Regulation could also be useful as a possible consent management tool. Consumers could be able to define preferences regarding personal data processing in their digital identity profile – which could also address issues facing certain lawful grounds, such as 'consent fatigue'. Qualified bots could be used to better inform data subjects of their rights.

While the possibility of exercising GDPR rights in open finance is crucial, it is important to consider the possible administrative burden of such consent management tools, as well as the potential cost of developing such a tool due to its complexity. Beyond consumer tools, the reuse of 'consent forms' could also avoid duplicative requests, lower the costs of attaining consent and facilitate clarity of data consent via a uniform format. In this respect, the 'common European data altruism consent form' introduced by the Data Governance Act will use a modular approach allowing for customisation for specific sectors and purposes in the context of altruistic data sharing.[22] Furthermore, data minimisation principles may also be facilitated through the employment of new market models for data intermediation, which are based on several ethical data walls and rely directly on open data. Namely, the intermediary may access and process open data without knowing the identity of the consumer and later pass on the results to the data user, which will be able to identify consumer but not to access his/her data or use other privacy enhancing technologies (PETs). This would also need to be facilitated by the regulatory requirements applicable to the service or product, and the Expert Group is

[21] In specific context of the PSD2 review, the EBA has recently recommended that Payment Service Users (data subject) be allowed to withdraw consent given to the Account Information Service Provider (third party provider) via the Account Servicing Payment Service Provider (data holder). See EBA's response to the Call for advice on the review of PSD2.pdf (europa.eu) (June 2022).

[22] The common European consent form will be introduced by the Commission via implementing Acts, see Article 22 Data Governance Act.

envisaging further work on the matter. Such scenario introduces limits to data access and processing. Some members argue that the use of such data collections is limited because of data anonymization and data processing.

5.5. Data perimeter for specific use cases

Some members argue that the introduction of precise 'data perimeters' for open finance use cases – clearly delineating the categories of personal data necessary for each open finance product or service - could be an approach to strengthen control over data use and enhance transparency in the data value chain. The aim of a data perimeter would be to define the list of permissible data to be used for each open finance use case (see example box below). Other members however disagree with this recommendation and feel that the concept of data perimeters would fail to serve to the purpose of offering innovative services to customers, limit the opportunity for promoting financial inclusion and would be technically challenging to implement to an extent that would negatively impact transparency and also competitiveness with other regions.

Example box: Opinion 11/2021 of the European Data Protection Supervisor (EDPS)

The European Commission adopted on 30 June 2021 a Proposal for a Directive on Consumer Credits. In Opinion 11/2021, the EDPS noted that the Proposal has a clear impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, in particular in light of the provisions concerning creditworthiness assessment, personalised offers based on automated processing and the use of personal data in the context of advisory and other activities.

To promote fair access to credit and data protection, the EDPS recommends clearly delineating the categories and sources of personal data that may be used for the purpose of creditworthiness assessment. In particular, the EDPS invites the legislator to strive for increased consumer protection and harmonisation by clearly specifying the categories of data that should and should not be processed.

There are benefits and challenges to implementing a data perimeter approach. In terms of benefits, some members argue that a data perimeter could create a controlled environment that excludes the use of other types of data beyond the list (and therefore minimizes the risk of data misuse). Moreover, they argue that perimeters can clearly delineate what categories of personal data are processed (including whether this may include certain special categories of data under Article 9 GDPR). In turn, they argue that perimeters may increase transparency and clarity in the decision process which benefit to industry and consumer as regards explainability of decision processes. Data in the scope of the perimeter would be safe to use for a specific use case. Data outside the perimeter could still be processed by data users but would need to be carefully evaluated, in line with EU data protection framework and in line with other relevant frameworks which may prohibit the use of certain data sets. From a financial inclusion perspective, some members argue that a data perimeter could be composed with data that everyone is able to provide – if this is not the case, exclusion may arise from the inability of a consumer to provide data, rather than the assessment based on the data provided (see Section

5.6).As an alternative to a data perimeter, a 'white list' of permissible data may also help strengthen a level playing field among financial institutions and others actors that might not have the same chance to access particular data.

On the other hand, other members argue that categories of processed personal data are already subject to clear delineation in the GDPR records of processing activities, and as such accessible to data subjects (GDPR Art 12 "Right to access"). Additionally, the GDPR Articles 13 and 14 oblige data controllers to provide data subjects with extensive information on the personal data processed. Defining a specific data perimeter for each product and service may be technically challenging and complex to implement, whereas GDPR Article 25 leaves flexibility to business for estimating and adjusting what data is necessary for each new project. Depending on the use case, data perimeters may not be sufficiently flexible to keep up with new innovative data opportunities that may arise through new data combinations.

In addition, defining a data parameter too narrowly may also undermine the ability of market participants to access a holistic view on customers: customers with 'thin' files may benefit from the inclusion of more variables outside of the data perimeter to access services.

Moreover, some members argue that a data perimeter may in fact legitimise the use of more data than is necessary (despite of GDPR Article 25) to the detriment of the data subject. They are concerned that the concept of data perimeter related to personal data would not be compatible with the principle of data minimisation under the GDPR (as some data users may use models with less variables, while others may use more variables). Indeed, some members argue that the concept of data perimeters may be challenging in the context of data use for AI models, which tend to use as many variables available as possible and have the capacity to define different segments that are affected by different groups of variables.

In the specific case of creditworthiness assessments, some members argue that the EBA guidelines establishes the need to gather all the required information to perform an adequate creditworthiness assessment.

Example box: EBA Guidelines on Loan Origination and Monitoring

5.1 Information and documentation

84. Institutions and creditors should have sufficient, accurate and up-to-date information and data necessary to assess the borrower's creditworthiness and risk profile before concluding a loan agreement.

85. For the purposes of the creditworthiness assessment of consumers, institutions and creditors should have available, and use, information supported by necessary and appropriate evidence
…
88. If the information and data are not readily available, institutions and creditors should collect the necessary information and data from the borrower and/or third parties, including relevant databases, when relevant

Some members argue that if data perimeters are to be used in open finance, they should be subject to a detailed case-by-case analysis, and only included where they provide a clear benefit to all. A starting point could be for the financial institutions to describe (transparency) the data perimeter currently used to allow the supervisor to control their GDPR compliance. As innovation can provide access to new and relevant data, the perimeter should be monitored and assessed by the regulator on a regular basis. Other members emphasise that data perimeters can be helpful for setting out what data is expected to be shared within the open finance model only but should not exclude existing data sharing systems. Other members however argue that adding extra supervision on models will increase the burden and would go against innovation.

An additional question is who should be responsible for defining the data perimeters, and what form these data perimeters should take.[23] The Expert Group envisages further work on the detail of data perimeters.

5.6. Consumer protection issues

The opening up of data sharing under open finance may create risks that need to be mitigated. These include:

- Risk of exclusion or overcharging because of certain characteristics[24]
- Risk of data misuse, misselling of advice or misleading advice in the context of switching between products and services, financial crime and/or fraud
- Cyber risks that could affect the consumer or underlying open finance infrastructure
- Liability claims due to the sharing of outdated or incomplete data sets
- Lack of consumer trust in the sharing or reuse of personal financial data

Certain consumer protection issues can be addressed in the context of contractual relations. However, in the event of more complex relations with more parties involved, the question remains open whom consumers may address with a complaint or an issue. For the comfort of the consumer, it might be preferable to establish clear liability framework (see Section 8 on liability issues).

Some members argue that it is an important a "requirement" to guarantee the access and use of "default option products & services" to people who have decided to share the "necessary" and only "the necessary data" with their financial services providers. These products and services should be the ones offered to guarantee the financial inclusion of people who might not have or may not have much digital data because of choice or life circumstances. Data subjects should have the right to give consent to share their personal data to decide on how their personal data is used.

[23] An example of a data perimeter designed by the financial sector itself - OPIN standard [Insert reference here to public version of OPIN standard: https://docs.google.com/spreadsheets/d/1Y0Gk_LpTvTNEfoDMdIxeD7juv3E8FKcbE3mHUJNV5JY/edit#gid=0]

[24] When, for example, the product design does not consider "digitally excluded" people's characteristics and needs

On the risks of exclusion: if consumers decide not to share their data, they may not get access to all the services and products offered in an open finance context. There is therefore a need to ensure that all consumers with a proper risk profile are proposed appropriate financial services and products, in line with applicable law. Some members stress that, 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. This does not mean that consumers which provide the data will automatically obtain a positive decision to access these services: the possibility to assess, for example, a person's income, should be universal – however this does not mean that all consumers are creditworthy. The important societal dimension to data sharing and reuse is also why some members argue that data considered 'necessary' for the performance of a contract should be precisely defined and presented to consumers in the pre-contractual phase (see 6.5 on data perimeter).

In addition, one important development that could be explored is the extent to which consumer protection could be enforced by new actors. In this respect, it may be important to consider the possible role that data intermediaries introduced by the Data Governance Act could play to ensure trust in data sharing. According to the DGA, providers of data intermediation services could make the sharing of personal data easier for data subjects to exercise their rights under the GDPR.

6. Data standardisation

The primary question raised during the discussion of the subgroup focused on the level of the data and API standardisation requirements, and the balance between providing market players with necessary flexibility while ensuring a certain level of data uniformity.

Summary of views on data and API standardisation:

1. Standardisation of data and APIs are an important element to support open finance. Different levels of and approaches to standardisation may be appropriate for different aspects of open finance.
2. API requirements should be flexible in order to adjust to changing market needs; an open finance framework should allow market players to implement APIs in a way that is suitable to their technical capabilities and resources.
3. The role of the regulator should be to focus on establishing a framework that incentivises high quality APIs and promotes standardisation of new market developments. This include defining a security and performance criteria. Examples of useful features for common data model developments are also highlighted in this section.
4. A higher level of standardisation is required for specific core data fields. Guidelines or a common taxonomy could be developed in collaboration with industry players to promote harmonisation of standards. Nevertheless, industry players should always be free to define additional company-specific data that can provide specific services and innovation and to differentiate in competition.
5. Standardisation should in principle stay at "business rules" level, not entering the technical implementation layer. Nevertheless, where there is evidence of market distortion, a minimum set of standardised data could be developed to guarantee the provision of innovative services.

6.1. The extent of standardisation required to achieve harmonisation at EU level and considerations when deciding on relevant standards

It was noted that that while a single API standard could be beneficial, it would likely result in difficulties in terms of implementation. Highly standardised API requirements can create barriers to adoption for market players due to extensive technical and/or cost requirements. The cost aspect would be especially acute to parties that would be required to replace already implemented APIs that meet existing recognized standards. Furthermore, enforcement of a highly standardised format would be harder to regulate and could lead to less efficient services. Accordingly, decisions regarding the extent of standardisation should weigh both usefulness and ease of implementation of the chosen standard/ framework.

However, some members argue that it may be beneficial to establish at least one API standard for each sector or sub-sector (e.g. vehicle insurance, life insurance) beyond existing PSD2 API standards. Individual firms would be able to decide to either use these agreed API standard or offer an API of their own.

Example box: opportunities of the Legal Entity Identifier (LEI) for open finance

The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code established by the Financial Stability Board (FSB) and developed by the International Organization for Standardization (ISO). Since its introduction, the Legal Entity Identifier (LEI) has been adopted by more than 2.1 million entities across more than 200 countries holding a unique LEI code for the clear identification of their organisations.

The LEI could play an important role in open finance by promoting standardised data identification and aggregation, improving data quality and transparency, and reducing costs related to verification checks. Data sharing could be made possible if data is collected in a standardised and harmonised way with structured identifiers, such as the LEI. Moreover, the LEI could facilitate identification of financial service providers and other legal entity parties in a seamless way through its publicly accessible Global LEI Repository.

In terms of data access, the LEI could also play an important role in the functioning of application programming interfaces (API). The LEI could allow consumers, API providers and supervisory authorities to identify API users. The use of the LEI to identify API users in this public list could facilitate verification and validation of the API users through open Global LEI Repository, which would reduce data accessibility costs for API providers substantially.

Especially important is for SMEs to be identified easily through their LEI, so they can pull their data together under this single identity, into a portable credit file to shop around for the finance they need. And because of its global recognition, it will help all businesses, but particularly SMEs, access trade finance. Another use case is the Global Value Chain Passport (GVC) promoted by the Business 20 (B20), which demonstrates how to design an authenticated, authoritative, verifiable 'financial fingerprint' of a given legal entity, based on its LEI. Leveraging the LEI as a global identifier, the GVC aims to overcome the need for companies to reproduce the same documentation on multiple occasions and eliminate duplicative verifications.

Supervisors like the ESRB have strongly recommended that relevant authorities pursue and systematise their efforts to promote the adoption and use of the LEI. In 2020, the European Systemic Risk Board (ESRB) issued a Recommendation (ESRB/2020/12) for the introduction of a Union legal framework to uniquely identify legal entities engaged in financial transactions by making use of the LEI.

Attention was also drawn to the implementation of the API requirements under the PSD2 (and the accompanying Regulatory Technical Standards), which provides an overall framework as well as obligations for interfaces, but does not dictate a specific API standard. This approach ensures technology neutrality and allows market players to implement the APIs in a way that is most suitable to their existing technical capabilities and resources. However, the flexibility of a framework approach also leads to different implementations of the API requirements and can result in variability of data formats and fragmentation within the market. Thus, a certain level of harmonization is required to ensure the development of open finance and interoperability with the data space.

Taking the above into consideration, the group identified a need for a higher level of standardisation for core data fields, while suggesting a more market driven and flexible approach for APIs and their technical specifications.

Market-driven open finance interface standards would enable market players to provide APIs and related data in a desired fashion without adding further regulatory restrictions. The role of the regulator would focus on establishing a general regulatory framework, providing incentives to implement good quality APIs and promoting standardization of new market developments. Notably, development of API framework should be considered in a cross-sectoral context, i.e. entities holding non-financial data (e.g. public sector data, utility providers, enterprise resource planning (ERP) providers) should be incentivised to develop APIs meeting similar requirements to financial APIs and should be based on widely recognized standards. Where relevant, this could consider cross-sectoral standardisation rules introduced by the proposed Data Act proposal and the Data Governance Act proposal.

A higher level of standardisation of core data fields (metadata such as identification attributes) would also achieve greater harmonisation and avoid regulatory interpretation that might cause fragmentation at the EU level. The standardisation may be implemented by delineating which data fields should be shared, how to fill such data fields and the minimum criteria that should be observed to implement established APIs.[25] The suggested elements for standardisation could include authentication and identity management (e.g., based eIDAS Regulation standards) and technical requirements (e.g., field names, messaging format syntax, information exchange protocols), and existing global data standards. Where there is evident and well-assessed market distortion, a minimum set of standardised data should be developed to guarantee the provision of innovative services across the sector and base access to required data. In this context it should be clear that the introduction of a possible minimum set of standardised data should not create an obligation for industry players to collect and provide data that are not relevant to their specific service offerings. The standardising should also consider existing regulations (e.g., eIDAS standards for identification, existing legal mandates

[25] Data standardisation and interoperability efforts are further discussed in the DGA and the Data Act proposals (with references also made to the Standardisation Regulation ((EU) No 1025/2012)). In the context of the PSD2, minimum criteria for APIs are already outlined within the Regulatory Technical Standards on strong customer authentication and secure communication under PSD2.

to use certain global data standards (such as the LEI requirements in EMIR, MiFIR, etc), flexibility to meet local specifics (e.g., different address formats), potential ability to be implemented on cross-border basis and alignment with existing widely used standards (including ISO standards).

Other issues that were highlighted include consideration of existing local projects and historical data transformation rules. It was noted that there may be national standards and ongoing projects that could be affected by common EU requirements. Furthermore, data standardisation efforts should consider historical data and a need to adapt data transformation process to a new framework.

To address certain issues explained above, a good starting point could be to rely on standards which are internationally agreed and recognized, such as standards published by the European standardisation bodies and the International Organization for Standards (ISO). The example provided above in the example box on the LEI (ISO 17442) could be supported and extended with following additional ISO standards:

- ISO 3166 – Country Codes
- ISO 5009 – Official Organizational Roles
- ISO 6166 – International Securities Identification Number (ISIN)
- ISO 8601 – Date and Time Format
- ISO 20022 – Universal Financial Industry Message Scheme
- ISO 20275 – Entity Legal Forms (ELF)ISO 4127 – Currency Codes
- ISO 24165 – Digital Token Identifier

In certain cases, the published standards provide the range of allowed values and the schema behind these values, but they do not deliver the exact use cases for application. For instance, country codes (ISO 3166) deliver codes on a country and on subdivision level as well. In some cases, there are overlapping codes for the same item and therefore two different values (one on country level and one on subdivision level) for identification. To ensure consistency among the different players, some members argue that it would be beneficial to establish a governance structure to define, manage and provide guidance for the different standards (covering both API and data elements). Such a governance body could be a bridge between private and public sector, between the regulator and the business, and in between different sectors beyond finance, also considering the role of the European Data Innovation Board in the framework of the Data Governance Act. An example for an already established by the public-private relationship is the Global LEI System. In sum, some members argue there is a need for automation in open finance based on open, fee-, and license-free (ISO) standards, in particular reference data (identifiers) and messaging data standards, which some members believe could be backed by a standard agnostic, neutral open source Common Domain Model which is able to support these standards (see Example Box on CDM - Common Domain Model highlighting features for common data model approaches).

Example box: the Common Domain Model initiative

Key enablers for global data standardisation are collaborative industry efforts coalescing into an open-source common data model. The Common Domain Model (CDM) initiative is arguably a sound illustration of such a forward-looking approach.

The CDM initiative was initiated by the International Swaps and Derivatives Association (ISDA). The initiative aims to help automate workflows, reduce friction between trading, risk management, settlement systems and improve interoperability between different market infrastructures, entities. Consistent reporting is a prime use case for the common data model. The initiative has extended across markets to support automation of securities lending processes with the International Securities Lending Association (ISLA), and bonds and repos processes with the International Capital Market Association (ICMA). As an "open-source, standardised, machine-readable and machine-executable blueprint for how financial products are traded and managed across the transaction lifecycle", the CDM present several helpful features:

Logical: As a scenario-based model, the CDM is documented through a logical data layer that defines a common path for different standards, systems, languages, and formats to speak to each other.

Reusable and Scalable: The CDM focuses on documenting the core granular data denominators that represent a financial transaction and associated primitive business events. This data can be reused across products to describe processes, business and regulatory workflows at scale.

Functional**:** The CDM goes beyond proposing a set of common data definitions by also documenting their relationships, how to instantiate the corresponding data records and compute automatically the state transitions of a business life cycle.

Human readable: By focusing on the data expected logic expressed in a very accessible language, the model is by design human readable, particularly with those less familiar with technology. Reference to contracts, regulations, best practices, examples are all readable in one place.

Open-source and test-driven: The CDM model is widely accessible for ongoing testing by participants within their existing environments. Its development is based on examples and sample test data provided by the industry.

Through a standardised of data definitions, the model sets the groundwork for the definition and designs of standard APIs, particularly when involved in applications reliant on external reference data sources such as GLEIF (for Legal entity identifier counterparty related data) or ANNA DSB (for reference data).

6.2. Entities that are well placed to develop relevant standards

The group focused on the role of the market players/ market groups and their expertise. The subgroup highlighted the need for standardisation efforts to remain flexible and at a 'business rules' level, leaving the market to decide on the technical implementation level.

The subgroup highlighted a possibility to base new developments on existing widely used standards. Attention was drawn to APIs under the PSD2, where several industry standardisation groups have emerged to work on API standards in the context of PSD2. For instance, markets players in Germany primarily use NextGenPSD2 XS2A framework developed by the Berlin Group, while market players in France use STET. In addition, SEPA was mentioned as another example of pan-European data standardisation to improve interoperability within the financial sector. These industry standards allow to reduce access fragmentation and complexity, although they currently do operate on more local levels. However, there is no enforcement mechanism applicable to these industry standards, which gives individual actors flexibility to change certain data fields and could potentially hamper interoperability. A potential tool to promote further harmonisation of these standards may be development of a common taxonomy in collaboration with industry players to ensure alignment with national and industry standards and practices.

The importance of collaboration within market groups was also highlighted in relation to data standardisation questions. It was noted that the development of API specifications and common standards for core data fields could be undertaken by market players who are well placed to understand the industry's needs.

Furthermore, it was noted that the variability of API frameworks under the PSD2 also created a business model for API aggregators. The aggregators connect different APIs into one single output and act as another commercial solution to the existing market situation. Some participants expressed a view that similar developments could be anticipated in a broader open finance context.

Discussion regarding possible standardisation frameworks also noted importance of utilizing the existing tools. Attention was drawn to requirements on interoperability and data spaces within the Data Act proposal (Article 28), and possible support from the European Data Innovation Board (EDIB) to identify the relevant standards and interoperability requirements for cross-sector data sharing (as provided in the Data Governance Act) and work of EU standardisation agencies. Notably, the EDIB could assist and advise the Commission on the data governance strategy, including questions on interoperability and development of technical requirements. The EDIB will also be composed of industry members, researchers, civil society and academia to ensure in-depth advice. However, the EDIB is a purely public authority body that will act solely as an adviser to the European Commission.

7. Liability issues

Open finance should be based on clear obligations and rights to determine liability with regards to accessing, processing, sharing and storing data. Entities in the data value chain must be able to address liability claims in cases of misuse and sharing of outdated or incomplete data sets. Addressing liability issues is therefore key to fostering legal certainty, accountability and trust in open finance.

Summary of views on liability issues:

1. A clear liability framework - a set of principles that clearly allocates liability – is required for open finance. Such a framework should apply as a minimum requirement for both contractual and non-contractual data exchange, provided that flexibility is maintained in the case of contractual liability and should preferably be based on existing rules.
2. A liability framework would need to remain flexible enough to accommodate new risks posed by digital innovation.
3. The development of dispute resolution procedures by market participants should be promoted to facilitate out-of-court settlements.

7.1. Contractual vs non-contractual data exchange

Members agree that a liability model is required for open finance, however a distinction should be made between contractual and non-contractual data exchange.

Where data exchanges are based on contractual agreements, liability questions could be established directly in these agreements. The parties would be free to agree the terms and conditions within the limits of applicable rules (consumer protection rules and specific protections applicable to SMEs). In case the data is directly delivered to the consumer who is also the data subject this would be covered by contractual arrangements with the consumer.[26]

Data exchange could also happen inside regulated financial services, in which case financial legislation applies in terms of customer and/or consumer protection and liability, such as PSD2 (in relation to payment accounts), Mortgage Credit Directive (in relation to mortgages), Insurance Distribution Directive (in relation to activities of insurance and reinsurance), MiFID II (in relation to the performance of investment activities). Current financial services legislation can address some of the risks based on key principles (e.g. ensuring that firms act in the best interest of the consumer, respect rules on disclosures, and provide sound advice).

Non-contractual data exchange could be based on existing legislation, which provides common rules governing liability and can be relied on to address issues of data misuse. Horizontal rules

[26] In a B2C context, relevant consumer protection rules include, for example, the Unfair Contract Terms Directive (Directive EU 2019/2161) protects consumers against unfair standard contract terms imposed by traders. In a B2B context, the Data Act proposal recommends introducing rules to safeguard proportionate liability terms in a contract, as per Article 13 Data Act (unfair terms related to data access)

would apply, for example to the right of data portability under the GDPR (for access to personal data), Database Directive and Directive 2018/1673 (in relation to SME information and IoT data), Product Liability Directive and, where relevant, national law (liability due to software malfunctions in in-vehicle case).

7.2. A framework to define and allocate liability for specific cases

While data exchange could be based on existing legislation, from a consumer's perspective, it may not always be clear to whom consumers can address a complaint in cases of non-contractual data exchange.

An example to clarify would be the case when an energy company provides energy consumption data to a mortgage intermediary. In this example, the data was wrong or incomplete, and therefore the mortgage provided was too high, leading to affordability issues with the consumer. In this scenario, the consumer may be confronted with a mortgage intermediary, energy company and a bank providing the mortgage all pointing towards each other. The open finance framework should clearly determine who would be liable - which in this specific case should not be the consumer.

Complications may also arise with respect to liability if the data sharing is not based on a contract. In the example above, the data intermediary, the energy company and bank may also struggle to divide responsibility amongst each other. In case the sharing by the energy company is not based on a voluntary contract, its liability should be limited. This is because the energy company cannot decide for which use cases with potential liability its data is used.

One way to address uncertainty may be to set a clear liability (or 'responsibility') framework - a set of principles that clearly allocates liability in an open finance context. The principles could assign clear roles and responsibilities to all the actors that participate in open finance, to avoid and manage potential risks that arise from the sharing of data. The liability framework should apply as a minimum requirement for both contractual and non-contractual data exchange. However, in the case of contractual liability, provided that the applicable regulations are complied with, there must be room for freedom of agreement between parties. It is also noted that any existing liability rules (in civil law and sectorial legislation) should be considered to clearly identify their scope and potential shortcomings. This will allow to understand the required extent of the liability framework and specific issues that it should address. In addition, the liability framework should be based on existing rules to the extent relevant to ensure coherence across legislation.

7.3. Dispute resolution

In addition, the development of **dispute resolution procedures** by participants for both contractual and non-contractual agreements should be promoted to ensure that liability can be allocated out of court, without having to resort to judicial proceedings[27]. Existing rules

[27] The Commission's 2018 report on the evaluation of the product liability directive showed that a clear majority of cases (68%) were settled through extra-judicial arrangements, such as direct negotiation with the person or entity held liable, or

should also be considered: dispute resolution mechanisms are established under the relevant financial services legislation (e.g. Mortgage Credit Directive, Insurance Distribution Directive). Moreover, FIN-NET provides a financial dispute resolution network of national out-of-court schemes that are responsible for handling cross-border disputes between customers and financial services providers, which could be applicable to an open finance context.

A liability framework would need to remain flexible enough to accommodate new risks posed by digital innovation. This is an issue that exists today as liability issues arise in relation to emerging technologies. In the insurance sector, one issue is that of cloned cars (e.g. VIN-number cloning) and potential negative impact this can have on the driver owning the original car, and cars requiring identification of the driver and impact of this data on the car owner (as opposed to older cars that do not have this technical possibility).

alternative dispute resolution methods. See Evaluation of Council Directive 85/37/ECC on the approximation of laws, regulations and administrative provisions of the Members States concerning liability for defective products.

8. Cost of data access and level playing field

Open finance must ensure a level playing field for all actors - big or small, start-up or incumbent. Proportionate and fair access to data can help promote a customer centric view that allows customers to reuse their data to access a broader range of products and services. If level playing field principles are not applied thoroughly, however, open finance may suffer from distortions in the market structure that can lead to less fair outcomes in terms of prices, quality, choice and innovation therein. These risks need to be mitigated in an open finance context.

Summary of views on cost of data access and level playing field:

1. Open finance should be based on fair and proportionate access to data for market participants.
2. To ensure the fair allocation of costs among different players of the data value chain, a compensation scheme should be based on the following principles:
    a. Principle 1: A fair compensation scheme should allow parties providing data (data holders) to recover cost (e.g. collecting, generating preparing and sharing the data) in addition to a reasonable margin of profit (see principle 3), except in duly justified circumstances where there may be an overriding public policy interest to enable data access for free.
    b. Principle 2: The data sharing framework should be based on incentives for data holders to encourage high quality data sharing.
    c. Principle 3: Any compensation exceeding the cost of the data sharing that is agreed between a data holder and a data user should be reasonable and should not lead to anti-competitive effects. However there may be specific cases where overriding public policy objectives would justify that data access should be provided for free.
3. Some members recommend that there should be at least one free-of-charge, real-time (user) interface for data subjects to retrieve their data and see this as a practical way of implementing the principles in point 2. Some members argue this would leverage on the GDPR right of data subjects to retrieve their personal data for free. Other members however disagree with this recommendation as they argue that provision of a real-time free-of-charge interface would not encourage data availability and can result in significant costs to individual open data actors, which would go against the principle of a fair allocation of costs between different participants in the data chain.
4. Market participants carrying out the same activity and creating the same risks should be subject to the same standards and same regulation in relation to competition, consumer protection and operational resilience.

8.1. Proportionate and fair access

The approach to data sharing should be cross sectoral and multilateral to avoid any distortion of competition between firms offering products, intermediaries, third party providers and other relevant stakeholders.

Some use cases conducted by the subgroup indicated that equal access to data is limited where all relevant data is held by one group of market players (e.g. in-vehicle data held by manufacturers). Standardised and direct data access framework could allow all relevant market actors to compete on an equal footing, which would safeguard effective competition and would also ensure transparency and promote switching for customers and providers as to which data are available. In this respect, the Data Act proposal may help by giving greater access to IoT data held by manufacturers. Moreover the proposed Digital Markets Act may help give greater access to online platform data.

In addition, use cases conducted by the subgroup pointed to possible level playing field risks if data use standards for different entities offering services in the financial sector are not fully aligned or are unevenly enforced. Open data frameworks should also allow customers to use their data to access a broader range of products and services (e.g. use of online sales activity data by SMEs). As a general rule, members stressed the chosen framework should aim to ensure a fair distribution of value and risks among all market participants. Ensuring proportional and equal access to relevant data could also help to guarantee the same opportunities regardless of the size of the relevant market player. It was further suggested that proportionate and fair access may be ensured if Data Holders can only benefit from open finance data access only if they also made their data available to third parties, i.e. ability to access data would depend on the participation in the overall data sharing framework. The scope of such proportionate data access would follow data sharing principles established within the Report (e.g. no obligation to share Enriched Data or Inferred and Derived Data as outlined in Section 8.2 below).

8.2. Compensation

Members agree on the importance to ensure the fair allocation of costs among different players of the data value chain to safeguard fair competition. A compensation scheme would need to be designed in a proportionate manner in a B2B context, and it should be determined on a horizontal approach in line the Data Act proposal which requires compensation to be fair, non-discriminatory and reasonable.

Several principles could be considered for a compensation scheme to attribute costs:

- **Principle 1:** A fair compensation scheme should allow parties providing data (data holders) to recover the cost of collecting, generating, preparing and sharing the data (e.g. putting in place the data sharing infrastructure and its maintenance, data collection, data validation and authentication, data preparation required for compliance with applicable laws, etc.) in addition to a reasonable margin of profit (see

principle 3), except in circumstances where there may be an overriding public policy interest to enable data access for free.

- **Principle 2:** The data sharing framework should be based on incentives for data holders to encourage high quality data sharing.
- **Principle 3:** Any compensation exceeding the cost of the data sharing that is agreed between a data holder and a data recipient should be reasonable and should not lead to anti-competitive effects. However there may be specific cases where overriding public policy objectives would justify that data access should be provided for free.

While views diverge, some members recommend that there should be at least one free-of-charge, real-time (user) interface for Data Subjects to retrieve their data and see this as a practical way of implementing the principles above. Members representing the consumer organisations are of the opinion that data subjects should have access to their personal data free of charge, in accordance with GDPR Article 12(5)[28] and note that the proposed Data Act limits compensation for B2B relations (Article 9 Data Act proposal), and that no compensation can be requested from the data subject. Moreover, some members argue that implementing at least one free-of-charge, real-time user interface for data subjects could benefit competition. They argue this would be similar to the provisions of Article 4(1)[29] and Article 5(1)[30] of the proposed Data Act. Other members however disagree with this recommendation. They argue that the recommendation contradicts the "principles for a fair allocation of costs between the different participants in the data value chain". Furthermore, it can result in significant costs to individual open finance actors, would not encourage quality data availability and would increase data sharing risks.

In addition, several areas have been identified for further work to design a fair and proportionate compensation scheme:

First, there is a need to understand the **different cost elements** that should be considered in a compensation scheme. Cost elements could include: (i) costs related to production of data, e.g. standardising data to facilitate sharing and reuse, data preparation required for compliance with applicable laws, etc.; (ii) cost related to maintaining data access, to maintaining the required infrastructure (e.g. APIs). Any data availability requires a setup and maintenance cost, to ensure the quality of the data and to control its availability, as well as to ensure the security

[28] According to recital 31 of the proposed Data Act, if the data holder and the data intermediary are unable to find an agreement that does not prevent the data subject to use his or her right to portability. In addition, Article 12(5) GDPR states that that information related to personal data 'shall be provided free of charge' except in case of requests unfounded or excessive.

[29] Article 4 (1) of the proposed Data Act states that, where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done based on a simple request through electronic means where technically feasible.

[30] Article 5(1) of the proposed Data Act states that upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.

of the data communications. Data access costs may also vary depending on the type of service (e.g. insurance, investment, banking), the scale of access, as well as the number of data access points in existence. It was noted that there is no clear distinction within open finance as to who is allowed to access APIs, which does not allow to efficiently control the potential scale of API users (as opposed to PSD2 that delineates which users should be authorised). Accordingly, a relevant supervisory body could create a public list of users that are allowed to access APIs to reduce data verification and authentication costs for individual API providers. Open public access to API user information could also reduce identification and authorization costs and prevent unauthorized access.

In addition, it was acknowledged that cost issues may arise in situations with limited access points (e.g. where data is not accessible and a new access point is being created) or other monopoly situations. Accordingly, when there is an evident and well-assessed market distortion, and when there are no other remedial measures to alleviate them, the data holders' ability to charge for data access should be limited through maximum compensation ceiling and associated cost restrictions (e.g. defining which cost elements may be recovered by fees). It was further suggested that any cost restrictions should aim to ensure to at least cover the costs of data sharing with other parties. There should also be safeguards from unilaterally imposed unfair terms to ensure level playing field. Moreover it could be considered to introduce disclosure and transparency requirements, e.g. the requirement to publish price lists under the Markets in Financial Instruments Regulation (MiFIR).

Third, some members argue that the cost division should consider the position of small market players, taking into account the principles in the Data Act proposal. Members stressed that it is important to avoid excessive data access costs to ensure similar footing for smaller and larger market players. Additionally, it was noted that costs incurred by parties whose business model is based on sale of data are likely to differ from parties that sell data occasionally/ it is not a central part of their business (e.g. differences based on scale of data sale, data processing processes, know-how, etc.). Therefore, these differences should also be considered when defining specific cost elements. Other members however argue that differentiating companies according to size may not be a relevant measure to judge a firm's bargaining position in negotiating cost. It may therefore be very difficult to make this principle a legal criterion.

It was also noted that in some situations or for some sectors a specific cost sharing model may be applied. For instance, data sharing between actors may be facilitated via a national data hub that may also be responsible for data quality oversight, other supervisory roles and help to keep track of the market actors with access to specific data. A possible example of this model is Denmark's PensionsInfo portal which is described in more detail in Section C. However, it is important to note that any national data hub should not be a costly intermediary in an open finance.

8.3. Principle of same activity, same risks, same rules

Financial regulation must ensure that all market participants carrying out the same activity and creating the same risks are subject to the same standards in relation to consumer protection and operational resilience. New entrants offering regulated financial services should and in

practice are fully under existing regulation, including regulation that protects consumers in the financial sector (e.g. IDD, MiFID, GDPR, DORA). However, there might be additional risks that are not adequately captured by the current supervisory framework, as indicated in the Joint ESAs response on Call for Advice on Digital Finance[31]. As indicated in the Joint ESAs response, complex arrangements within a company group that provides both financial and non-financial services with blurred lines between these services can pose certain supervisory challenges. Some market participants that are systemically important to the provision of financial services may also fall outside the regulatory perimeter of financial supervisors. Financial customers should enjoy the same level of protection, regardless of whether they are served by incumbents or new entrants, by bringing them into the scope of an open finance framework, irrespective of whether it is based on a mandatory or a voluntary framework. One way forward could be to create a license and a public list of users that are allowed access to APIs in an open finance context.

This license would come with a supervisory criterion that would outline the conditions for access, and the obligations to maintain access (e.g. AISPs in the PSD2). It may therefore be necessary to have clearly defined selection criteria on with whom data can be shared and ensure that it can be shared only with relevant market actors with the approval of the data subject.

Another way forward, advocated by other members of the group, would not go as far as requiring a licencing regime, which could hinder innovation and competition, but instead establish a "central registry" with certain adherence criteria, e.g. the implementation of data security standards and eIDAS qualified certificates for identification. Other members however argue that this would be problematic in terms of maintaining a level playing field and ensuring a high level of protection in areas such as cybersecurity. The Expert Group envisages further work on the detail of this matter.

Moreover, market participants in an open finance context may be engaged in different activities that generate different risks – and may require other rules as a result.

[31] The three European Supervisory Authorities (EBA, EIOPA and ESMA) published a joint report in February 2022 in response to the Commission's 2021 Call for Advice on Digital Finance. The ESAs note that the use of innovative technologies is facilitating changes to value chains, that dependencies on digital platforms are increasing rapidly, and that new mixed-activity groups are emerging. These trends open a range of opportunities, but also pose certain new risks. ESA joint advice master file (EIOPA) for BOS (europa.eu)

9. Key actors and success criteria for open finance

Summary of views on key actors and success criteria:

1. Designated authorities and stakeholder associations should monitor the evolution of the open finance market based on a number of established Key Performance Indicators (KPIs) and conduct market analyses and impact assessments of open finance's success in meeting its objectives.
2. Open finance participants could publish basic information on for example the open data services offered, the number of clients using these services and the volume of transactions executed in an open finance context to facilitate market monitoring/ assessment of success criteria. Costs for market participants should however be a factor to consider in the publication of such information.

9.1. Key actors in an open data framework

The discussions have identified seven main stakeholders[32] active in the data value chain: Data Subject, Data Rights Owner, Data Holder, Data User, Data Intermediary and Data Broker as defined in Section 2.

Use cases could be initiated by the Data Subjects, whose data is collected during provision of services and further processed, analysed and otherwise used in accordance with the purpose for their collection. Natural persons are entitled to certain rights related to their data as provided within the GDPR. Use cases could also be initiated by the data holders or the data users depending on the data sharing model (for more detail, see Part C)

The financial market players undertake a central role within the relevant use cases. Namely, financial institutions offer investment services/products (credit institutions/ asset managers/ investment firms/ insurance companies) to retail and professional customers, creditors and credit intermediaries are closely involved in the origination of mortgage agreements, SME financing includes lending companies as well as other payment services providers acting as SME Data Holders. Insurers and other financial institutions may also benefit as users of open data frameworks (e.g. providing insurance based on in-vehicle data, holistic overview of consumer insurance policies or switching services). Furthermore, open data framework can facilitate the development of new service providers (such as wealthtechs, financial and risk planners, insurance/pension dashboards and robo-advisors).

[32] These main stakeholder categories are not mutually exclusive: in certain cases, the data property rights holder may be the data holder or data subject.

An open finance ecosystem also places emphasis on the role of Data Brokers, including third party providers, which may act both as providers of services and information brokers. The relevant Data Brokers include PSD2 TPPs dedicated platforms, business data management vendors and verification providers, and independent and neutral automotive gateway administrators. In mortgage market, an important role is also undertaken by tied and independent credit intermediaries (the criteria for extended knowledge and assessment of market offers applicable mainly to independent intermediaries) and insurance intermediaries with part of their functions resembling the role of Data Brokers.

Relevant data holders for an open finance framework could also include public bodies (social security, tax authorities, land registries), credit registers and bureaus, private companies (utility and telco companies, ecommerce platforms, supply chain platforms/ online marketplaces holding data required for SME financing). Depending on the specific data elements getting exchanged, other TPPs may also be significant for provision of data when consumers use their services. These data holders could be in the position to significantly contribute to cross-sectorial data sharing, as data held by them could create innovative use cases and allow for interoperability between data spaces.

Other key actors include consumers (which act primarily as Data Subjects and should benefit from better tailored services), SMEs engaged in SME financing (acting primarily as Data Subjects) as well as OEMs and vehicle manufacturers (acting as Data Property Rights Owners or Data Holders of in-vehicle data).

9.2. Establishing an overall success criterion for an open data ecosystem

A possible success criterion for an open finance ecosystem should provide measures and goals that could be used to determine whether, and how well, open data initiatives have met their purpose. The success criteria may address open finance from several perspectives: access to more relevant data, including quality of data, reasonable costs/ fair prices, consumer choice and improve inclusion as well as specific use case KPIs[33]. It is noted that chosen KPIs should be aligned with the overall open finance goals of better access to data, improvement of financial products/ services, better financial stability of the ecosystem, more dynamic data sharing and emergence of new disruptive and innovative products/ services. Significant focus should also be placed on consumer interests and ensuring sufficient consumer rights protection within all of the value chain and by all of the relevant actors. This focus should help to minimise the risks of poor financial advice that could have e significant economic consequences for the individual customer.

Furthermore, for a commercial model to be viable, it is also important to identify all the costs incurred in making data available with quality (structured digital data, robust and governed data) and the necessary infrastructure to provide proper access. Improvement of the data

[33] KPIs could be: number of institutions involved, number of products / services signed, the deployment rate of open data solutions, overall increased provision of relevant financial products, etc.

exchange framework or relevant product can also be evidenced through resulting fairer prices (prices that allow financial health of companies without excessive costs for consumers).

Where data access includes personal data, the consumers should also be able to conveniently choose products and services that fit their needs. Accordingly, consumer should have the necessary informative capacity about the quality and characteristics of a product as well as tools to manage their data (e.g. to guarantee the capacity to exercise GDPR rights). This criterion could be evidenced through increase in consumer's ability to respect the T&Cs of the contracts due to being better informed, avoiding default risks and increase in overall consumer satisfaction /loyalty. Because of better and more granular risk selection (for example in insurance), and for the sake of the financial inclusion[34] of people with a higher risk profile, the market of financial products such as insurance considered as necessary for social inclusion should be adequately monitored to support an improvement of this segment due to more relevant and efficient risk assessment data to be used (e.g. IoT being used to complement collected data), appropriate pooling to guarantee affordable premium for all (fix a minimum level of mutualisation), better product design to maintain large access for higher risk profile (e.g. basic insurance package for higher risk profile).

Other factors for success criteria focus on both quantitative and qualitative performance factors. Suggested quantitative data include measuring the increase of the collected data, the number of institutions using new platforms and number of products/ services signed, the deployment rate of the open data solution (e.g. number of connected vehicles providing data, number of new products available), increased provision of relevant financial products (e.g. data on volume and value of SME loans provided by ECB statistics), percentage of supported public data and reduction in expected public spending in relation to investment products. Equally importantly, another method to measure success of an open finance ecosystem could be to primarily look at market terms, e.g. assess if open finance grows the market, also in terms of financial solutions. To facilitate these evaluations, open finance participants could be required to share basic information on the open data services offered, the number of clients using these services and the volume of transactions executed in an open finance context. However, it is recognised that such requirement could impose an additional reporting and financial burden for the relevant participants.

However, some reservation was indicated regarding imposition of technical KPIs due to difficulty in their implementation, enforcement and potential for bypassing such requirements. An example was drawn to API KPIs under the PSD2, whereas a high number of successful requests sent via the API is in reality misaligned with the rate of actual conversion rates (i.e. the number of successful payment service user authentications from the total authentication attempts). Therefore, it was suggested that KPIs should be primarily related to desired outcomes (what should be achieved) rather than method of doing so.

[34] ARTIFICIAL INTELLIGENCE GOVERNANCE PRINCIPLES: TOWARDS ETHICAL AND TRUSTWORTHY ARTIFICIAL INTELLIGENCE IN THE EUROPEAN INSURANCE SECTOR ,A report from EIOPA´s Consultative Expert Group on Digital Ethics in insurance, 2021, p.24

Moreover, many members argue that focus should be put on the definition and monitoring of only a few market term-KPIs for an open finance framework, also in line with possibly existing ones on EU level. On the one hand, to avoid redundancies, on the other hand, to not overburden market participants and the responsible regulatory oversight function. Furthermore, some members in particular advocate that the main priority in monitoring the success of open finance should be that it does not place an additional administrative burden on market actors.

Qualitative data placed attention to better financial health of the relevant market players (e.g. household and company solvency risk improvement), innovation in the sector (e.g. new SME lending products, new insurance products developed (e.g. due to access to in-vehicle data)), qualitative assessment of the financial education and awareness of the population, part of investment being made in ESG investments and climate change contribution, etc.

Notably, due to the significantly different local pension systems, tax systems, overall welfare model, etc. for the investment use case, a national technical solution should be prioritized to ensure achieving its goals and to avoid unintended negative consequences to local markets (e.g. by altering existing local pension schemes). Accordingly, the relevant success criteria should be tailored to the national pension system and chosen solution.

The effects of open finance may be identified by conducting market analyses and impact assessments of open finance's success in meeting its objectives. Some members stress that these assessments are the most important tool to determine the success of an open finance framework. Designated authorities and stakeholder associations may also monitor the evolution of the open finance market based on known performance factors, market surveys or other available tools although efforts should be made to avoid duplication of KPIs and reporting requirements which may increase costs for market participants. Additionally, monitoring may be established at a market level through documentation governing the relevant open finance framework, i.e. documentation may specify information that the participants should provide to the framework manager to be able to perform its monitoring obligations.

Such monitoring could also facilitate a periodic review of how the initially intended objectives are being met.

PART C: Open finance use case analysis

Part C presents a selection of customer journeys and related business requirements in relation to a first set of use cases on data sharing and reuse. The use cases were developed by teams within the Expert Group, and do not specifically represent the views of all members.[35] Moreover, the use case work is not always aligned with the definitions outlined in Section 1 of this report. Some use cases also assess linkages between financial and nonfinancial data among licensed financial institutions and entities outside the financial sector. Part C consists of five subsections:

- Section 10. Mortgage use case
- Section 11. SME financing / creditworthiness
- Section 12. Open investment data and financial advisory
- Section 13. Energy, sustainability and climate data
- Section 14. Sharing of in-vehicle data

Further use cases and examples may be added as part of a possible second round of analysis. This includes, for example, examining the possibility of including data from financial institutions (e.g. security and custody accounts) as part of the open investment data use case (see section 12).

10. Mortgage use case

10.1. The purpose of the use case and the problems it intends to address

The purpose of the use case is to utilise the European financial data space to improve the mortgage credit market for consumers by ensuring choices that better fit consumer's needs and personal circumstances. This use case aims to demonstrate the positive impact the financial data space can have on the mortgage credit market through improvement in products, advice and creditworthiness decisions and improved transparency due to a more effective and less costly data access process. An impact assessment based on the identification of market failures and a cost-benefit analysis is recommended if it is decided to address identified issues through complementary regulation.

It is considered that a well-functioning and competitive market should generally allow consumers the following:

- to access qualitative mortgage credit at a fair price that allows financial health of companies without excessive economic rent;

[35] In particular, members from the banking sector of this Expert Group disagree with the mortgage use case's assessment (see Section 10).

- to choose conveniently the credit that fits their needs and circumstances; in line with the sustainability of a consumer's debt profile;
- to be able to respect the terms and conditions of the credit contract and to avoid the risks of default of payment or, in extreme cases, even of eviction.

Taking the above into account, the consumer representative identified several issues in the mortgage credit market that could benefit from an improved access to data. From the consumer perspective, the relevant issues include:

- The complexity of the product that stems from the informational/ data collection requirements that are considered as cumbersome by many of consumer representatives, i.e. extensive criteria (data) that have to be considered by consumers when choosing credit (e.g. mortgage amount, applicable fees and interest, type of interest rate (fixed or variable), duration of the mortgage, required guarantee).
- The burden for consumers to collect the information for the credit offers they want to compare (e.g. due to different types of marketing channels provided by different credit providers).
- The popular combination of mortgage credit with other financial services such as insurance and /or other attached products (e.g. payment account) which increases complexity of an effective comparison. Therefore, consumers' representatives consider that improved data access and more uniformity in relevant data formats can ease effective comparison.
- The level and amount of information to be provided by the consumers pursuant to the Mortgage Credit Directive (MCD)[36] and EBA Guidelines on loan origination and monitoring[37] before receiving a final offer.

Therefore, the analysis provided within the use case addresses how the European financial data space may address each of the above-mentioned issues. Among the solutions envisaged, a particular attention will be made on the positive role credit intermediary can have and under which conditions.

However, please note that the creditor representative does not agree with the consumer view stated above, because the complexity of the product is not related to data access. If any new requirements are considered, these must be accompanied with a framework that provides benefits for both parties (e.g. credit institutions and consumers). The Commission's

[36] 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.

[37] Final Report on Guidelines on loan origination and monitoring of the European Banking Authority of 29 May 2020 (EBA/GL/2020/06).

Communication of November 2021 on the Capital Markets Union noted that the open finance framework will be based on a principle of a level playing field.[38] This should be kept in mind.

10.2. Summary of the use case

Different views prevail in the use case definition between financial industry and consumer representatives.

From a financial industry perspective:

The data minimisation aspect the minimal information principle outlined in the framework of the Mortgage Credit Directive and EBA Guidelines should be followed. There is no market need for additional TPPs to gather information. The focus should be on standardising the core data set to improve the service to across different actors.

Data which constitute trade secrets or other business-sensitive information, as well as information related to product and services features that is not public and is considered strategic, are not in the scope of the use case.

Representatives from the banking sector of this expert group disagree with the use case's assessment due to the potential risks which may be caused either by an increase in personal data collection by credit intermediaries or by reshaping the pivotal role of the credit intermediary. The representatives of the banking sector also believe that the use case does not emphasise enough the benefits that could be gained should an open finance framework enable broader sharing of Public Sector data, which could deliver clear benefits to improve creditworthiness assessment and access to credit (such as tax payments timeliness, eventual tax debit, land registry information, etc.). Therefore, they strongly recommend undertaking an impact assessment of the use case based on the identification of market failures and a cost benefit analysis.

From a consumer perspective:

The use case should be limited to exchange of personal data that is strictly necessary and follow data minimization principles (as established in the GDPR). Data exchanged within the use case should have a proven positive impact on the issues and problems identified within the mortgage credit market. A proper analysis of the personal data flows between stakeholders and the necessary privacy walls to comply with GDPR principles should be at the heart of the use case to reach the highest level of confidence for consumers.

[38] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 25 November 2021 'Capital Markets Union - Delivering one year after the Action Plan.

10.3. Methodology considered when analysing the use case

It is noted that not every consumer segment faces the same issues when accessing qualitative mortgage credit.

Prof. Yi-Cheng Zhang, physics professor at the Fribourg University in Switzerland and director of the Complexity Research Center of Alibaba, in his book Matchmakers & Markets: The Revolutionary Role of Information in the Economy[39] proposes a new economic theory based on the role of information. The theory gives rise to a third actor – the information broker or "information matchmaker", which acts besides consumers and providers of services. It also defines a new metric called "infocap", which is the informative capacity that a consumer has about the quality and characteristics of a product.

A consumer with infinite infocap will know everything about a product. A consumer with infocap = 0 will not know anything about that product. The infocap depends on consumer's own factors (culture, experience, talent, and effort comprising diligence given to the task) as well as external factors (which can influence consumer's cognitive capabilities). Every analysis on how the financial data space can make the mortgage market simpler for consumers should include this infocap driver.

Relevant analysis should also consider specifics of different economic regions since empirical evidence shows that in advanced economies financial services are widely available and the credit markets will be more developed.[40]

Causal relationships leading to data exchange in the mortgage market and its improvement in terms of fairer prices should be evidence based.

10.4. The steps, information and data necessary to guarantee a qualitative advice from a credit intermediary

Credit intermediaries, sometimes also called mortgage brokers, provide value-added services to credit/mortgage requestors and/or to credit/mortgage providers. Often, they are collecting credit offers from multiple providers, e.g. banks, and then assists the requester in selecting, agreeing, and handling the mortgage contract throughout its lifetime. In other cases, they help credit providers to extend their reach, for example in running promotions.

Credit intermediaries are regulated by the MCD as they are considered as closely involved in the origination of credit agreements. The Article 4(5) of the MCD defines 'credit intermediary' as a natural or legal person who is not acting as a creditor or notary and not merely introducing, either directly or indirectly, a consumer to a creditor or credit intermediary, and who, during his trade, business or profession, for remuneration, which may take a pecuniary form or any other agreed form of financial consideration:

[39] Oxford University Press, 2020.

[40] BIS working paper no 986 on Platform-based business models and financial inclusion of January 2022, p. 16. https://www.bis.org/publ/work986.pdf

(a) presents or offers credit agreements to consumers;
(b) assists consumers by undertaking preparatory work or other pre-contractual administration in respect of credit agreements other than as referred to in point (a); or
(c) concludes credit agreements with consumers on behalf of the creditor.

Credit intermediaries are also partially competitors to creditors since they get a part of the value chain of mortgage loans. Therefore, any distortion of competition between these parties should be avoided.

The MCD further distinguishes between independent and tied credit intermediaries. The Article 4(7) of the MCD defines 'tied credit intermediary' as any credit intermediary who acts on behalf of and under the full and unconditional responsibility of:

(a) only one creditor;
(b) only one group; or
(c) a number of creditors or groups which does not represent the majority of the market.

As a result, it should be considered that tied credit intermediaries would probably assess a limited number of providers. Therefore, the criteria for extended knowledge and assessment of market offers will have to target independent credit intermediaries.

It is also relevant to note that consumers use credit intermediaries for a variety of reasons with the main ones being convenience (removes the need to assess several credit providers' offers) and financial literacy concerns (lack of the necessary understanding of mortgages and related issues by the consumer).

The following stipulations are proposed for guaranteeing qualitative advice from a credit intermediary:

- The independent credit intermediary has extensive knowledge (potentially an established minimum percent of the market) about the mortgage credit proposed on the market and has collected the data based on which a credit should be chosen (e.g. a list).

  Consumers' representatives consider the added value of credit intermediary relates to the quality of its analysis. The existence of a credit intermediary, for the time being, has not guaranteed (in all cases) an improved credit decision. Therefore, to generally improve quality of analysis it is essential to address the following question: How to ensure that the credit intermediary is analysing a significant share (or even 100%) of the mortgage market? Does the answer to above question relate to financial data space or some other instruments? The quality of credit intermediaries' service is regulated by the MCD.

- The credit intermediary understands demands of the borrower (potentially through a structured questionnaire) and has identified the specific criteria that matter for particular consumers. To make sure that the credit intermediary brings added value, the following question is essential for consumer representatives: How to make sure

that the credit intermediary is properly analysing the demand and relevant personal circumstances of the client? Does the answer to above question relate to financial data space or other instruments? The credit intermediaries' services to the client are regulated by the MCD.

- The credit intermediary provides to consumer a short list of final offers that includes all costs – insurance fees, other fees, other financial services attached to the mortgage credit and expected changes in these cost (e.g. whether the fees are fixed or use variable rate, changes in insurance premiums, etc.). To make sure that the credit intermediary brings added value, the following question is essential for consumer representatives: How to make sure a short list of final offers is provided? Does the answer to above question relate to financial data space or to other instruments? The credit intermediaries' services to the client are regulated by the MCD.
- The credit intermediaries' remuneration does not "prejudice their ability to act in the consumer's best interest" and is set in a way that avoids potential conflicts of interest (Art. 7(4) of the MCD).

10.5. Broader policy objectives that should be considered in relation to the use case

Any additional data envisaged for Credit Worthiness Assessment (CWA) should be based on a proven added value and consider the following considerations:

- The potential improvement of CWA based on access to payment account data;
- Ability to strictly comply with the GDPR and establishing privacy walls, i.e. information barrier protocols intended to prevent exchange of information that may lead to conflicts of interest (privacy walls are already operated by private companies);
- Compliance with the EBA Guidelines on loan origination and monitoring regarding the CWA requirements;
- Capacity to provide a clear response on the reason for refusal of credit;
- The quality of the data (e.g. complete, up to date, accurate, etc.) and its capacity to limit risk of undesirable bias of discrimination;
- The capacity to guarantee data access to all players (strengthening the level playing field principles);
- Cost effectiveness of access to and use of additional data.

In addition, it would be important to outline the relevance of the mortgage use case for all the stakeholders (also considering the diversity of consumers and not only as one sub-group), impact on competition, on market supervision and companies' compliance with supervisory authorities.

10.6. Analysis whether the relevant data is already stored and by whom

"General Information" listed in the "Pre-Sales" phase is already stored as follows:

- High-level "Product & Portfolio information" is typically available on the website of the creditor.
- More detailed mortgage conditions and terms and conditions (T&Cs) are usually available in a PDF format, stored on the creditor's system. Article 14(1-2) of the MCD also establishes a requirement to provide consumers with pre-contractual personalised information needed to compare the credits available on the market, assess their implications and make an informed decision on whether to conclude a credit agreement. This pre-contractual information is provided through the European Standardised Information Sheet (ESIS) on paper or on another durable medium. The ESIS format is established in the Annex II of the MCD.
- Prospect data is stored by credit intermediaries; however, it is not publicly available.
- The mortgage calculator or comparison tool is provided by the credit intermediary and is usually available on the credit intermediary's website and/or its intranet with the results also made available to the customer via email or PDF.

The information required for the "Contract Preparation" phase comes from various sources, but most, if not all, of that data in some form is also stored by the Data Subjects themselves. The exception from that is account information of the customer, which is stored by his/her banks or other PSPs, although customers may also have a copy of it stored themselves.

10.7. Overview of existing access to data via regulatory requirements and/or contractual arrangements and relevant legal issues

10.7.1. Access to data in the Pre-Sales phase

Creditors have a legal obligation to provide a certain set of information about their offers. Therefore, pre-sales information is often publicly available, e.g. on their website or can be obtained in written format from their branches.

More detailed T&Cs will be the intellectual property of the creditor and visibility to them may only be given following a contractual agreement, which in this case would be between the creditor and credit intermediary. Access to the credit intermediary's mortgage calculator or comparison tool is typically also subject to a contractual agreement, in this case between the credit intermediary and the customer.

For comparison in the aspect of transparency for the consumer of mortgage loans, the United States Home Mortgage Disclosure Act (HMDA) requires financial institutions to maintain, report, and publicly disclose information about mortgages. Starting in 2018, the loan originator is identified via the Legal Entity Identifier (LEI) and the universal loan identifier (ULI) which is used to uniquely identify each loan and incorporates the LEI. This enables the following consumer protection analysis in a consistent and standardised way:

- Given the originator LEI is embedded in the ULI, data users can always trace the loan back to the originator regardless of whether the loan is subsequently sold. Additionally, given the history of legal entity reference data available in the Global LEI System, the loan originator can be traced even if it subsequently merges or retires. This improves the ability to assess whether financial institutions are meeting the housing needs of their communities regardless of changes to corporate structure over time.
- Information on direct and ultimate 'parents' will help public users understand differences in loan originators across group entities. For example, public users or even institutions themselves will be able to compare loans originated by different subsidiaries and investigate if there are anomalies for similarly situated originators.

10.7.2. Access to data in the Contract Preparation phase

Data collected during identification (KYC) process:

Identification data for Know Your Customer requirements (KYC) is currently provided by the consumer based on his/her identification documents in compliance with the Anti-Money Laundering Directive (AMLD)[41].

Data collected during CWA:

Art. 18 of the MCD established an obligation to assess the creditworthiness of the consumer, including his/her financial data. As per Article 20 of the MCD, the CWA is based budget related data demonstrating income and expenses (flows) of the consumer and other relevant financial and economic circumstances. Patrimony assets (credits and debts) also have an impact on the income and expenditures (budget) and are an important part of the CWA. Data on these assets are available from diverse sources (e.g. credit register, open banking, etc.). However, the CWA should not be predominantly based on the value of the residential immovable property (Article 18(3) of the MCD). Article 19 of the MCD also establishes principles for property valuation.

Furthermore, specific data to be used for CWA is already thoroughly outlined by the EBA in its Guidelines on loan origination and monitoring. Therefore, the assessment in the use case exercise would benefit in being aligned and kept within this list.

Annex 2 of the Guidelines on loan origination and monitoring lists the following information and data for the CWA when lending to consumers:

1. Evidence of identification
2. Evidence of residence
3. Where applicable, information on the purpose of the loan
4. Where applicable, evidence of eligibility for the purposes of the loan
5. Evidence of employment, including the type, sector, status (e.g. full-time, part-time, contractor, self-employed) and duration

[41] 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

6. Evidence of income or other sources of repayment (including annual bonus, commission, overtime, where applicable) covering a reasonable period, including payslips, current bank account statements, and audited or professionally verified accounts (for self-employed persons)
7. Information on financial assets and liabilities, e.g. savings account statements and loan statements indicating outstanding loan balances
8. Information on other financial commitments, such as child maintenance, education fees and alimonies, if relevant
9. Information on household composition and dependants
10. Evidence of tax status
11. Where applicable, evidence of life insurance for the named borrowers
12. Where applicable, data from credit registers or credit information bureaux or other relevant databases, covering the information on financial liabilities and arrears in payment
13. Information on the collateral, if any
14. Evidence of ownership of the collateral
15. Evidence of the value of the collateral
16. Evidence of insurance of the collateral
17. Information on guarantees, other credit risk mitigating factors and guarantors, if any
18. Rental agreement or evidence of potential rental income for buy-to-let loans, if any
19. Permissions and cost estimates, if applicable, for real estate building and improvement loans

Financial data related to budget-flows – usually available on the payment accounts:

The situation is different where the data is held by a party other than consumer, e.g. bank account data held by customer's bank, customer data held by a credit intermediary or a TPP. When not using online services, providing such data may be a cumbersome manual process, which should be automated as much as possible (especially for the purpose of establishing the customer's creditworthiness). However, access to and processing of such (personal) data by anyone other than the customer requires a lawful ground according to Article 6 of the GDPR, which applies to both the Data Holder and the Data Broker. Such lawful ground could be contractual agreements, but there are alternatives, e.g. the legal obligation of a bank (Data Holder) to allow access to payment accounts by a PSD2-licensed Data Broker. The Data Broker, i.e. the credit intermediary in this case, on the other hand, does not have such a legal obligation and therefore must obtain another lawful ground, e.g. the customer's consent or performance of a contract.

Where PSD2 open banking data is used, it is also important to have a process to make the provision of payment account data to third parties compliant with the GDPR principles of data minimisation. That is, only the data necessary for the CWA should be used and amount of collected data minimised. Therefore, not all data/information should be accessible or used. The appropriate granularity and perimeter of data should also be in some ways standardised to facilitate data use and to ease the capacity to explain credit decisions.

Other financial data (assets, savings, etc.):

The PSD2 and Commission Delegated Regulation (EU) 2018/389[42] supplementing the PSD2 only regulate access to payment accounts that are accessible online and are provided by account servicing payment service providers. Therefore, access to data from "non-payment" accounts is not regulated under the PSD2 but solely by the GDPR, which is why this case is looked at separately here. The GDPR access and portability provisions are rather generic and do not specifically differentiate between Data Holders offering real-time online access to the customer's data, or not. Pursuant to Art. 12(3) of the GDPR, the controller must provide the customer data "without undue delay and in any event within one month". Therefore, data controllers who do not offer real-time online access are given up to one month for provision of data, whilst those who do offer real-time online access would arguably cause undue delay if they would obstruct their customer in accessing and retrieving their data in real-time. Based on this, it is common practice that customers can either manually or automatically browse their bank account data in real-time or can give consent to a service provider doing that on their behalf. This practice could apply here for establishing the customer's creditworthiness relating to non-payment account records, e.g. savings or securities accounts. However, the purpose of this use case is not to extend the PSD2 beyond payment accounts.

As outlined above, obtaining data on "other assets" that are not accessible via an online account could potentially result in a one-month delay. Therefore, where creditworthiness investigations relate to such other assets (information from nr. 7 of the credit origination guideline list above mentioned), it makes more sense for customers in some form to provide the required information themselves to avoid access delays.

Some members highlighted that the key piece of information is the appraisal/valuation of the house that guarantees the loan. For banks, the ratio, loan to value, is a key element to decide on admission. For consumers, the valuation has a high impact on the terms and conditions. Therefore, the online open availability of information from valuation companies could also have a positive impact on customer experience as it would significantly reduce timelines in giving an admission response.

Credit risk assessment using credit bureau/register data must be separated as well since they follow very different rules. In such situation the financial data is collected by a third-party credit bureau and is processed based on legitimate interest, with the consumer informed in advance via the T&Cs of their bank or other relevant credit provider. Granting the creditor access to that data and credit scoring is often mandatory for getting mortgage offers. In some EU countries creditors have a legal obligation to consult credit databases whereas in some other this is not the case (see COM mapping[43] of national approaches in relation to credit risks assessment and ACCIS' survey[44]). Moreover, the content of such database varies between

[42] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

[43] https://ec.europa.eu/info/sites/default/files/mapping_national_approaches_creditworthiness_assessment.pdf

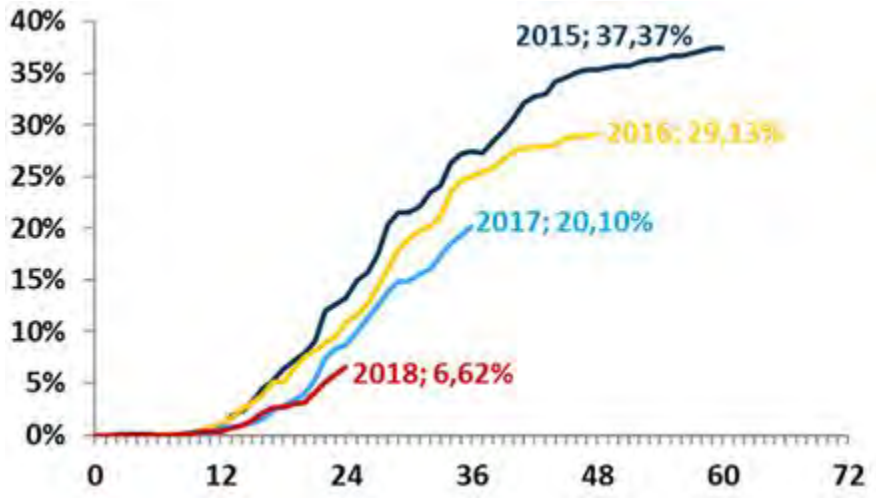
[44] https://accis.eu/facts-and-figures/

countries and can include only negative (e.g. overdue debt) data (e.g. in France) or, most frequently, both positive and negative data, coming from various sources and updated according to different timescales depending on the database.

10.8. Creditworthiness assessment using non-traditional information

Lack of traditional credit history, as per the CWA examples listed above, means that potential mortgage borrower segments (i.e. younger people that have not yet built an extensive credit history, often called thin file customers) may struggle to access loans due to less favourable offers (e.g. higher interest requirements, etc.). Innovative players are exploring ways of collecting "non-structured/ alternative data" (to the extent they are compliant with the MCD) to improve predictive power for their credit risk models. That would lead to broaden the scope of customer accessing a mortgage loan or to guide/help the individual to build a credit history to receive more favourable/ better tailored mortgage loan offers.

In some regulated players and countries a non-traditional risk assessment may take the form of psychometrics questionnaires or the combination of mobile data (questionnaires may be used as one of the elements influencing the crediting decision and complimenting the CWA). For example, the use of an online psychometric questionnaire in the loan application process within a portfolio of self-employees, thin file customers in a European retail bank showed that the use of non-traditional data may be, at the same time, **credit inclusive and a booster for the credit model accuracy, leading to dramatically lowering default rates. As you can see in the chart below, write off rates before the scoring deployment (2015 and 2016) were 30-37% and after the deployment (2017 and 2018), the write off rates hovered 6-8%.**[45]

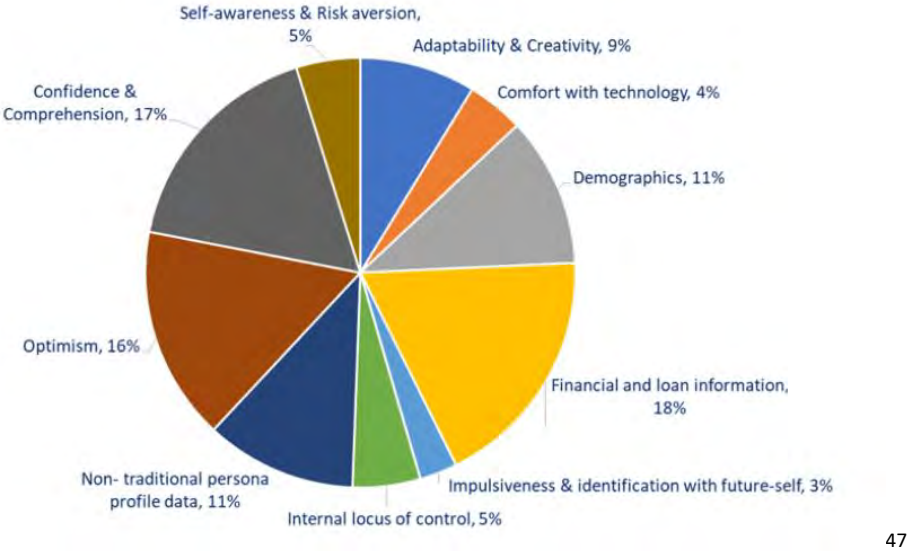


[45] Source: MicroBank (Caixabank's Social Bank) – 2022.

Young customers willing to ask for a mortgage may face the same problem as self-employees or other thin file customers looking for cash flow loans: by definition, they are not able to provide much credit data, but they do provide alternative data.

Lower default rates mean more clients could benefit and access the mortgage market if similar approaches are assessed.

Psychometric data looks for personality traits (optimism, confidence, self-awareness, locus of control[46], etc.) as drivers for default but also, and more important, gives the customer a hint on what he/she could do to improve the likelihood of accessing a loan when no traditional data can be provided. **It is a tool promoting credit inclusion.**



47

Nevertheless, there is the risk for players that are not regulated in the financial sector or other Third Parties or matchmakers to use different alternative data, coming from browsing behaviour, emails, etc. and leading to unfair competition, as seen in the text below from BIS working paper no 986:

"In credit, one of the biggest drivers of insolvency are divorce proceedings. This is generally not known and hence cannot be used by traditional banks. Yet big tech providers may be able to infer from browsing behaviour, e-mails, transaction or geolocation data if an individual is having an affair, if a couple is in marriage counselling or if they are likely to be divorced in the near future. This knowledge, gleaned from big data and machine learning, and perhaps not even clear to the (human) staff of a platform provider, can give an incomparable advantage to platform lenders. These providers may automatically decline from showing a credit product to that individual, meaning that this potential borrower ("lemon") is left for traditional

[46] The degree to which a person believes that he/she has control over the outcome of events in his/her live (as opposed to external forces).

[47] Source: MicroBank (Caixabank's Social Bank) – 2022.

competitors. The level playing field may then be compromised and competition would suffer."[48]

However, while use of both non-traditional/unstructured data and traditional data can improve scoring models' predictive power (thus producing a better outcome for thin file consumers willing to ask for a mortgage), it also raises some privacy issues. Therefore, these two aspects should be balanced against each other.

From a consumer protection perspective, any potential usage of non-traditional data should be assessed against the intrusiveness and excessive disclaiming that may be asked for. Thus, it should be demonstrated that the benefits arising from use of non-traditional data are real and outweigh the detriment that can arise from the data exploring.

10.9. Existing technical solutions to make the data available

Once consumer consent is obtained, any exchange of data happening directly between the Data Subject and the Data Broker would normally be done mostly online or by email, fax, post, phone or physically (branches). Any non-manual, automated exchange, in particular between a Data Holder and the Data Broker, requires a less standard, technical solution.

Access to payment account data is regulated under the PSD2, which requires to permit access to payment accounts either through the use of a "dedicated interface" or the use of any existing "user interface". Access to non-payment accounts, on the other hand, is available only through user interfaces as there are no equivalent third-party access rules in relation to these accounts.

In this context it is important to differentiate between the interface technology (e.g. API or HTTP) and whether the interface is dedicated or not. Historically, user interfaces were mostly HTTP based but are now increasingly API based (e.g. mobile apps). Similarly, service providers (e.g. TPPs under the PSD2) are more frequently using APIs instead of HTTP to access interfaces primarily "dedicated" to them, i.e. not accessible to users directly. Such dedicated APIs are typically limited to payment accounts due to their regulation under the PSD2. However, some of these APIs are now getting extended to non-payment accounts, whilst at the same time "losing their dedication", so that they become accessible to users as well, e.g. corporate bank APIs.

Retrieving data from accounts that are not accessible in real-time online (through standard browsers), is sometimes available through non-standard, bespoke arrangements, e.g. allowing a download from a "data portal" made available for such purpose. A common example of this arrangement would be some of the BigTechs providing links (on request) that allow users to download their data.

[48] BIS working paper no 986, p. 10.

10.10. Current level of data standardisation within the market and further steps for harmonising data formats and access conditions (to ensure that data sets are of needed quality)

The PSD2 has encouraged financial institutions (account servicing payment service providers) to make payment account information available via standardized interfaces (API) for third party service providers. This enables the Data User the access to well-structured and standardized data and eases further processing and analysis. However, even with the PSD2 there is no one single API standard and even though most of this data is standardized, it is not harmonized across all players. Therefore, received data often requires additional transformation steps before the third-party service provider can fully utilize the data.

The creditor representative also highlighted that while there is no one single PSD2 API standard, banks and other stakeholders (including TPPs) invested a lot in implementing the required API standards. Therefore, relevant financial institutions are not interested in rebuilding APIs or re-adjusting their business model to new APIs.

In addition, some of the data is obtainable only from the contracts between the different parties. This data is unstructured, sometimes even only available as a scanned pdf document. This hinders automated information extraction and further data processing. To overcome this challenge an application of additional standards could be explored and evaluated. A possible starting point could be the Open Contracting Data Standard, already widely used for public contracting.[49]

To ensure certain level of data quality, there is a need for dedicated unified data governance and data quality management programs. Specific goals (e.g., quality criteria such as accuracy, reliability, completeness, validity) and requirements on the data (e.g., exact thresholds per criterion) will enable the development of a suited framework with corresponding data quality gates. For instance, pre-check facilities could enable remediation of potential quality issues before data reaches the next gate.

10.11. Data protection framework

10.11.1. Enforcement of personal data, commercial data and intellectual property rights

Some high-level data about the mortgage offer (e.g. ESIS document) must be made available publicly, as defined in the relevant mortgage legislation. However, most of the data exchanges in this use case must be protected through contractual agreements, in particular all commercial data and intellectual property rights. All personal data is of also protected by the GDPR.

[49] More information available here: https://standard.open-contracting.org/latest/en/.

10.11.2. Application of the GDPR data principles (e.g. data minimisation, purpose limitation) and legal grounds for the processing (e.g. consent, contract)

Each of the data processing entities, in this use case particularly the creditor and credit intermediary, is obliged to comply with the GDPR. Prescribing how these obligations must be complied with does not seem to be necessary. Nevertheless, the clarification of precise perimeter, as the EDBS support in its opinion on the new consumer credit directive and as the EBA describes in its Guideline on Loan origination, seems to be a good practice from a consumer perspective.

10.11.3. Establishment of privacy walls to limit access to Raw Data

Data access limits or segregation requirements are defined by law and it would seem sufficient to rely on existing procedures for their enforcement, especially in the financial services area, where the relevant entities must be licensed or are otherwise supervised. Building additional technical barriers would have a high risk of creating obstacles.

10.11.4. Operational challenges to implement a state-of-the-art data governance framework

This use case does not seem to suggest the need for any additional data governance beyond the existing legislation. One potentially questionable part relates to the automated exchange of data without the presence of the Data Subject and which is not specifically regulated already, i.e. not under the PSD2. However, as explained above, this appears to be sufficiently regulated by the GDPR, so that additional data governance would not be required.

10.12. Issues related to the costs of making data available

Data are not at the heart of the value creation of mortgage brokerage. Credit intermediaries can easily get the data they need from prospects either online or through branches. The heart of the business is firstly a commercial service – providing an access for customers to mortgage loans either online or through branches. Other secondary services include a preliminary risk assessment and a comparison between different credit offers which requires exchanges with several credit institutions. Credit intermediaries are generally remunerated for these value-added services rather than provision of data since consumers wishing to obtain a loan can to provide credit institutions with required data directly. Analysing the role of brokerage through data is a very narrow approach to the business and overlooks the main value of credit intermediaries. In addition, the approach of any business case concerning relevant data should be cross sectoral and multilateral to avoid any distortion of competition between creditors, credit intermediaries, TPPs or other stakeholders.

10.13. Possible liability issues that would need to be addressed within the use case

The majority of data exchanges in this use case, and the liability questions arising from them, must be based on contractual agreements, where the parties are either mainly free to agree to the T&Cs (in case of business-to-business contracts) or free within the limits of consumer protection rules (in case of business to consumer contracts).

Any non-contractual data exchange and liabilities would be based on existing legislation, in particular the GDPR, the MCD and the PSD2.

11. Enhancing SME credit worthiness assessment to improve SMEs financing

11.1. The purpose of the use case and the problems it intends to address

Access to credit by small and medium enterprises (**SMEs**)[50] is an important opportunity for SMEs' financial health and development. SMEs frequently have challenges accessing credit and frequently face higher transactions costs and higher risk premiums than larger enterprises. Lenders often lack sufficient information to assess adequately SME creditworthiness, price credit risk and tailor credit products. To make sure the credit provided is appropriate to the SMEs' needs and adapted to their economic and financial circumstances, credit institutions and other parties providing loans might benefit from the access of data that allow them to better tailor their offers. This improvement in the quality of financing (size, duration, cost) and in the relevance of the credit form might impact positively the general health of SMEs – more balanced balance-sheet, better debt structure (LT/ST), reduction of financial costs, etc.

11.2. Summary of the use case

This use case aims to improve SME CWA to offer them better access to financing considering their online commercial activity and other cross-sectoral data.

Using online commercial activity and other cross-sectoral data improves SME CWA and, therefore, SME financing. These data help to paint a 360º business view and allow a better understanding of SME needs. Additionally, online commercial activity provides a rich and reliable view of the performance and strength of the SME business and can be used to help them get better CWA, financing and additional financial services embedded in their digital activities.

Furthermore, helping SMEs contributes to improved productivity and hence economic growth.

11.2.1. Key actors within the use case

The key participants of this use case are: SMEs, utilities, bureaus, ecommerce platforms, supply chain platforms, online marketplaces, SME data providers, banks, payment services providers, public sector, lending companies, and providers of services to lending companies.

11.2.2. Type of data considered within the use case

In terms of data, the use case aims to go beyond current data being traditionally used in the admission process, considering cross-sectoral data which can contribute to have a holistic view of SMEs, with higher quality, reliable, precise, richer and up-to-date data. In particular, the following data was considered:

[50] As defined in the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

SME identification data:

Data held by business registries which plays a key role in SME identification, group structure and source of powers of attorney. For proper management, it is crucial to understand the SME perimeter, i.e. the ownership structure and whether it is part of a group of companies.

Additionally, SME identifiers are key in linking data from different sources.

The business registries in EU member countries must be made publicly available as mandated within the Open Data Directive.[51] Unfortunately, there is no consistent implementation of the Open Data Directive among all countries nor standardized formats that ensure a common understanding of the information available.

There are different initiatives aimed to better identify companies, such as Legal Entity Identifiers (**LEIs**) and the global registry, as well as others.[52]

Global LEI Repository is an open source for legal entities' identification. The LEI is a 20-digit alpha-numeric code based on the ISO Standard 14772. It connects key data elements enabling the unique identification of entities world-wide. In addition, the LEI provides insights about the corporate structure of an organization by displaying the direct and ultimate parent-child relationships based on accounting consolidation. Through the established mapping program, the LEI is already linked to additional identifiers such as the BIC and ISIN numbers. Thus, the LEI serves as a linchpin between different data sources and helps for further standardization and harmonization of heterogeneous data during a data integration process.

LEIs would help improve the cross-border identification of European companies. Another interesting initiative as a data source for this use case could be the global registry of beneficial owners that provides transparency and quality.

SME general information:

General information covers SME business information and is the basic information for a CWA. Improving access to this information would reduce the time needed to gather information by SMEs to apply for financing. General information includes:

- Balance sheet and profit and loss statements (**P&Ls**) and sector activity (usually held by business registries). This is the traditional information used for CWA that for SMEs tends to have between 9 months and 1 year delay since the end of fiscal year, whereas large corporations where financial statements are audited and disclosed at an earlier stage;

[51] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information

[52] In accordance with Directive 2012/17/EU, the European Commission also maintains a registry of company information, including from SMEs, from national business registers. https://e-justice.europa.eu/489/EN/business_registers__search_for_a_company_in_the_eu

- Historical tax data (invoice tax held by the tax authority) help to improve the prediction performance of the CWA, providing early indicators of the balance sheet and P&L, such as value added tax (**VAT**);
- Social security data such as mandatory payments, arrears and number of employees that helps to improve the prediction performance;
- Public grants (held by national authorities) are regularly demanded by authorities when European funds are involved. Banks are requested to verify this information.

Financial behaviour:

SME PSD2 payment account transactions and balances with history held by banks and payment services providers and are freely available.

Online commercial activity:

The referred data, such as B2B activity, aggregated real time sales, inventory, customer satisfaction, cross border activity, wish lists, refunds, etc. would be accessible via ecommerce platforms that have to make it available.

These data would help to improve the CWA, such as for SMEs with a good sales trend, repeating customers, geographical diversification, customer satisfaction, etc. and, to innovate in financing products and services addressed to SMEs and possibly embedded in their activity, e.g., offering merchant cash advance.

Supply chain activity:

B2B activity such as purchase orders, invoice flows and financial reports. Accessible via supply chain platforms.

This data would help to improve the CWA, e.g., small providers with recurring sales to big buyers. These data also allow innovation in financing offering and help to make supply chains more robust by avoiding financing and cash flow problems.

Basic services:

Energy, water and communication suppliers' data are early indicators of an SMEs activity, e.g., in industries, an increase in electricity and water consumption indicates an increase in production and, possibly, future sales.

ERP/online accountability:

On premise sales, invoice flows and financial reports. Accessible via enterprise resource planning (**ERP**) platforms with prior SMEs' consent.

This data would help to improve the CWA, e.g., the accounting data are early non-consolidated information of the P&L of the company. Additionally, these data allow innovation such as financing invoices when they are issued.

Default behaviour:

Positive and negative behaviour held by credit bureaus. This data would help SME CWA since it helps identify default situations.

The use of the above-listed data may vary depending on the customer journey. The CWA can be embedded in different types of customer journeys, for example, open market, customer offering or as an event embedded in a supply chain. The type of data used in the CWA should be a trade-off between a good CWA and friendly customer experience.

11.3. The relevance of the use case for stakeholders and foreseeable impact of the use case

Using cross-sectoral data including online commercial activity will improve SME CWA and, consequently, SME financing.

The following aspects are relevant for SMEs and should also make it easier to apply for financing:

- Easier process for providing the required documentation for SMEs;
- Reduction of lead times[53] required to collect all the necessary information from SMEs, and reduction of lead times to analyse and respond to SME request;
- Loan request process homogenization among financial institutions
- In some cases, better financing options such as increased acceptance rates, risk selection, new financing products and lower interest rates due to a more accurate creditworthiness assessment;
- Making credit accessible to a broader and more inclusive pool of SMEs – facilitating access to SME activity data will also help the smallest SMEs to gather information required for CWA and should allow access to the same opportunities regardless of the size of the SMEs;
- Greater financing choices from different sources as well as promoting innovation of new products and services embedded in their digital activity, e.g. merchant cash advance, purchase order financing and other cash management solutions;
- Empowering SMEs to use or re-use their data (e.g. online sales activity) for own benefit, e.g. to access a broader range of products and services themselves.

The use case also has the following relevance for financial firms:

- Better credit risk assessment and, therefore, lower default rates and higher acceptance rates with more reliable and up-to-date sources of information;
- Better customer knowledge and holistic vision of SME activity;
- New business opportunities developing innovative products;

[53] Lead time refers to the amount of time that passes from the start of a process until its conclusion (e.g. CWA).

- Reduction of lead times and potentially costs to collect all necessary information from SMEs, and reduction of lead times to analyse and respond to SME requests.

Furthermore, the access to cross-sectoral data together with online commercial and public sector data (e.g. taxes) **will improve the sustainability and resilience of the financial system because it will**:

- Increase data quality and reliability;
- Facilitate a more up to date picture of SMEs' financial position since current analysis primarily relies on yearly SME financial reports; Balance sheet and profit and loss statements (P&Ls) (usually held by business registries). This information held by business registries can be delay up to 1 year after the termination of the previous fiscal year. Additionally, SMEs' annual accounts tend to be more volatile over short periods of time, so having an up-to-date picture is essential for SMEs CWA.
- Advance data standardization to make SME financial ratios used for CWA more comparable.

Moreover, this approach contributes to a more level playing field with a horizontal and cross-sectoral and customer centric deployment. Data access improvements will help SMEs in their CWA by enhancing their data which is often less accurate and not up-to-date compared to large companies. Additionally, digitally available cross-sectoral data will improve the CWA automatic processes that are widely used by SMEs.

Additionally, the use of cross-sectoral data allows new solutions and innovation in financing and novel customer journeys:

- Working capital financing such as merchant cash advance, PO financing, factoring, etc.;
- Payment solutions such as financial advisory tools that help to indicate the best suited payment related services to boost SMEs' commercial activity;
- Cash management solutions;
- Insurance and warranties based on commodities and operations throughout the supply chain allow real time and agile online solutions.

11.4. Broader policy objectives and KPIs that should be considered in relation to the use case

The broader policy objectives of the use case include:

- Promotion of digital transformation and innovation through the creation of digital processes to access, use and re-use SME data available in different sectors;
- Financially empowering and strengthening individual SMEs helps to strengthen the entire use case ecosystem;
- Promoting Capital Markets Union[54] by adopting common open finance standards;

[54] European Commission's plan to create a single market for capital.

- Improving consumer access to finance according to the Capital Market Union principles[55];
- Making credit accessible to a broader and more inclusive pool of SMEs.

The following business case KPIs were indicated in the use case:

- Increase in data collected
- Innovation in SME lending
- Increase in SME volume of loans
- Identifying financial exposure of SMEs[56] based on the residence of the obligor. Such data is currently published by ECB, Supervisory Banking Statistics.[57]
- Volume of loans to non-financial corporations should be assessed based on the defined tranches:
    - Up to EUR 250 000
    - Over EUR 250 000 and up to 1 000 000
    - Over EUR 1 000 000

  Such data is currently published by ECB, Statistical Data Warehouse.[58]
- Solvency risk improvement

11.5. Analysis whether the relevant data is already stored and by whom

Required data are stored by a varied number of entities, both public and private.

For the use case to capture its full potential, it would be necessary to have a full picture of the use case within the cross-border context by identifying storing of relevant data across the EU. The following table refers to Spain.

[55] As outlined in the five-year Capital Market Union action plan published by the European Commission on 24 September 2020.

[56] The risk that is inherent in providing financing to the particular SME.

[57] ECB's Supervisory Banking Statistics are based on aggregated supervisory banking data considered at the highest level of consolidation and which covers EU countries participating in the Single Supervisory Mechanism (SSM). In relation to financial exposure, the Supervisory Banking Statistics publishes exposure values of SMEs. More information may be found here: https://www.bankingsupervision.europa.eu/banking/statistics/html/index.en.html.

[58] More information may be found here: https://sdw.ecb.europa.eu/reports.do?node=1000002885.

Short term credit & loan application	**Data elements needed**	**Data Holder**
SME identification (KYB)	SME identity verification and information on group structure	Business registry
	SME and attorney identifiers and power of attorney	Business registry
SME general information	Tax historical data	Tax authority
	Social security data	Social security providers
	Balance sheet and P&L (company and group turnover, sector in which it operates, assets, financial results, etc.)	Business registry
	Public grants (not public financing)	National authorities
Financial behaviour (PSD2 banking data)	SME payment account transactions and balances with history	Banks and other account servicing payment service providers
Online commercial activity	Aggregated (non-personal) real time sales, inventory, customer satisfaction, wish lists, refunds, customer distribution (B2B-B2C anonymised data), cross border activity	E-commerce platforms
Supply chain activity	Information on buyer and suppliers: purchase orders, invoice flows and financial reports	Supply chain platforms
Basic services (utilities)	Energy, water and communication supplies data	Utilities companies
ERP/ online accountability	Information on buyer and suppliers: invoice flows and financial reports	SMEs on their infrastructure/ ERP online accountability in cloud storage
Default behaviour	Positive default behaviour (data from banks, telecommunications, utilities and real estate companies, etc.)	Bureaus
	Negative default behaviour (data from banks, telecommunications, utilities and real estate companies, etc.)	Bureaus

11.6. Overview of existing access to data via regulatory requirements and/or contractual arrangements

Short term credit & loan application	**Data elements needed**	**Data accessibility & availability**
SME identification (KYB)	SME identity verification and information on group structure	• Public data • Contract between Data User and Data Broker Other methods including access through APIs
	SME and attorney identifiers and power of attorney	• Public data • Contract between Data User and Data Broker • Other methods including access through APIs
SME general information	Tax historical data	• Private data provided with SME's consent • Agreement between SME and Data User • Web access
	Social security data	• Private data provided with SME's consent • Agreement between SME and Data User • Provision of data on paper/ via digital access (online)
	Balance sheet and P&L (company and group turnover, sector in which it operates, assets, financial results, etc.)	• Public data provided with SME's consent • Agreement between SME and Data User
	Public grants (not public financing)	Public data
Financial behaviour (PSD2 banking data)	SME payment account transactions and balances with history	• Private data provided with SME's consent • PSD2 legal obligation • Data accessible through APIs
Online commercial activity	Aggregated (non-personal) real time sales, inventory, customer satisfaction, wish lists, refunds, customer distribution (B2B-B2C anonymised data), cross border activity	• Contract between Data Holder and Data User • If Data Holder is a gate keeper, access is granted by the Digital Markets Act
Supply chain activity	Information on buyer and suppliers: purchase orders, invoice flows and financial reports	Contract between Data Holder and Data User
Basic services (utilities)	Energy, water and communication supplies data	• Contract between Data Holder and Data User • Contract between Data Holder and SME

ERP/ online accountability	Information on buyer and suppliers: invoice flows and financial reports	• Contract between Data Holder and Data User • Contract between Data Holder and SME
Default behaviour	Positive default behaviour (data from banks, telecommunications, utilities and real estate companies, etc.)	• Private data provided with SME's consent • Consent agreement between Data Holder and Data User
	Negative default behaviour (data from banks, telecommunications, utilities and real estate companies, etc.)	• Private data provided with SME's consent • Consent agreement between Data Holder and Data User

All the data listed above is digitalised and, therefore, available via API solutions or accessible via file transferring.

11.7. Current level of data standardization within the market and further steps for harmonizing data formats and access conditions (to ensure that data sets are of needed quality)

11.7.1. Technical accessibility of different types of data within the use case

SME identification data:

Depending on the data source, data can be available via an API or via web with a machine-readable format.

Business registries in the EU member countries must be made publicly available in accordance with the Open Data Directive. Unfortunately, there is no consistent implementation of the Open Data Directive among all of the countries. Some registries keep the entire data behind a pay wall (e.g., Spain), others provide just some basic information and for additional documents there is a fee (e.g., Italy). In some other cases, all data are available free of charge (e.g., Belgium, Bulgaria) and some of the registries provide an API free of charge (e.g., Ireland).

SME general information: Taxes are accessible via web, social security data are accessible via web and paper, P&L and financial statement are generally accessible via an API directly from relevant data providers or via web request from the public registry. Information on grants is accessible via web.

Financial behaviour: This information is currently accessible via PSD2 APIs.

Supply chain activity: Supply chain activity data is not standardised but initiatives such as Open Contracting[59] provide a standard/ define a common data model (Open Contracting Data Standard) for disclosure of data and documents used during the contracting process.

[59] https://www.open-contracting.org/.

Online commercial activity, basic services and ERP/ online accountability: The data is currently available only through an agreement between Data Holders and Data Users. Some of these data are accessible via an API. However, there is no open access that would allow SMEs to share their data with Data Users for the purpose of improving their financial choices.

Default behaviour: This information is already available via APIs (in Spain only negative data bureau is available).

11.7.2. Challenges to technical accessibility and standardization of relevant data

Some of the identified challenges include:

- SME cross-border identification;
- API access to public data;
- SME access to the data generated by their sales activity and held by platforms;
- Cross-border data standardization;
- Unstructured contract data (usually available as pdf files) are difficult to be processed in a fully automated way;
- Lack of a unified definition and implementation of standards for high-quality data;
- Data linkage, integration, and consolidation among all different, heterogenous data sources.

11.7.3. Existing data standardization

Short term credit & loan application	**Data elements needed**	**Data use & standards**
SME identification (KYB)	SME identity verification and information on group structure	Key data are standardised by country but differ cross boarder
	SME and attorney identifiers and power of attorney	Key data are standardised by country but differ cross border. Use of machine-readable format
SME general information	Tax historical data	Generally, data are standardised by country (VAT standardized cross border/ corporate tax does not standardize cross border)
	Social security data	Data are standardised by country (not structured)
	Balance sheet and P&L (company and group turnover, sector in which it operates, assets, financial results, etc.)	Key data are standardised but formats differ
	Public grants (not public financing)	Key data are standardised by country. European grants are standardized but grant formats differ

Financial behaviour (PSD2 banking data)	Payment account transactions and balances with history	Private data is provided according to the PSD2 standards. Structured data
Online commercial activity	Aggregated (non-personal) real time sales, inventory, customer satisfaction, wish lists, refunds, customer distribution (B2B-B2C anonymised data), cross border activity	Not standardised
Supply chain activity	Information on buyer and suppliers: purchase orders, invoice flows and financial reports	Not standardised
Basic services (utilities)	Energy, water and communication supplies data	Not standardised
ERP/ online accountability	Information on buyer and suppliers: invoice flows and financial reports	Not standardised
Default behaviour	Positive default behaviour (data from banks, telecommunication, utilities and real estate companies, etc.)	Key data are standardised but formats differ (cross boarder)
	Negative default behaviour (data from banks, telecommunications, utilities and real estate companies, etc.)	Key data are standardised but formats differ

11.8. Data protection framework

Almost all the data indicated within the use case are SME data (legal entities) to which the GDPR does not apply as it regulates only information relating to an identified or identifiable natural person. Where personal data is used, it is limited to data related to SME's attorney/ representatives and, to the extent required, the personal data used during the KYB process. The use case does not include data from employees or other natural persons related to the SME.

The use case includes data coming from e-commerce activity where sales should be considered at aggregated level and anonymised. In line with Recital 26 of the GDPR, the regulation does not concern the processing of personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The following table outlines the relevant data elements used within the use case.

Short term credit & loan application	**Data elements needed**	**Data Protection**
SME identification (KYB)	SME identity verification and information on group structure	Public data
	SME and attorney identifiers and power of attorney	Public data
SME general information	Tax historical data	Private SME data
	Social security data	Private SME data
	Balance sheet and P&L (company and group turnover, sector in which it operates, assets, financial results, etc.)	Public SME data Private data that may be subject to sui generis database right[60]
	Public grants (not public financing)	Public data
Financial behaviour (PSD2 banking data)	SME payment account transactions and balances with history	Access covered by the PSD2 (accessibility as an AISP). Bank secrecy laws apply
Online commercial activity	Aggregated (non-personal) real time sales, inventory, customer satisfaction, wish lists, refunds, customer distribution (B2B-B2C anonymised data), cross border activity	Private data
Supply chain activity	Information on buyer and suppliers: purchase orders, invoice flows and financial reports	Private data
Basic services (utilities)	Energy, water and communication supplies data	Private data
ERP/ online accountability	Information on buyer and suppliers: invoice flows and financial reports	Private data
Default behaviour[61]	Positive default behaviour (data from banks, telecommunications, utilities and real estate companies, etc.)	Private data
	Negative default behaviour (data from banks, telecommunications, utilities and real estate companies, etc.)	Private data

[60] Where applicable, the sui generis database right protects the content of database by preventing the extraction and/or reuse of the whole or a substantial part of the database's content.

[61] Please note that such private data may nonetheless be held by a public body/database (e.g. in Spain by the Bank of Spain with customer consent required to access the relevant database).

11.9. The nature of the relevant data

Regarding the nature of data, with the exception of the personal data used in the KYB process, the rest are all non-personal data. There are two main types of data within the use case:

- Public data such as the public registry data or public grants;
- Private data such as taxes held by public bodies or accountancy by private entities. SME consent is needed to access private data and bank secrecy applies in the case of financial data.

The following data formats have been identified within the use case:

- **SME identification**: Use of public data where some information is structured (e.g. tax ID, address, etc.) and some non-structured (e.g. public power of attorney.
- **SME general information**: Some information is public (e.g. the P&L and grants) while other is private (e.g. SME taxes). There is also both structured (e.g. taxes) and non-structured data (e.g. data from financial statements).
- **Financial behaviour**: Private and structured data.
- **Ecommerce activity, supply chain activity, basic services and ERP/ online accountability**: Private information. Data formats vary and may include unstructured data.
- **Bureau data**: Private and structured data.

11.10. Issues related to the costs of making data available

Given the diverse sources of data within the use case (government, platforms, credit agencies, etc.), several there are different commercial models to access the data:

a. Free of charge with SME consent when customer identifies himself (e.g. by using a digital certificate) or when SME consents to Data Users to access their tax data;
b. Free access when accessing payment accounts transaction and balance data (as established within the PSD2 regulation);
c. Fee access, set by contract between Data Holders and Data Users, when accessing data (for example, or business registry in Spain).

It is also noted that for a commercial model to be viable, it is important to identify all the costs incurred in making data available with quality (structured digital data, robust and governed data) and the necessary infrastructure to provide proper access.

Some of the existing data access costs are identified below:

- **SME identification**: Business registries in EU member countries must be made publicly available in accordance with the Open Data Directive. However, as further detailed in Section 12.8.1. above, directive's implementation is inconsistent which affects the data access costs. Therefore, cost of access may be the following: all of the data kept behind a pay wall (e.g., Spain), basic information provided free of charge with a fee for

additional data (e.g., Italy), all of the data available free of charge (e.g., Belgium, Bulgaria) or provision of an API access to the registry free of charge (e.g., Ireland).

- **SME general information**: Some information is free of charge (e.g. taxes) and some accessible by paying a fee to the relevant public registry or data provider.
- **Financial behaviour**: Free access in accordance with the PSD2 requirements.
- **Ecommerce activity, supply chain activity, basic services and ERP/ online accountability**: Access via commercial model set up in a contract between the data holder and the data user with SME consent.
- **Bureau data**: Access via commercial model set up in a contract between the data holder and the data user with SME consent.

11.11. Possible liability issues that would need to be addressed within the use case

Data sharing legal framework can be mandatory as established within the PSD2, regulated or because of an agreement between the parties:

- SME identification: Within the European context governed by the AMLD and Directive 2018/1673[62] and local implementing laws (e.g. in Spain governed by the Law 10/2010).[63]
- SME general information:
    - Taxes: Liability issues established within the agreement between the SME and the Data User. E.g. in Spain governed by the Law 2/2011 on Sustainable Economy.[64]
    - Balances and P&L: Some of the liability issues addressed within the Database Directive and local (implementing) laws (e.g. in Spain within the Law 2/2011 on Sustainable Economy).
    - Public grants: Some of the liability issues addressed within the public grant requirements and the Database Directive and local (implementing) laws. E.g. in Spain governed by the Law 2/2011 on Sustainable Economy.
- Financial information: Access to information is regulated by the PSD2.
- Ecommerce activity, supply chain activity, basic services, ERP/ online accountability and bureaus: Governed by the contract between Data Holders and Data Users with SME consent.

The European Digital Identity (e-IDAS)[65] should contribute to making use case deployment more robust as it will help to better identify and manage data sharing.

[62] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.

[63] Law 10/2010 of 28 April on the Prevention of Money Laundering and Terrorist Financing.

[64] Law 2/2011 of 4 March on Sustainable Economy.

[65] As established within the Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

12. Open investment data and financial advisory use case

12.1 The purpose of the use case and the problems it intends to address

The purpose of the use case is to make relevant individual customers' data available to financial institutions and, by taking into consideration additional relevant parameters, to facilitate provision of high-quality financial advice to these customers.

The first step (**Phase 1** below), will examine the possibility to elaborate a complete and in-depth customer profile by financial institutions, based on their access to customer data within the public sector and upon customers' request. This data could include the individual customers' social benefits / social security, tax payments, pensions and data from land registry offices.

When having access to such data, financial institutions could achieve better portfolio analysis results for individual customers' portfolios and, thus, enhance their offers to individual customers through a retirement planning advice that is more personalized, tailored to specific customer needs and supports long-term savings. Additionally, financial institutions' advice on investment planning and its suitability to meet individual customers' needs could increase customer's awareness and strengthen financial literacy.

12.2 Summary of the use case

The conditions for opening the described public sector data shall be examined. It shall be looked at examples outlining whether an API or APIs could give financial institutions access to certain individual customers' standardized data held by the public sector within the national states in the EU (social security, tax authorities and land registry offices), to achieve the use case' objectives.

The use case deliverables for Phase 1:

1. Describe the use case
2. Identify data sets
3. Detail customer journeys and related business requirements

12.1.1 Key actors within the use case

The following actors have been identified as relevant for the use case:

- **Data Subject:** Retail customers of financial institutions (credit institutions/asset managers/investment firms/insurance companies);
- **Data Property Rights Owner:** Public bodies;
- **Data Holder:** Financial institutions (credit institutions/asset managers/investment firms/insurance companies) and public bodies (Social Security, Tax authorities, Public land registry)

- **Data Intermediary:** Data aggregation companies or a dedicated trustworthy platform for the common good, avoiding a multiplication of commercial platforms that could add another layer of costs, and potentially offering room for misusing the system
- **Data Broker:** N/A
- **Data User:** Financial institutions (credit institutions/asset managers/investment firms/insurance companies), wealthtechs, robo-advisors.

12.1.2 Type of data considered within the use case

The so far identified customer journeys and involved data sets for Phase 1, based on key actors listed above:

Open investment data and financial advisory	Data elements needed	Data				
		Owner	Holder	Interm.	Broker	User
Advisory						
General information in relation to advisory (public data)	Public pension and social security	Public sector or private individuals	Public sector	N/A	N/A	Financial institution
	Tax	Public sector or private individuals	Public sector	N/A	N/A	Financial institution
	Real Estate Data / confirmation of ownership	Land registry office or private individuals	Land registry office	N/A	N/A	Financial institution
	Real Estate Data / valuation of ownership	Real estate broker / notaries chamber or private individuals	Real estate broker / notaries chamber	N/A	N/A	Financial institution
Customer Identification						
	Personal Identification Number	Private individuals	Public sector	N/A	N/A	Financial institution
During lifetime						
Changes in applicable law	Changes in public sector (eg tax, legal, etc.) data impacting customers' profiles and therefore impacting advisory	Private individuals	Public sector	N/A	N/A	Financial institution
Administration / back end						
Change in terms and conditions	Changes in public sector (eg tax, legal, etc.) data impacting customers' profiles and therefore impacting advisory	Private individuals	Public sector	N/A	N/A	Financial institution
	Changes due to termination	Private individuals	Public sector	N/A	N/A	Financial institution

12.2 Relevance of the use case for stakeholders

12.2.1 Benefits of the use case

The benefits of the described use case could be manifold:

- For individuals, profiting from increased transparency in financial advisory, to make necessary adjustments and ensure a sufficient economic foundation upon retirement.

- For financial institutions, enhancing their understanding of customers' needs and offers to individuals, leading to possible positive effects in financial results.
- In terms of national policy objectives, potentially enhancing circle of individuals benefitting from financial advisory services and lowering the future burden of public pension systems by increased private financial and retirement planning.
- In terms of EU policy objectives, supporting competition, facilitating development of innovative services in a level playing field for all participants in the financial ecosystem, including public sector data, fostering cross-sectorial data sharing and data-driven innovation, ensuring participation of more Data Holders and thereby exploring great potentials for standardization in data-sharing across the EU.

12.2.2 Negative effects of the use case

Possible negative effects of the outlined use case could be as follows:

- There is a risk of commodification of individuals and their personal data. Access to personal data might be misused by single market players ("gate keepers" as defined within the Digital Markets Act) for other purposes, by e.g. monetizing the data for purposes which had not been intended by or known to individuals, or recruiting individuals with apparently attractive offers which, however, might not correspond to their specific needs and investor profile. Nonetheless, the latter aspect could also come into effect at present since current market offerings to individuals are not based on complete individuals' profiles as part of the personal wealth data (e.g., available within the public sector) is not reflected in these.

- Another risk could consist in the use case not being taken-up due to individuals being afraid to lose control over their data and, therefore, not participating in this part of the financial ecosystem. This possible negative effect could however be solved through implementation of clear information and consent mechanisms.

- The lack of standardization and exchange rules could hamper the data sharing as outlined in the use case.

- The risk for financial institutions, notably banks, to possibly be obliged to bear the costs of required IT transformation for all included market players, especially in a possible further use case phase (please refer to Section 13.11. for description of Phase 2), as it has been the case when implementing the PSD2.

- Possible higher costs for public bodies to allow for structured data sharing and implementation of APIs.

- Unregulated entities might get access to individuals' data and misuse these, given the wider perimeter of the use case compared with financial institutions' offers today.

While not touched upon in the use case, it is important to highlight national and technological differences in pension systems as well as national differences in the advancements of elaboration of customer profiles that enable personalised advisory on private savings. Some of the data mentioned in the case is already partly accessible to financial firms, e.g., in Denmark

via the national solution PensionsInfo. Thus, national differences in access to customer data as well as fundamental differences in local pension systems, tax systems, etc. also highlight the importance and urgency to establish / enable national solutions, and potentially at a later stage connect it to wider European Union open finance framework' solutions, leveraging on a European Union open finance framework.

12.3 Overview of existing access to data via regulatory requirements and/or contractual arrangements and relevant legal issues

There is – to the involved experts' knowledge – no current EU-wide obligation for public bodies to share pension related data with third parties on the request of individuals. The access to public data of the individual customer that is relevant for the creation of an in-depth customer profile most likely varies from country to country. There are nevertheless initiatives and solutions at national level – for instance, in Denmark or in the Netherlands. In Denmark, there is a national solution (PensionInfo) where some of the relevant data to construct an in-depth customer profile (such as pension savings) is available and accessible to financial firms based upon customer request. To enrich the use case by ensuring access to publicly available data, additional arrangements would need to be done and relevant legal aspects would need to be analysed. Given the importance of the free movement of labour throughout Europe, it seems necessary to extend and align these initiatives to offer the same level of data access across the Union. In the understanding of the involved experts, a legal basis (i.e. a law) could be necessary to enable such sharing of data, especially since these data are generally being held by public bodies (in several, if not all, of the EU countries).

Another aspect with regards to data accessibility relates to financial assets being owned by individuals in partnerships. Personal data privacy would need to be guaranteed in cases where one of the individuals / asset holders gives consent or enters into a contract that triggers a consent mechanism which could possibly unintentionally reveal personal details to the other person in this relationship. Specifically, arrangements would need to be met for data access cases where one of the parties / individuals would want to keep secret from the other(s).

Existing technical solutions to make the data available

In Denmark, the Danish National Pension Tracking Services "PensionsInfo" gives an online overview of pensions' savings and allows the individual to send their pension information (digitally) from the tracking service to a pension provider or to a pension broker. This national technical solution / data hub can be complemented with the public data mentioned in this use case.

However, due to the significantly different pension systems, tax systems, etc. in each country, it is stressed that a national technical solution should be prioritized for this use case to ensure achieving its goals. The relevant data can be made available via an API by public bodies, subject to an identification (e-ID for instance) and a consent mechanism. Given the difficulty to standardize data between countries, one may imagine that data points differ slightly, based on local specificities.

12.4 Current level of data standardisation within the market and further steps for harmonising data formats and access conditions (to ensure that data sets are of needed quality)

The public data are to a great extent standardized on the national level, but currently are not entirely readily accessible from a technical perspective. However, a common national standard on data should be formulated to ensure that all available data are standardized.

Initiatives to pre-align needed data formats on the EU level would significantly ease later possible EU level standardization.

12.5 Data protection framework

Enforcement of the GDPR could be a potential challenge and must be addressed meticulously in this case. However, as a rule, the individual financial institution should be responsible for ensuring consent by the involved individual before accessing and using his / her data from a national public data hub. Furthermore, it should also be the responsibility of the individual financial institution to ensure that there is a legal basis for using the data as well as upholding the individuals' rights in relation to the GDPR (access to data on pension accrued rights is usually strictly restricted due to personal data protection reasons). In some countries data subjects nevertheless have the possibility to consult their accrued rights on a dedicated portal. Such access is personal and credentials enabling such access shall not be shared with third parties.

In a similar way as established in the PSD2, one may imagine a regime enabling data subjects to grant third parties – i.e. financial institutions – the right to access their personal data based on a so-called technical "consent" mechanism. The processing consisting of sharing the data by the public body would be lawful based on a legal obligation to which the public body is subject[66] and the processing performed by the financial institution would be justified by the performance of a contract to which the Data Subject is party[67].

12.6 Issues related to the costs of making data available

To avoid excessive cost, establishing an access platform could be a sector approach (e.g. by financial institutions) based on payment of a fee to access and utilize the data.

A trustworthy third party either on national or European level could be put in place to ensure that data access is management at a European sovereign level and required data protection.

For data held by public bodies, a similar regime as the one laid down in Article 6 of the Open Data Directive could be envisaged:

[66] Article 6 (1) c) of the GDPR.
[67] Article 6 (1) b) of the GDPR.

Principles governing charging

1. *The re-use of documents shall be free of charge. However, the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed.*

2. *By way of exception, paragraph 1 shall not apply to the following:*

   (a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;
   (b) libraries, including university libraries, museums and archives;
   (c) public undertakings.

3. *Member States shall publish online a list of the public sector bodies referred to in point (a) of paragraph 2.*

4. *In the cases referred to in points (a) and (c) of paragraph 2, the total charges shall be calculated in accordance with objective, transparent and verifiable criteria. Such criteria shall be laid down by Member States.*

   The total income from supplying and allowing the re-use of documents over the appropriate accounting period shall not exceed the cost of their collection, production, reproduction, dissemination, and data storage, together with a reasonable return on investment, and — where applicable — the anonymisation of personal data and measures taken to protect commercially confidential information. Charges shall be calculated in accordance with the applicable accounting principles.

5. *Where charges are made by the public sector bodies referred to in point (b) of paragraph 2, the total income from supplying and allowing the re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, data storage, preservation and rights clearance and, where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information, together with a reasonable return on investment.*

   Charges shall be calculated in accordance with the accounting principles applicable to the public sector bodies involved.

6. *The re-use of the following shall be free of charge for the user:*

   (a) subject to Article 14(3), (4) and (5), the high-value datasets, as listed in accordance with paragraph 1 of that Article;
   (b) *research data referred to in point (c) of Article 1(1).*

12.7 KPIs that should be considered in relation to the use case

Business case and KPI's will be dependent upon national solutions to access public data due to the significantly different pension systems, tax systems, etc. in the individual EU countries. The ambition of the underlying use case is to improve financial advice to individual customers, increase customer satisfaction, increase wealth, etc.

Targeted KPI's could be:

- A set percentage of public data is provided and supported on the established access platform
- Number of financial institutions using the access platform
- Data traffic within the access platform
- Reduction in expected public spending
- Qualitative assessment of the financial / pension education and financial awareness of the population
- Deployment rate of the open finance solution
- Part of the investment is made in Environmental, Social and Governance (ESG) investments
- Cyber risk monitoring

As mentioned above, KPI's should be tailored to the national pension system and platform.

12.8 Possible liability issues that would need to be addressed within the use case

Most importantly, the enforcement of the GDPR and consumer consent must be addressed properly to ensure that any access to individual customer data is legally sound.

Further liability issues might arise from the contractual obligation between financial institution and customer.

12.9 Further work on the use case

Based upon Phase 1 results and findings, the use case could be expanded (Phase 2) to include data from financial institutions, such as security/custody accounts, etc.

In a second phase, a possibility to set up an API / APIs with access to certain customer securities' data held at financial institutions can be evaluated. Such API could potentially support several use cases by enabling the assessment of the customers' financial situation (e.g. pensions' savings in different financial institutions). Such an evaluation shall include a thorough risks-benefits analysis including all the following aspects:

- Customers – value proposition / value added vs. risk of data misuse and fraud, lack of secure access and transfer mechanisms for the sharing of data, standardization, data protection;
- Financial institutions – fair distribution of value and risks among all participants;
- The type of customers' data to be shared – product information, customer's balance information, customers' investment history / transaction data.

The second phase could be started, after completion of the first phase, and upon assignment.

Case study of "PensionsInfo.dk"

1. Overview of the Pensionsinfo.dk

The main characteristics of the platform:

- Developed and run by a private association (since 1999)
- All pension providers are connected
- An online 24/7 service – www.pensionsinfo.dk
- Personal pension information from all 3 pension pillars
- Online data delivery (within 60 seconds)
- One data standard for all pension providers
- Own access only - personal login with national log-in solution for all Danes
- No storage of pension data
- 2021 statistics of PensionsInfo:
  - 1 628 450 users out of the 5 800 000 Danish population
  - 5 179 355 log-ons
  - 20 557 911 times a pension provider delivered personal pension data to PensionsInfo

2. Sharing Data from PensionsInfo

The users' ability to share their data from PensionsInfo is one of two main purposes for the tracking services. The other is to give the user an overview of their pensions.

To share her/his personal data the user has to:

- Log on to the personal and secure part of the receiving company's website
- Single Sign On (SSO) from the company's website to PensionsInfo. In the SSO the company can indicate if the user just wants to send their personal information to the company
- The data collection from all the users pension providers are done (maximum 60 seconds)
- The user hits the button "Send my data to *the company*"
- The user's data (either in XML- or JSON format) is send through secure connections to the company
- On the pension tracking service the user session is ended and the browser is closed.

3. How is the data used?

The receiving companies have many different reasons for receiving personal pension data from their customers. For instance:

- Pension planning
- Optimizing of pension – e.g. do the user have dormant pension accounts that can be transferred to the users current account?
- General credit rating

- General financial advice
- Use the information to calculate pensions

In the Danish set-up there is no limit on the type of companies users can choose to send their data to. But it is very important for PensionsInfo that the companies and start-ups which receive data from PensionsInfo are very aware of the GDPR regulation and how to manage individual pension data in a secure way. Prior to connecting to the system, employees from PensionsInfo go through the set-up and the user journey together with the receiving company. However, it is the receiving company that has the full responsibility of the data it receives.

4. Receiving of data – fee

The annual cost of running and development of PensionsInfo is around 2 000 000 euros.

The members share of the cost depends on how many times they have delivered data to PensionsInfo. In 2022 it is expected that the cost will be around 10 cent per data delivery. On average, users have 4,5 different pension providers. The members that deliver data to PensionsInfo do not pay any extra for receiving data.

The fees for companies to connect to and receive data from PensionsInfo:

- One time entry fee to become a member of the association is 10 000 euros. It covers technical set-up, access to test facilities, support in the establishment phase;
- A yearly fee depends on the number of times a customer has send PensionsInfo to the receiving party

5. Technical set-up

The PensionsInfo system operates on an Azure platform (cloud computing platform). There is encryption of personal data in the databases.

Secure set-up from the API to all pension providers and data receivers include:

- HTTPS
- JSON Web Token (JWT)
- IP whitelisting

One standardized data format is used:

- All providers deliver data in the same format
- All providers receive data in the same format
- Data is validated

13. Energy, sustainability and climate data use case

13.1. The purpose of the use case and the problem it intends to address

The use case is based on the acquisition of energy efficiency, energy consumption and climate data to provide a range of financial services to consumers. The use case includes two levels of services depending on the amount and type of data provided:

- Service level 1: Supporting consumers in protecting the value of their property by meeting applicable regulatory requirements and helping to control their energy consumption.
    - Examples of services: Energy renovation loans for housing having energy efficiency class ratings E-G,[68] loans for replacement of oil-fired boilers.
- Service Level 2: Providing consumers with details about their carbon footprint and offering services/ products which aim to reduce their environmental impact.
    - Examples of services: green financing, green bonds,[69] insurance covers, providing comparison and recommendations for consumers regarding specific services/ products, etc.

13.2. Summary of the use case

The use case aims to support customers in reducing their energy consumption and carbon footprint as well as using related products/ services with environmental focus.[70]

Service Level 1:

Type of data used	Acquisition mode	Actors
Energy performance classes of Energy Performance Certificate (EPC)	Collection in branches	- Financial institution - Consumers
	External	- Financial institution - Public body in charge of relevant data collection - Intermediaries for specific services (aggregation or put in quality of data)

[68] According to the Energy Performance Certificate as regulated by the Directive 2010/31/EU of the European Parliament and of the Council of 19 May 2010 on the energy performance of buildings.

[69] Green loans and green bonds are types of financing that are used exclusively to fund projects with environmental objectives and that adhere to specific principles and standards set in applicable regulation.

[70] White cells within the table relate to the use of internal data and green cells to the use of external data (i.e. data acquired from other parties than the data holder itself).

Service Level 2:

Type of data used	Acquisition mode	Actors
Energy consumption indicators and related data	Estimation based on payments data (e.g. amounts spent to pay energy suppliers) held by financial institution providing the service/ product	- Financial institution - Consumers
	Estimation based on payments data held by a third-party financial institution	- Financial institutions - Consumers
	External (non-payment data)	- Financial institution - Utilities suppliers - Consumers
Transports (use of and remuneration to transport providers (e.g. trains, airlines))	Estimation based on payments data held by financial institution providing the service/ product	- Financial institution - Consumers
	Estimation based on payments data held by a third-party financial institution	- Financial institutions - Consumers
	External (non-payment data)	- Financial institution - Transport companies - Consumers
Gas & fuel conversion factors (litres -> $KgCO^2$)	External	- Financial institution - Public body

13.3. The relevance of the use case for stakeholders

Relevance for consumers:

- Maintain the value of their property;
- Reduce expenses and save money through reduced energy consumption;
- Improving/reducing their carbon footprint.

Relevance for financial institutions

- Helping to establish and/or adhering to existing corporate social responsibility (CSR)[71] policies within the financial institution;
- Mitigating the solvency risk of households in fuel poverty;
- Commercial development (products and services proposals)

13.4. Broader policy objectives and KPIs that should be considered in relation to the use case

The broader policy objectives of the use include:

[71] CSR refers to company goals and policies through which they integrate certain social and environmental concerns in their business operations.

- Contribution to development of data driven innovation which is identified as one of the priorities of the Digital Finance Strategy for the EU (24/09/2020);
- Contributing to EU environmental transition, the building renovation plan and the wide use of EPC data through the single EU repository "building stock observatory" (as provided in the recast of the Energy Performance of Building Directive).

The following business case KPIs were indicated in the use case:

- Increase in collected data;
- Number of product & services signed by consumers;
- Consumer solvency risk improvement;
- Contribution to fighting climate change;
- Increase of consumer satisfaction/ loyalty.

13.5. Overview of existing data access via regulatory requirements and/or contractual arrangements and existing technical solutions to make the data available

Service Level 1:

Type of data used	Acquisition mode	Accessibility	Technical solution
EPC's energy performance classes	Collection in branches	- Collection is integrated into the mortgage granting process (as supporting documents) - It is planned to acquire this data in other customer's journeys (e.g. during meetings to discuss possible savings solutions, etc.), including operations initiated at the customer's own initiative through internet banking/ banking application ("self-care").	- Manual collection
	External	- Public body: open licence - Data provider: contract - The recast of the Energy Performance of Buildings Directive (EPBD) could improve accessibility of data (EU data base and new rules on interoperability and access to data)	- No specific technical solution: structured data delivered on a file

Service Level 2:

Type of data used	Acquisition mode	Accessibility	Technical solution
Energy consumption	Estimation based on payments data held by financial institution providing the service/ product	- Consumer consent	-Data already held by the relevant financial institution
	Estimation based on payments data held by third party financial institution	- Consumer consent	- PSD2 API
	External (non-payment data)	- Contract and consumer consent - The Data Act proposal could improve IoT data access (e.g. connected house)	- No specific technical solution at this stage (potential use of API in the future)
Transports	Estimation based on payments data hold by financial institution providing the service/ product	- Consumer consent	- Data already held by the relevant financial institution
	Estimation based on payments data hold by a third-party financial institution	- Consumer consent	- PSD2 API
	External (non-payment data)	- Contract and consumer consent - The Data Act proposal could improve IoT data access (e.g. connected vehicles, smart cities…)	- No specific technical solution at this stage (potential use of API in the future)
Gas & fuel conversion factors (litres -> KgCO2)	External	- Public Data	- No specific technical solution at this stage (potential use of API in the future)

13.6. Current level of data standardisation within the market, applicable data protection framework and issues related to the costs of making data available

Service Level 1:

Type of data used	Acquisition mode	Data used & standard	Data protection	Commercial model
EPC's energy performance classes	Collection in branches	- Manual entry of performance classes in the IT system	- GDPR and ePrivacy Directive	- Costs: Collection cost borne by financial institution - Benefits: Service not charged to consumers. Benefits come from profit margin on services and increased customer satisfaction and loyalty.
	External	- Data could be standardised or not depending on the data holder - At this stage transfers via APIs are not used	- Non-personal data	- Costs: Usually data are freely available. Some optional services could be paid (data quality (e.g. structuring), data aggregation from different sources…). - Benefits: Service not charged to consumers. Benefits come from profit margin on services and increased customer satisfaction and loyalty.

Service Level 2:

Type of data used	Acquisition mode	Data used & standard	Data protection	Commercial model
Energy consumption / Transports	Estimation based on payments data held by financial institution providing the service/ product	- Already in IT system	- GDPR	- Costs: Free access - Benefits: Service not charged to consumers. Benefits come from profit margin on services and increased customer satisfaction and loyalty.
	Estimation based on payments data held by a third-party financial institution	- PSD2 API standards	- PSD2 (accessibility as AISP) - GDPR	- Costs: Free access - Benefits: Service not charged to consumers. Benefits comes from profit margin on services and increased customer satisfaction and loyalty.
	External (non-payment data)	- Not standardized	- Private data under GDPR right of portability requested by consumer	- Costs: Free portability - Benefits: Service not charged to consumers. Benefits come from profit margin on services and increased customer satisfaction and loyalty.
Gas & fuel conversion factors (litres -> KgCO2)	External	- Standardized	- Public Data	- Costs: Free access - Benefits: Service not charged to consumers. Benefits come from profit margin on services and increased customer satisfaction and loyalty.

13.7. Possible liability issues that would need to be addressed within the use case

Liability issues were not discussed. Specific liability situations would need to be identified to identify possible liability issues.

14. Sharing of in-vehicle data use case

14.1. The purpose of the use case and the problems it intends to address

The purpose of this use case is to develop a vehicle data sharing framework so that insurers, among other stakeholders, can offer innovative products, motivate prevention of damages, help improve road safety and eco-friendly mobility and stimulate the successful development and uptake of connected, and later possibly automated and autonomous cars.

To that end, the use case seeks to address the issue of access by insurers to the data generated by vehicles. The use case also has a greater societal purpose by allowing access to aggregated driving data that can be used to improve traffic safety (e.g. insight into areas of heavy traffic) or incentives to make environmental-friendly choices (e.g. leaving car at home when air pollution is especially bad or choosing more eco-friendly routes). Thus, this case also seeks to address societal issues around increased road traffic and improving road safety.

14.2. Summary of the use case

Vehicles generate more and more data which can be used by insurers to offer a range of new products and services, as well as finetuning existing pricing, products and services. In-vehicle data can also enable insurers to better understand emerging risks, such as those related to automated and autonomous cars, or cyber risks for connected cars.

Insurers therefore need access to real time data, including:

- **Usage data** (driving and vehicle status and events) to be able to provide new or easy services including preventive measures and products such as customer onboarding, usage-based insurance and the handling of claims based on use of assisted and automated driving functions.

- **Accident data** (DSSAD and EDR/contextual)[72] to help provide, for example, assistance if required for the customer, deliver immediate services to the customer, claims management and to clarify the causation of accidents, and to better understand any potential (new) risks associated with automated and autonomous driving.

At this stage, vehicle manufacturers (VMs) act as gatekeepers of in-vehicle data. In fact, the solutions promoted by vehicle manufacturers enable them to control the volume, cost and quality of the data they make available. They also control which provider has access to the vehicle data, thus limiting the free choice of provider for the customer.

Concretely, this means that consumers have very limited power to decide who can access their vehicle data and for what purpose, and that insurers cannot access the data without having to go through the vehicle manufacturers' server or connecting via other devices, e.g. dongles or app solutions.

[72] DSSAD/EDR: Data Storage System for Automated Driving/ Event Data Recorder

The use case would therefore focus on developing a framework to guarantee consumer choice as well as a level playing field for in-vehicle data sharing. Furthermore, the case should also focus on the societal benefit of accessing aggregated data on driving behaviour and accident data as input to improving traffic safety and environmental-friendly mobility choices.

14.3. Broader policy objectives that should be considered in relation to the use case

The use case would put customers in control of their data, which is a policy objective in its own right. Customers would be able decide who can access their vehicle data, and for what purpose. Customers would also benefit from a wider range of innovative products that respond better to their needs and preferences.

From a wider societal perspective, the use case can also contribute to other policy objectives such as reducing C02 emissions and improving traffic safely. On the former, with in-vehicle generated data, service providers, including insurers, could develop services that incentivize people to drive less and to drive in a way which reduces their emissions. On the latter, access to in-vehicle data provides important insights into overall road traffic trend thus significantly contributing to improving road/traffic safety.

The data could also be used to enable multimodal mobility and sharing concepts, i.e. the integrated use of several different forms of transport.

The use case would ensure transparency for customers and providers related to which in-vehicle-data are available.

The sharing of geolocation and severity of accidents would also be significant enabler to increase road safety across Europe e.g. related to improvement of infrastructure and understanding of vehicle risks for automated and autonomous vehicles.

Regarding possible negative impacts of the use case for consumers, financial exclusion is not a specific issue for this use case and products of this kind (like Tesla insurance) are already available in the market, and this use case would not bring anything new from a consumer's perspective. However this use case could also bring a risk of financial exclusion like other use cases already existing in the market – and there is a need to actively manage these risks.

Conversely, this use case might also bring the opposite, financial inclusion, like in the case of young drivers that today have to pay high price independently of how they drive. For instance, in Italy the positive impacts of insurance relying on vehicle data are already being seen, as both 'pay how- you-drive' and mileage-based products have been offered to customers since 2011. More and more tailor-made products are being offered based on driving styles, as well as awarding more favourable tariffs to lower-risk drivers. The claims frequency of vehicles equipped with telematics devices is significantly lower than that of vehicles without such technology. This is even more true for young drivers. Those who are aware that they are being monitored adopt a more careful driving style.

Having access to in-vehicle data would allow all market operators to compete on an equal footing. Third party service providers, such as insurers, would be able to offer innovative

products and services and contribute to road safety objectives, notably by incentivising safe driving and making clearer connections between driving behaviour, risk and pricing or product. It is however important that if customers receive advice on how to enhance their driving behaviour it should be on a voluntary basis, and in those cases where customers choose not to heed the advice, it should not have negative consequences, e.g. in case of a claim.

Insurers will also be able to understand new risks associated with automated and autonomous driving (i.e. the circumstances of an accident) which is a precondition to insure such new cars.

14.4. Broader policy objectives and KPIs that should be considered in relation to the use case

The business case should consider 3 topics: the financial equilibrium, the rate of deployment of the solution and the qualitative benefits for European citizens, society and businesses.

Firstly, with regards to financial equilibrium - cost related to implementing the solution - are minimal compared to the benefits this use case would bring for European citizens and society.

The business case and KPI's associated should focus on consumer protection to avoid possible negative repercussions of access to in-vehicle data. Furthermore, the KPI's should also focus on product innovation and availability of products that meet the needs of consumers, as well as societal benefits of improved insights into road traffic. Given the above, important KPIs could be:

- Consumer protection: possibility for the consumer to exercise their rights in relation to GDPR (could be measured by the number of times GPDR rights have been exercised).
- Product development: number of new insurance products developed as a result of access to in-vehicle data.
- Use of aggregated data to improve road safety: the extent to which insurance companies and public bodies access aggregated in-vehicle data to get an overview of current traffic trends, with the aim to introduce measures that improve road safety.

Secondly, the rate of deployment of connectivity should be targeted and tracked. For instance: % of vehicles in use which are connected; % of these connected vehicles whose data is accessible by the different stakeholders; % of existing data which are accessible to the stakeholders such as insurers (with the consent of the customer); % accessible in real-time.

Thirdly, the business case should also monitor qualitative benefits for Europe, its citizens and businesses.

One such benefit can be linked to vehicles with delegated driving. To proceed with a compensation in case of an accident, it is essential that the insurer can know the elements that establish whether the insured was the master of the vehicle (with the powers of control and direction that characterize this mastery) or, on the contrary, whether he had become a

simple user, without power of direction and control, and therefore not a driver. Access to the accident data at the time of the loss is therefore decisive for the insurer to know whether or not to compensate for bodily injury and property damage. The access to these elements must be direct. Otherwise, the insurer would have to file a summary judgment to obtain the accident data or wait for the authorities to send the reports, which can delay the start of the legal amicable compensation procedure between 6 months to 1 year.

For instance, in France, this delay in compensation and the foreseeable judicialisation run contrary to the Law n° 85-677 dated 5 July 1985 ("Badinter law") which aims at the amicable and rapid compensation of victims. To avoid such a delay, the French *Ordonnance* n° 2021-442 dated 14 April 2021 introduced some new rules on access to vehicle data. In accordance with Article L-1514-5 of the Transports Code introduced by this Ordonnance, in the event of a traffic accident, insurance companies are granted access to the data held in the system recording the driving delegation status with respect to the activation, de-activation or the control recovery of the automated driving system. The purpose of such access by insurance companies in the context of Article L-1514-5 of the Transports Code is the determination of the extent to which an indemnification is necessary to perform a given insurance contract, in accordance with the Badinter law. In this case, the consent of the data subject - driver or user of one of the vehicles involved - to the data processing is not necessary, given that processing is based on a legitimate interest.

In another field, public authorities want to use these means of communication to increase road safety and reduce pollution through the exchange of data between road users and road managers. In 2014, the European Commission launched the Cooperative Intelligent Transport Systems (C-ITS) deployment platform for this purpose.

14.5. Overview of existing access to data via regulatory requirements and/or contractual arrangements and relevant legal issues

At this stage, insurers do not have the legal framework necessary to access in-vehicle data on a fair, reasonable and non-discriminatory basis. There is currently no transparency about the data actually available to OEMs (per manufacturer and on vehicle model basis), a public catalogue of in-vehicle data would be necessary. Differences between the markets might exist in terms of data available.

Insurance based on direct access to in-vehicle data are therefore still rare and, when it exists (based on B2B arrangements between vehicle manufacturers and insurers) they tend to relate to limited sets of data. This means that the access provided to insurers does not enable insurers access to the data they need for the most advanced services that insurers seek to offer for connected vehicles.

This solution proposed in this use case would allow continuous, standardised access to in-vehicle data by the owner as well authorized persons, in line with all relevant data protection requirements. This data could be then anonymized and be made available for statistical evaluations. Society has a legitimate right to know how often autonomous systems are responsible for injuries to persons or damage to property. Mobility data, for example on traffic loads, could also be available in anonymized form.

Furthermore, easy access to data could substitute pricy and complex additional hardware features, e.g. dongles or other connecting boxes to the car. App or likewise features can today be used as a very insecure proxy for driving.

No legal obstacles have been identified at EU level.

14.6. Existing technical solutions to make the data available

There are multiple technical data sharing solutions. For instance, Secure-On-Board Telematics Platform (S-OTP) ensures independent applications to be safely and securely implemented in the vehicle to optimise in-vehicle data processing, whilst supporting decentralised communication to/from the vehicle with alternative service providers obtaining direct consumer consent. In particular, the S-OTP could:

- Ensure direct access to data, functions and resources by all authorised parties.
- Put consumers in full control to decide which service providers can access their data, without interference from vehicle manufacturers.
- Safeguard effective competition and non-monitoring of independent competing businesses by vehicle manufacturers.
- Enable innovative solutions and new business models.
- Ensure a high level of safety, security and data protection.

Beyond existing market solutions, another option would be the introduction of an independent data trustee which would allow for the implementation of broad business cases (especially with regards to accident data, automated driving data, vehicle inspection data) as it would make data available for providers and consumers.

Integration of mobile devices (e.g. Android Automotive, Apple Carplay) could also help integrate services in the vehicle providing a non-discriminatory access to the infotainment environment.

Table 1 below presents an analysis of the technical solutions to make data available, with their pros and cons.

Table 1 on principles of a balance ecosystem[73]:

Practical details / Principles	Extended vehicle server	So-called neutral server	Data marketplace server	Vehicle physical interface	On-board application platform
Data accessibility	Partial, remote, by manufacturer	Partial, remote, harmonised	Partial, remote, harmonised	Partial, direct vehicle, standardised	Direct vehicle, standardised
Consent	Intermediated, monetisation of personal data	Fluid	Intermediated, monetisation of personal data	Fluid	Fluid
Market asymmetry	Strong	Average	Average	Low	Low
Cost of data access*	Base cost + margin	Base cost	Base cost + margin	Base cost + equipment	Base cost
Real time access	Risk of latency	Risk of latency	Risk of latency	Yes	Yes
HMI integration	Low	No	No	No	Yes
Electronic Control Unit data	No, aggregated	No, aggregated	No, aggregated	Possible	Possible
Security and Cybersecurity**	Yes	Yes	Yes	Yes	Yes
Assessment	Unsatisfactory as is	Useful but not sufficient	Unsatisfactory as is	Necessary but not sufficient	To implement

14.7. Current level of data standardisation within the market and further steps for harmonising data formats and access conditions (to ensure that data sets are of needed quality)

There are very few examples of standardised data and those do not include all OEMs/vehicle brands or data points necessary to develop innovate services.

For example, the Connected Vehicle Systems Alliance (COVESA) in partnership with the World Wide Web Consortium (W3C) has produced vehicle signals standard and includes among its contributors BMW, Volvo Cars, Jaguar Land Rover, and Bosch. It has recently extended the data domain model to align with the data standard produced the Open Insurance Initiative (OPIN).[74]

While not all data and functions need to be standardised, a core set of mandated data points, provided in a highly standardised format, are required to enable the development of insurance multi-brand services, facilitating the establishment of scalable independent automotive services at a competitive price.

It must be decided which data points should be made available for statistical purposes at an aggregated level to serve the purpose of improving overall road traffic.

The framework should establish a baseline set of common datapoints, which could be further expanded in the future. Standardised APIs may need to be developed too.

[73] Connected vehicle: 8 principles for a balanced ecosystem accessible to everyone, Alliance Mobilité Connectée Pour Tous – Alliance Connected Mobility For Everyone.
[74] https://openinsurance.io/opin-covesa-data-alignment/.

Some data related to automated and autonomous driving are standardised either via United Nations Economic Commission for Europe (UNECE) regulations as well as in national legislation (e.g. German Road and French Traffic Acts for automated and autonomous vehicles)

14.8. Data protection framework

14.8.1. Enforcement of personal data, commercial data and intellectual property rights

Data subjects would have full control over the services used in their vehicle, over which services require access to what data and what services require access to the mobile communication resources of the vehicle. In accordance with General Data Protection Regulation (GDPR) requirements, vehicle owners and drivers would have the ability to opt in or opt out of data sharing agreements at any time exercise their rights, such as their right of access, rectification or erasure, and also profit from their data portability rights enshrined in Article 20 GDPR.

14.8.2. Application of the GDPR data principles (e.g. data minimisation, purpose limitation) and legal grounds for the processing (e.g. consent, contract)

Data subjects would be enabled to stop the collection of their personal data, temporarily or permanently, at any moment, unless there is a specific legal ground that the controller can rely on to continue the collection of specific data. Data controllers will be required to ensure that technologies deployed in the context of data collection are configured to respect the privacy of individuals by applying the obligations of data protection by design and by default as required by Article 25 GDPR.

14.8.3. Operational challenges to implement a state-of-the-art data governance framework

Attention must be made to the technical requirements to uphold differential data privacy (i.e. for the consumer to exercise their control over which services have access to their data). The solution must technically ensure that the data subjects can chose who should have access to their data. Furthermore, the technical solution must ensure that the data subject can exercise his/her rights, including the “right to be forgotten” (to the extent applicable), as well as get insights into the data the actors have access to and how this data has been used.

In any event, OEMs can only share data within the boundaries of the GDPR and if they have ownership or a license regarding the respective data (civil law perspective):

- In the event of a sharing of personal data, the OEMs must comply with the requirements of the GDPR, in particular they must have a lawfulness basis for the processing. Typically, that would be the consent of the concerned data subject without further restrictions defined by the OEM to “safeguard their customers”. However, depending on the respective scenario, it is also thinkable that an OEM can

share in-vehicle (personal) data based on a contract entered between the data subject and the OEM.[75]
- Alternatively, OEMs can share anonymized data (non-personal data) which is outside the scope of the GDPR.

14.9. Issues related to the costs of making data available

FRAND principles would not be enough to ensure fair contract conditions because, based on insurers' experience until now, the negotiations on contracts with car manufacturers would be lengthy and would not meet the objective of reasonable and proportionate fees. They would also put smaller insurers at a significant competitive disadvantage as they have little bargaining power compared to big vehicle manufacturers.

The framework should therefore include standard terms for data sharing contracts and define what cost elements may be recovered by fees, including a maximum fee for data/function access.

Excessive prices can definitely block the development of a sound data ecosystem. Therefore, an appropriate framework seems necessary.

The prices for data should not above after-market solutions e.g. crash sensors mounted to the windscreen.

New edge computing technologies and solutions will reduce network and storage costs on OEMs while allowing for more detailed, accurate and real time vehicle analytics.

14.10. Possible liability issues that would need to be addressed within the use case

Liability issues can be tackled in line with the following legal frameworks:

- Liability for errors caused by software malfunctions would be allocated in accordance with the Product Liability Directive and national tort law.
- Privacy infringements will be addressed according to GDPR and ePrivacy rules.
- Any solution that leads to cyber risks for connected vehicles could subsequently lead to liability for the parties involved.
- Attention must be made to cloned cars (and in particular VIN-number cloning) and what negative impact this can have on the driver owning the original car.
- Finally, it is also important that the use case considers the situations where the driver must identify him/herself upon driving the car (see also use case analysis table). While this is becoming a more common feature in newer cars, older cars do not have this technical possibility, hence this data point is only available for some cars but can have significant impacts on the car owner.

[75] As a reference, the European Data Protection Board has been addressing in detail the different data processing, including by insurance companies, involved in the context of connected vehicles and mobility related applications (Guidelines 01/2020 adopted on 9 March 2021).

14.11. References

The present use case analysis has been developed based *inter alia* on the following references:

- Open Insurance Initiative: open-insurance-discussion-paper-28-01-2021.pdf (europa.eu)
- E-privacy regulation: EUR-Lex - 32002L0058 - EN - EUR-Lex (europa.eu)
- OPIN/COVESA data standard alignment: OPIN-COVESA Data Alignment - Open Insurance
- European Commission Cooperative intelligent Transport Systems: Specifications for the provision of cooperative intelligent transport systems (C-ITS) (europa.eu)
- Connected vehicle: 8 principles for a balanced ecosystem accessible to everyone, Alliance Mobilité Connectée Pour Tous – Alliance Connected Mobility For Everyone.