EUROPEAN
COMMISSION

Brussels, 28.6.2023
COM(2023) 360 final

2023/0205 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554

(Text with EEA relevance)

{SEC(2023) 255 final} - {SWD(2023) 224 final} - {SWD(2023) 230 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

To be successful in a data driven economy that works for the people and businesses, Europe must strike a balance between the flow and wide use of data and preserving high privacy, security, safety and ethical standards. In the communication on a European strategy for data,[1] the Commission set out how the EU should create an attractive policy environment so that, by 2030, its share of the data economy at least corresponds to its economic weight.

In finance, the Commission identified the promotion of data-driven finance as one of the priorities in its 2020 digital finance strategy[2] and announced its intention to put forward a legislative proposal on a framework for financial data access. The 2021 Communication on a Capital Markets Union[3] confirmed the Commission's ambition to accelerate its work on promoting data-driven financial services. It announced the establishment of the Expert Group on the European Financial Data Space to provide input on a first set of use cases. More recently, Commission President von der Leyen confirmed in her 2022 State of the Union letter of intent that data access in financial services is among the key new initiatives for 2023.

Customers of the EU financial sector currently cannot efficiently control access and sharing of their data beyond payment accounts. Data users, i.e. firms that want to access customer data to provide innovative services, have problems accessing data held by data holders, i.e. financial institutions that collect, stores and process that customer data. As a result even where customers so wish, they do not have widespread access to data-driven financial services and financial products. A set of inter-related problems explain the limited access to data. First, in the absence of rules and tools to manage data sharing permissions, customers do not trust that potential risks of sharing data are addressed. Therefore, they are often reluctant to share their data. Second, even if they want to share data, the rules governing such sharing are either absent or unclear. As a result, data holders such as credit institutions, insurers and other financial institutions holding customer data are not always required to enable the access of data users, like for for example, FinTech companies, i.e. companies using technology to support or provide financial services, or financial institutions that provide financial services and develop financial products on the basis of data sharing to their data. Third, data sharing is made more costly as both the data itself and the technical infrastructure are not standardised and therefore differ significantly.

This proposal aims to address these problems by enabling consumers and firms to better control access to their financial data. This would make it possible for consumers and firms to

---

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 February 2020, A European strategy for data (COM (2020) 66 final).

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 29 September 2020, on a Digital Finance Strategy for the EU (COM/2020/591 final)

[3] 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 (COM/2021/720 final)

benefit from financial products and services that are tailored to their needs based on the data that is relevant to them, while avoiding the inherent risks.

The general objective of this proposal is to improve economic outcomes for financial services customers (consumers and businesses) and financial sector firms by promoting digital transformation and speed up adoption of data-driven business models in the EU financial sector. Once achieved, consumers which want to do so would be able to access personalised, data-driven products and services that may better fit their specific needs. Firms, notably SMEs, would enjoy wider access to financial products and services. Financial institutions would be able to take full advantage of digital transformation trends, while third-party service providers would enjoy new business opportunities in data-driven innovation. Consumers and firms will be given access to their financial data to enable data users to provide tailored financial products and services that better suit customers' and firms' needs.

The proposal does not entail administrative cost savings, as it is a new legislation not amending previous EU rules. For the same reason, this is also not an initiative included under the Commission's regulatory fitness and performance programme (REFIT) aimed to ensure that EU laws deliver on their objectives at a minimum cost for the benefit of citizens and businesses.

- **Consistency with existing policy provisions in the policy area**

This proposal builds on the revised Payment Services Directive (PSD2), which enabled the sharing of payments account data ('open banking'). This proposal enables the sharing of a broader set of financial services data and sets the rules according to which the sharing of the data is going to be achieved. It also sets out the rules applicable to the market participants who will engage in this activity.

- **Consistency with other Union policies**

This proposal respects the General Data Protection Regulation (GDPR) which sets the general rules on the processing of personal data related to a data subject and ensures the protection of personal data as well as the free movement of personal data.

This proposal also is a sectoral building block that fits into the broader European strategy for data and enables data sharing within the financial sector and with other sectors. It is based upon the key principles for data access and processing set out in the Commission's cross-sectoral initiatives. The Data Governance Act focuses on increasing trust in data sharing and improving seamless interconnection ('interoperability') between data spaces and creating a framework for data intermediation service providers. Another cross-sectoral initiative is the Digital Markets Act which establishes a number of data related obligations to tackle the power of gatekeeper platforms and ensure contestability in the digital markets by, for example, allowing financial institutions on behalf of their customers or when using gatekeeper core platform services to access data held by gatekeepers. Yet another cross-sectoral initiative is the proposal for a Data Act[4] that would establish new data access rights for the Internet of Things (IoT) data – i.e. the data that products obtain, generate or collect concerning their performance, use or environment – for both product users and providers of related services. It also establishes generally applicable obligations for data holders, which are required to make data available to data recipients under EU law or national legislation adopted in line with EU law.

[4] Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), COM/2022/68 final.

This proposal also complements the EU retail investment strategy[5]. It will support its objective to improve the functioning of the retail investor protection framework by providing safeguards in the use of retail investor data in financial services. Moreover, it ensures compliance with the rules on cybersecurity and operational resilience in the financial sector, as set out in the Digital Operational Resilience Act that entered into force on 16 January 2023.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The Treaty on the Functioning of the European Union (TFEU) confers on the EU institutions the power to set rules on Member States' approximation of laws that have as their objective the establishment and functioning of the internal market (Article 114 TFEU). This includes the power to enact EU legislation to approximate requirements on the increasingly important use of data for financial institutions, as financial institutions active across borders would otherwise face diverging national requirements, rendering cross-border activity more costly. Creating common rules for data sharing in the financial sector will contribute to the functioning of the internal market. Common rules will ensure a harmonised regulatory framework on financial data governance, in line with the European strategy for data. These results will best be achieved by adopting a Regulation, which is directly applicable in Member States.

• Subsidiarity (for non-exclusive competence)

The data economy is an integral part of the internal market. Data flows form a core part of digital activities, and they mirror existing supply chains and collaborations between firms and consumers. Any initiative aiming to organise such data flows must apply to the internal market as a whole. As data holders are generally licensed financial institutions subject to broad and detailed set of rules largely set out in directly applicable regulations and supervisory arrangements for which convergence is ensured at EU level, action at EU level is needed to set common conditions and preserve a level playing field among financial institutions to safeguard market integrity, consumer protection and financial stability. Another reason for action at EU level is the high level of integration in the financial sector. Financial institutions also conduct significant cross-border activity.

The problems described in the impact assessment accompanying this proposal are common for all EU Member States. Regulating financial services is a power shared between the EU and its Member States. These problems cannot be solved by Member States acting alone, given that the holders and potential users of customer data in finance often operate across several Member States. Therefore, a customer may have data held by financial institutions in different Member States. To improve trust and allow the integrated use of those data all these financial institutions would need to be governed by the same legal framework and the same technical standards. Individual national rules would result in overlapping requirements and disproportionately high compliance costs for firms without being the most beneficial to firms and consumers.

---

[5] The retail investment strategy adopted includes the proposal for a Directive of the European Parliament and of the Council amending Directives (EU) 2009/65/EC, 2009/138/EC, 2011/61/EU, 2014/65/EU and (EU) 2016/97 as regards the Union retail investor protection rules and a proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 1286/2014 as regards the modernisation of the key information document.

- **Proportionality**

In line with the principle of proportionality, the proposal does not go beyond what is necessary to achieve its objectives. It only covers the aspects where the administrative burden and costs are proportionate to the objectives to be achieved. For example, proportionality is carefully designed in terms of scope and stringency. It is underpinned by qualitative and quantitative assessment criteria to ensure that the new rules will have a broad effect. Annex 5 to the accompanying impact assessment explains how proportionality has guided the selection of data sets. Annex 8 to the accompanying impact assessment explains the measures taken to ensure a proportionate impact on SMEs.

- **Choice of the instrument**

This proposal should take the form of a regulation, which is directly applicable in all Member States. This is to ensure that common rules apply across all Member States on the conditions for access to and handling of financial services customer data.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

This new proposal does not rely on any existing legislation. It builds on the open banking regime set up in Directive (EU) 2015/2366 but creates a new data access right for sets of data not previously covered by any other EU legislative framework.

- **Stakeholder consultations**

On 10 May 2022, the European Commission launched a call for evidence on financial data access. The call for evidence closed on 2 August 2022, gathering 79 responses. Persons responding in individual capacity expressed concerns about data sharing in the absence of a framework adopting clear safeguards, such as privacy dashboards, clear delineation of its scope and a level playing field among market participants. Firms were rather positive as long as proper safeguards were put in place. The call for evidence showed that if properly designed, access to financial data could have a positive impact.

On 10 May 2022, the European Commission also launched a joint public consultation on the review of the revised Payment Services Directive (PSD2) and financial data access. The public consultation closed on 2 August 2022. The responses on financial data access confirmed the views expressed in the call for evidence. While most of the general public who responded would want to share their data based on strong consumer consent/agreement, some concerns were expressed over sharing financial data. These concerns were based on a lack of trust over privacy, data protection and digital security issues and a general sense of not being in control how their data is used.

Professional stakeholders (corporate users, fintech firms, consumer organisations as well as relevant public authorities and national regulators) were more favourable to data sharing and mentioned benefits to the customer journey in terms of increased competition and innovation for financial products and services. A significant minority of professional respondents also voiced concerns over competition, security and data misuse.

On 10 May 2022, the Commission also launched a targeted consultation on financial data access and data sharing in the financial sector. The targeted consultation closed on 5 July 2022, gathering 94 responses from professional stakeholders.

The purpose of the targeted consultation was to gather their expert input in data sharing in finance. The professional stakeholders targeted included financial institutions, data vendors, fintechs, corporate users, consumer protection associations as well as relevant public authorities and national regulators). Overall, the responses highlighted that most professional respondents see the potential benefits of a legal framework for financial data access and therefore support regulatory intervention in some areas. However, responses to the targeted consultation suggest that stakeholders' views diverge substantially and support from consumers and data holders is conditional on how those data will be accessed and shared.

- **Collection and use of expertise**

On 24 October 2022, the Commission received a report on open finance from the Expert Group on the European Financial Data Space. The Expert Group brings together experts from academia, consumers, and industry (including banking, insurance, pensions, investment, as well as third-party providers and fintech firms). The report describes key components of an open finance ecosystem as seen by the Expert Group (data accessibility, data protection, data standardisation, liability, level playing field and the key actors) and sets out considerations on each element, while also presenting divergent views within the group. To illustrate the challenges and opportunities of open finance, the Expert Group has assessed several specific use cases which are detailed in the report. The use cases and the findings of the report were used to develop this proposal, particularly in determining the data covered within scope of the proposal.

- **Impact assessment**

The proposal is accompanied by an impact assessment, which was submitted to the Commission's Regulatory Scrutiny Board (RSB) on 3 February 2023 and approved on 3 March 2023. The RSB recommended improvements in some areas to strengthen the evidence base, put further emphasis on customer trust and protection of vulnerable consumers, as well as better define the limitations and uncertainties of the cost-benefit analysis for this proposal. The impact assessment was amended accordingly and addressed the RSB's more detailed comments.

Policy options have been chosen based on the Commission Expert Group on the European Financial Data Space and on stakeholder feedback.

Several options that were considered aimed at improving customer trust in data sharing, clarify the legal situation, promote standardisation and provide incentives. As regards customer trust, the options considered included the mandatory use of financial data access permission dashboards, setting rules on who can access customer data, and complementing those rules with other safeguards, including guidelines that protect the consumer against unfair treatment or exclusion risks.

To provide legal clarity, one option considered was the extent to which data holders could be required to share their customer data with data users. This could be done on a mandatory basis, subject to the customer request. The types of firms to be obliged to share data was also considered (credit institutions, payment service providers and other types of financial institutions across the entire financial sector).

Several options were considered to promote the standardisation of customer data and interfaces. One option was for market participants to jointly develop common standards for customer data and interfaces as part of financial data sharing schemes. Consideration was given as to whether market participants should be part of such a scheme on a voluntary or mandatory basis in order to access data. Another option was to develop such a scheme by

delegated or implementing acts (so-called Level II legislation that supplements or amends certain non-essential elements of basic acts).

A number of options were considered to implement high-quality interfaces for customer data sharing. One option could be for data holders to be required to put in place application programming interfaces (APIs) implementing the common standards for data and interfaces and make them available to data users without a contract and without being able to receive any compensation from data users for using these interfaces. Another option would be to allow reasonable compensation to set up and use the interfaces and agree on contractual liability.

The Commission considered that the preferred option is an EU Regulation that establishes a framework for financial data access, which includes the following characteristics:

- require market participants to provide customers with financial data access permission dashboards, set eligibility rules on access to customer data and empower the European supervisory authorities (ESAs) to issue guidelines to protect consumers against unfair treatment or exclusion risks;
- mandate access for data users to selected customer data sets across the financial sector, always subject to permission by the customers to whom the data relates to;
- require market participants to develop common standards for customer data and interfaces concerning data that are subject to mandatory access, as part of schemes; and
- require data holders to put in place APIs against compensation, implementing the common standards for customer data and interfaces developed as part of schemes and require scheme members to agree on contractual liability.

The expected overall economic impact of this proposal would be enhanced access to better-quality financial services, improving the overall price-quality relationship. Financial data access would result in more user-centric services: personalised services could benefit consumers seeking investment advice, and automated creditworthiness assessment can be expected to help facilitate access to finance for SMEs. The expected impact on the wider economy is positive due to more efficient service provision as a result of more effective competition. For these positive impacts to materialise, however, it is important to ensure that data reuse does not lead to anti-competitive behaviour and collusion, especially given the requirement for mandatory adherence to contractual schemes, and that data holders, in particular, do not foreclose competitors through high fees for accessing data.

The proposal can be expected to have an overall positive social impact provided that the associated risks are kept in check. Sharing of customer data would be controlled as it is subject to customer request – mandatory access would only be triggered once the customer has requested his or her data to be shared. More detailed data sharing could open up access to finance to previously excluded users. It could facilitate targeted savings and pensions by facilitating a comprehensive overview of private and occupational pension entitlements as well as other savings for retirement. On the other hand, without appropriate safeguards, more data use could, in specific cases, lead to a risk of higher cost or even further exclusion of customers with an unfavourable risk profile. Particular attention needs to be paid to services with inherent risk mutualisation, such as insurance. The preferred option would however mitigate any such impact since data sets which are directly relevant to essential financial services for consumers would be excluded from its scope and EBA and EIOPA guidelines on the applicable personal data use perimeters would constitute an additional safeguard.

Overall, financial data access can be expected to have a neutral to positive indirect impact on the environment, as it would likely support the uptake of innovative investment services, including those that channel investments towards more sustainable activities. Even though there could potentially be some negative implications from more intensive use of data centres that would go together with wider data reuse, these are likely to be limited in scope as most of the data covered by this proposal already exists in digital form. The additional processing volume would mainly come from data users accessing these data.

Given the limited data availability and the nature of this proposal, it is inherently difficult to make quantitative predictions about how it would benefit the economy as a whole. Likewise, it is equally challenging to disentangle the effects of each policy measure from the potential aggregate impact. Whilst the costs of each policy option are already challenging to estimate, its isolated benefits are even more difficult to gauge. An attempt was made to provide a macroeconomic assessment of the potential benefits based on a macro-level study, the aim of which however was not to quantify the benefits of this proposal explicitly. Thus, the range of figures presented below should be taken as an illustration of the potential benefits rather than a dedicated estimate. According to this macroeconomic assessment, the total annual benefits for the EU economy produced by enhanced access to and sharing of data in the EU financial sector ranges between EUR 4.6 billion and EUR 12.4 billion, including the direct impact on the EU financial data economy in the range of EUR 663 million to EUR 2 billion per year. The overall estimated cost of the proposal could be up to a range of EUR 2.2 billion to EUR 2.4 billion in one-off costs and between EUR 147 million to EUR 465 million in recurring annual costs.

Digital finance has many aspects that can improve the workings of economies and further the cause of sustainable development. Access to finance is one of the major challenges of sustainable development. While not the direct aim of the proposal, it will indirectly help advance inclusive and sustainable economic growth and employment. It can help socially excluded individuals gain better access to finance. This proposal is in line with building resilient infrastructure, sustainable industrialisation, and innovation. It can unleash competitive economic forces that improve connectivity in the area of finance. The proposal will also help address climate change through targeted investment advice, helping investors to make more informed decisions which can help to channel of capital flows towards sustainable investments.

- **Regulatory fitness and simplification**

This proposal will make it easier for data users to access customer financial data, thereby making it easier for customers to access innovative financial services. It will notably support SMEs and their access to finance. To mitigate any negative impact on SMEs as data holders, it includes several measures. For example, by introducing compensation for data access, smaller market participants would be allowed to recover costs incurred by the requirement to provide technical interfaces for data access (‘application programming interfaces‘). Moreover, SMEs acting as data holders could further reduce their implementation costs by developing joint interfaces or making use of external service providers. In addition, SMEs acting as data users will be able to access customer data against a reduced compensation, capped at cost, in line with Article 9(2) of the Data Act proposal. An option considered and rejected would be to exclude SMEs as data holders from the scope of the obligations to make data available. However, this option would have several disadvantages. It would considerably reduce the positive impact of the proposal, as some use cases rely on data from all financial institutions serving a particular customer and therefore holding their data to be pulled together. For example, use cases related to investment advice would only work efficiently if all relevant data on a customer’s assets and investments (whether they are held with smaller or larger

firms) are comprehensively available for access. Moreover, it would not be consistent with ensuring that all market participants abide by key rules to ensure a level playing field. More broadly, the administrative costs introduced for businesses (EUR 18.5 million one-off costs) is a proportionate and relatively small administrative burden.

- **Fundamental rights**

This proposal has an impact on the fundamental rights of consumers, notably Article 7 and 8 on the right to respect for private life and the right to the protection of personal data enshrined in the EU Charter on Fundamental Rights (the EU Charter). The proposal establishes access rights for data in the financial sector, which would contribute to increased sharing of data, including personal data, at customers' request. The impact to fundamental rights will be mitigated by ensuring that in line with Article 38 of the EU Charter there is a high level of consumer protection and that data sharing is strictly subject to the request of the customer. To uphold Articles 7 and Article 8 of the EU Charter, some provisions, notably financial data access permission dashboards and targeted guidelines in areas of higher exclusion risk, will boost customer trust and provide a framework of user control sharing personal data. The dashboard will strengthen customer control, notably when personal data is processed for the requested service, based on consent or necessary for the performance of a contract. In addition, restriction on re-use of data beyond requested service is introduced. Introducing the new category of authorised 'financial information service providers' would ensure that only trusted and secure providers are eligible to access and process customer data in the financial sector. In addition, consumers will be protected with strong security safeguards against possible data misuse and data breaches as both data holders as well as data users will be bound by the rules of the Digital Operational Resilience Act (DORA).

4. BUDGETARY IMPLICATIONS

The implementation of this proposal would not have an impact on the general budget of the European Union. Although the European Supervisory Authorities (ESAs) will need to undertake some tasks so that the legislation is properly implemented, most of these tasks fall within the existing mandates of the ESAs, e.g. preparing draft regulatory or implementing standards or guidelines for the better application of this Regulation. In addition, while the European Banking Authority (EBA) would be required to set up a register with information on e.g. financial information service providers, the cost of establishing such a register would be limited and should be covered by cost savings resulting from the synergies and efficiencies that all Union bodies are expected to realise. Conversely the legislation would not confer any new supervisory or monitoring tasks on the ESAs. Therefore, any costs resulting from the implementation of the proposed legislation should be covered by the existing budget of the ESAs.

There are limited implications in terms of costs and administrative burden for national competent authorities (NCAs). Their magnitude and distribution will depend on the requirement placed on financial information service providers to apply for a license provided by an NCA and the related supervisory and monitoring tasks. These costs to NCAs would be partially offset by the supervisory fees that NCAs would levy on financial information service providers.

Regulated financial institutions that already have a licence would not be affected by the new licensing regime that this proposal would establish, and there would be no additional regulatory reporting, licensing or other requirements. For the firms that would need to seek a licence, the total costs of seeking a licence is estimated to be about EUR 18.5 million, assuming that about 350 firms would apply to become financial services information

providers (FISPS) to be able to access customer data. These firms would also have to comply with the DORA requirements and put in place the required cyber-security standards.

5. OTHER ELEMENTS

• Implementation plans and monitoring, evaluation and reporting arrangements

Providing a monitoring and evaluation mechanism is necessary to ensure that the regulatory actions undertaken are effective in achieving their objectives. The Commission will assess the impact of this Regulation and will be tasked with reviewing it (Article 31 of the proposal).

• Detailed explanation of the specific provisions of the proposal

This proposal seeks to establish a framework governing access to and use of customer data in finance (financial data access 'FIDA'). Financial data access refers to the access to and processing of business-to-business and business-to-customer (including consumer) data upon customer request across a wide range of financial services. The proposal is divided into nine Titles.

Title I sets the subject matter, scope and definitions. Article 1 sets out that the Regulation establishes the rules in line with which certain categories of customer data in finance may be accessed, shared, and used. It also establishes the requirements for the access, sharing, and use of data in finance, the respective rights and obligations of data users and data holders and the respective rights and obligations of financial information service providers in relation to the provision of information services as a regular occupation or business activity. Article 2 sets the scope of the Regulation to certain exhaustively described sets of data and lists the firms to which this Regulation applies. Article 3 sets the terms and definitions that are used for the purposes of this Regulation, including 'data holder', 'data user', 'financial information service provider' and others.

Title II introduces a legal obligation on data holders and governs the way this obligation should be exercised. Article 4 indicates that the data holder must make available to customers the data within the scope of this Regulation based on a request. Article 5 provides the customer with the right to request that the data holder shares this data with a data user. Where personal data is concerned, the request must comply with a valid legal basis as referred to in the General Data Protection Regulation (GDPR) that allows for the processing of personal data. Article 6 imposes certain obligations on data users receiving data at the request of customers. There should only be access to the customer data made available under Article 5 and this data should be used only for the purposes and the conditions agreed with the customer. The customer's personalised security credentials should not be accessible to other parties and the data should not be stored for longer than what is necessary.

Title III sets the requirements to ensure responsible data use and security. Article 7 provides guidance on how firms should use data for given use cases and ensures that there will not be any discrimination or restriction in the access to services as a result of the use of the data. It ensures that customers that refuse to grant permission to use sets of their data will not be refused access to financial products just because these customers refused to grant permission. Article 8 establishes the financial data access permission dashboards to ensure that customers can monitor their data permissions by being able to access an overview of their data permissions, grant new ones and withdraw permissions if necessary.

Title IV sets the requirements for the creation and governance of financial data sharing schemes whose aim is to bring together data holders, data users and consumer organisations. Such schemes should develop data and interface standards, set the coordination mechanisms for the operation of financial data access permission dashboards as well as a joint standardised

contractual framework governing access to specific datasets, the rules on governance of these schemes, transparency requirements, compensation rules, liability, and dispute resolution. Article 9 provides that the data falling within the scope of this Regulation must be made available only to members of a financial data-sharing scheme, rendering the existence and membership to such schemes mandatory. Article 10 sets the governance processes of such a scheme, including the rules on the contractual liability of its members and the mechanism to resolve disputes out-of-court. Article 10 also provides for the developments of common standards for the sharing of data and the creation of technical interfaces to be used for the sharing of data. Such data-sharing schemes must be notified to the competent authorities, they must benefit from a passport for operations across the EU and or transparency purposes, the schemes must be part of a register to be maintained by EBA. The minimum arrangements for a financial data sharing scheme should also state that data holders must be entitled to compensation for making the data available to data users, according to the terms of the scheme they are both part of. Compensation in any case must be reasonable, based on a clear and transparent methodology previously agreed by the scheme members and should aim to reflect at least the costs incurred for making available a technical interface to share the data requested. Article 11 provides for a Commission empowerment to adopt a delegated act in the event that a financial data sharing scheme is not developed for one or more categories of customer data.

Title V sets out the provisions on authorisation and operating conditions of financial information service providers. These requirements highlight the required content of an application (Article 12), the appointment of a legal representative (Article 13), the scope of the authorisation, including the EU passport of financial information service providers (Article 14) and the right granted to competent authorities to withdraw an authorisation. Article 15 provides for the establishment of a register of financial information service providers and data sharing schemes to be held by the EBA. Article 16 provides for the organisational requirements of financial information service providers.

Title VI provides details on the powers of competent authorities. Article 17 imposes on Member States the obligation to designate competent authorities. Article 18 sets out detailed provisions on the powers of competent authorities, Article 19 provides for the power to reach settlement agreements and expedited enforcement procedures. Articles 20 to 21 detail the administrative penalties and other administrative measures, as well as the periodic penalty payments, that can be imposed by competent authorities. Article 22 sets out the circumstances that should be considered when competent authorities determine administrative penalties and other administrative measures. Article 23 covers professional secrecy for information exchanges between competent authorities. Title VI includes rules on the right to appeal (Article 24), the publication of administrative sanctions and administrative measures imposed (Article 25), the rules on the exchange of information between competent authorities (Article 26) and the settlement of disagreements between them (Article 27).

Title VII provides for the notification procedure to competent authorities for firms exercising the right of establishment and freedom to provide services (Article 28), as well as an obligation of information from competent authorities when they take measures involving restrictions on the freedom of establishment (Article 29).

Title VIII includes the exercise of the delegation with a view to adopt Commission delegated acts (Article 30), as the proposal itself contains an empowerment for the Commission to adopt a delegated act under Article 11. This Title also includes the obligation for the Commission to review certain aspects of the Regulation (Article 31). Articles 32 to 34 include the necessary amendments to the regulations establishing the ESAs to include this Regulation and financial information service providers within their scope. Article 35 includes an amendment to the

Digital Operational Resilience Act Regulation. Article 36 indicates that this Regulation enters into application 24 months after its entry into force, except for Title IV (on schemes) that enters into application 18 months after the Regulation's entry into force.

2023/0205 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[6],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) A responsible data economy, which is driven by the generation and use of data, is an integral part of the Union internal market that can bring benefits to both Union citizens and the economy. Digital technologies relying on data are increasingly driving change in financial markets by producing new business models, products and ways for firms to engage with customers.

(2) Customers of financial institutions, both consumers and firms, should have effective control over their financial data and the opportunity to benefit from open, fair, and safe data-driven innovation in the financial sector. Those customers should be empowered to decide how and by whom their financial data is used and should have the option to grant firms access to their data for the purposes of obtaining financial and information services should they wish.

(3) The Union has a stated policy interest in enabling access of customers of financial institutions to their financial data. The Commission confirmed in its communication on a digital finance strategy and Communication on a capital markets union adopted in 2021 an intention to put in place a framework for financial data access to reap the benefits for customers of data sharing in the financial sector. Such benefits include the development and provision of data-driven financial products and financial services, made possible by the sharing of customer data.

(4) Within financial services, and as a result of the revised Directive (EU) 2015/2366 of the European Parliament and of the Council[7], the sharing of payments account data in

[6] OJ C , , p. .

the Union based on customer permission has begun to transform the way consumers and businesses use banking services. In order to build upon the measures in that Directive, a regulatory framework should be established for the sharing of customer data across the financial sector beyond payment account data. This should also be a building block for fully integrating the financial sector into the Commission's strategy for data[8] which promotes data sharing across sectors.

(5) Ensuring customer control and trust is imperative to build a well-functioning and effective data sharing framework in the financial sector. Ensuring effective customers' control over data sharing contributes to innovation as well as customer confidence and trust in data sharing. As a result, effective control helps overcome customer reluctance to share their data. Under the current Union framework, the data portability right of a data subject in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council[9] is limited to personal data and can be relied upon only where it is technically feasible to port the data. Customer data and technical interfaces in the financial sector beyond payment accounts are not standardised, rendering data sharing more costly. Further, the financial institutions are only legally obliged to make the payment data of their customers available.

(6) The Union's financial data economy therefore remains fragmented, characterised by uneven data sharing, barriers, and high stakeholder reluctance to engage in data sharing beyond payments accounts. Customers accordingly do not benefit from individualised, data-driven products and services that may fit their specific needs. The absence of personalised financial products limits the possibility to innovate, by offering more choice and financial products and services for interested consumers who could otherwise benefit from data-driven tools that can support them to make informed choices, compare offerings in a user-friendly manner, and switch to more advantageous products that match their preferences based on their data. The existing barriers to business data sharing are preventing firms, in particular SMEs, to benefit from better, convenient and automated financial services.

(7) Making data available by way of high-quality application programming interfaces is essential to facilitate seamless and effective access to data. Beyond the area of payment accounts, however, only a minority of financial institutions that are data holders indicate that they make data available through technical interfaces like application programming interfaces. As incentives to develop such innovative services are absent, market demand for data access remains limited.

(8) A dedicated and harmonised framework for access to financial data is therefore necessary at Union level to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data. Specific rules are required to address these barriers to promote better access to customer data and hence make it

---

[7] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directive 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

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

possible for consumers and firms to realise the gains stemming from better financial products and services. Data-driven finance would facilitate industry transition from the traditional supply of standardised products to tailored solutions that are better suited to the customers' specific needs, including improved customer facing interfaces that enhance competition, improve user experience and ensure financial services that are focused on the customer as the end user.

(9) The data included in the scope of this Regulation should demonstrate high value added for financial innovation as well as low financial exclusion risk for consumers. This Regulation should therefore not cover data related to the sickness and health insurance of a consumer in accordance with Directive 2009/138/EC of the European Parliament and of the Council[10] as well as data on life insurance products of a consumer in accordance with Directive 2009/138/EC other than life insurance contracts covered by insurance-based investment products. This Regulation should also not cover data collected as part of a creditworthiness assessment of a consumer. The sharing of customer data in the scope of this Regulation should respect the protection of confidential business data and trade secrets.

(10) The sharing of the customer data in the scope of this Regulation should be based on the permission of the customer. The legal obligation on data holders to share customer data should be triggered once the customer has requested their data to be shared with a data user. This request can be submitted by a data user acting on behalf of the customer. Where the processing of personal data is involved, a data user should have a valid lawful basis for processing under Regulation (EU) 2016/679. The customers data can be processed for the agreed purposes in the context of the service provided. The processing of personal data must respect the principles of personal data protection, including lawfulness, fairness and transparency, purpose limitation and data minimisation. A customer has the right to withdraw the permission given to a data user. When data processing is necessary for the performance of a contract, a customer should be able to withdraw permissions according to the contractual obligations to which the data subject is party. When personal data processing is based on consent, a data subject has the right to withdraw his or her consent at any time, as provided for in Regulation (EU) 2016/679.

(11) Enabling customers to share their data on their current investments can encourage innovation in the provision of retail investment services. Primary data collection to complete a suitability and appropriateness assessment of a retail investor is time-intensive for a customer and constitutes a significant cost factor for advisors and distributors of investment, pension, and insurance-based investment products. The sharing of customer data on holdings of savings and investments in financial instruments including insurance-based investment products and data collected for the purposes of carrying out a suitability and appropriateness assessment can improve investment advice for consumers and has strong innovative potential, including in the development of personalised investment advice and investment management tools that can make retail investment advice more efficient. Such management tools are already being developed in the market and can develop more effectively in the context where a customer can share their investment-related data.

---

[10] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (recast) (OJ L 335, 17.12.2009, p. 1).

(12) Customer data on balance, conditions or transaction details related to mortgages, loans and savings can enable customers to gain a better overview of their deposits and better meet their savings needs based on credit data. This Regulation should cover customer data beyond payment accounts defined in Directive (EU) 2015/2366. Credit accounts covered by a credit line which cannot be used for the execution of payment transactions to third parties should be within the scope of this Regulation. It should therefore be understood that this Regulation covers the access to the balance, conditions or transaction details related to mortgage credit agreements, loans, and savings accounts as well as the types of accounts not falling withing the scope of the Directive (EU) 2015/2366[11].

(13) The customer data included in the scope of this Regulation should include sustainability-related information that should enable customers to more easily access financial services that are aligned with their sustainability preferences and sustainable finance needs, in line with the Commission's strategy for financing the transition to a sustainable economy[12]. Access to data relating to sustainability which may be contained in balance or transaction details related to a mortgage, credit, loan and savings account, as well as access to customer data relating to sustainability held by investment firms, can contribute to facilitating access to data needed to access sustainable finance or make investments into the green transition. Moreover, customer data in the scope of this Regulation should include data which forms part of a creditworthiness assessment related to firms, including small and medium sized enterprises, and which can provide greater insight into the sustainability objectives of small firms. The inclusion of data used for the creditworthiness assessment related to firms should improve access to financing and streamline the application for loans. Such data should be limited to data on firms and should not infringe intellectual property rights.

(14) Customer data related to the provision of non-life insurance are essential to enable insurance products and services important to the needs of customer like the protection of homes, vehicles, and other property. At the same time, the collection of such data is often burdensome and costly and can act as a deterrent against seeking optimal insurance coverage by customers. To address this problem, it is therefore necessary to include such financial services within the scope of this Regulation. Customer data on insurance products within scope of this Regulation should include both insurance product information such as detail on an insurance coverage and data specific to the consumers' insured assets which are collected for the purposes of a demands and needs test. The sharing of such data should allow for the development of personalised tools for customers, such as insurance dashboards that could help consumers better manage their risks. It could also help customers to obtain products that are better targeted to their demands and needs, including through more valuable advice. This can contribute to more optimal insurance coverage for customers and increased financial inclusion of otherwise underserved consumers, by offering new or increased coverage.

---

11 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337 23.12.2015, p. 35).

12 Communication From the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions, Strategy for Financing the Transition to a Sustainable Economy, COM/2021/390 final

Moreover, the sharing of insurance data can be beneficial for more efficient supply of insurance including, in particular, at the stages of product design, underwriting, contract execution, including claims management, and risk mitigation.

(15) The sharing of data on occupational and personal pension savings has strong innovative potential for consumers. Pension savers often lack sufficient knowledge about their pension rights, which is related to the fact that data on such rights are often dispersed across different data holders. The sharing of data related to occupational and personal pension savings should contribute to the development of pension tracking tools that provide savers with a comprehensive overview of their entitlements and retirement income both within specific Member States and cross-border in the Union. Data on pension rights concerns in particular accrued pension entitlements, projected levels of retirement benefits, risks and guarantees of members and beneficiaries of occupational pension schemes. Access to data related to occupational pensions is without prejudice to national social and labour law on the organisation of pension systems, including membership of schemes and the outcomes of collective bargaining agreements.

(16) Data which forms part of a creditworthiness assessment of a firm in the scope of this Regulation should consist of information which a firm provides to institutions and creditors as part of the loan application process or a request for a credit rating. This includes loan applications of micro, small, medium and large enterprises. It may include data collected by institutions and creditors as set out in Annex II of the European Banking Authority Guidelines on loan origination and monitoring[13]. Such data may include financial statements and projections, information on financial liabilities and arrears in payment, evidence of ownership of the collateral, evidence of insurance of the collateral and information on guarantees. Additional data may be relevant if the purpose of the loan application relates to the purchase of commercial real estate or real estate development.

(17) As this Regulation is meant to oblige financial institutions to provide access to defined categories of data at the request of the customer when acting as data holders, and allow the sharing of data based on customer permission when financial institutions act as data users, it should provide a list of the financial institutions that may act as either a data holder, a data user or both. Financial institutions should therefore be understood to mean those entities that provide financial products and financial services or offer relevant information services to customers in the financial sector.

(18) Practices employed by data users to combine new and traditional customer data sources in the scope of this Regulation must be proportionate to ensure that they do not lead to financial exclusion risks for consumers. Practices that lead to a more sophisticated or comprehensive analysis of certain vulnerable segments of consumers, such as persons with a low income, may increase the risk of unfair conditions or differential pricing practices like the charging of differential premiums. The potential for exclusion is increased in the provision of products and services that are priced according to the profile of a consumer, notably in credit scoring and the assessment of creditworthiness of natural persons as well for products and services related to the risk assessment and pricing of natural persons in the case of life and health insurance. Given the risks, the use of data for these products and services should be subject to specific requirements to protect consumers and their fundamental rights.

---

13 EBA Final Report on Guidelines on loan origination and monitoring.pdf (europa.eu), 29.05.2020.

(19) The data use perimeter thus established in this Regulation and in the accompanying guidelines ('the guidelines') to be developed by the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) should provide a proportionate framework on how personal data related to a consumer that falls within the scope of this Regulation should be used. The data use perimeter ensures consistency between the scope of this Regulation, which excludes data that forms part of a creditworthiness assessment of a consumer as well as data related to life, health and sickness insurance of a consumer, and the scope of the guidelines, which set recommendations on how types of data originating from other areas of the financial sector that are in scope of this Regulation can be used to provide these products and services. The guidelines developed by the EBA should set out how other types of data that are in scope of this Regulation can be used to assess the credit score of a consumer. The guidelines developed by EIOPA should set out how data in scope of this Regulation can be used in products and services related to risk assessment and pricing in the case of life, health and sickness insurance products. The guidelines should be developed in a manner that is aligned to the needs of the consumer and proportionate to the provision of such products and services.

(20) EBA and EIOPA should closely cooperate with the European Data Protection Board when drafting the guidelines, which should build on existing recommendations on the use of consumer information in the area of consumer and mortgage credit, notably the rules on use of creditworthiness assessment under Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, the European Banking Authority's Guidelines on loan origination and monitoring, and the European Banking Authority guidelines on creditworthiness assessment developed under Directive 2014/17/EU, as well guidelines provided by European Data Protection Board on the processing of personal data.

(21) Customers must have effective control over their data and confidence in managing permissions they have granted in accordance with this Regulation. Data holders should therefore be required to provide customers with common and consistent financial data access permission dashboards. The permission dashboard should empower the customer to manage their permissions in an informed and impartial manner and give customers a strong measure of control over how their personal and non-personal data is used. It should not be designed in a way that would encourage or unduly influence the customer to grant or withdraw permissions. The permission dashboard should take into account, where appropriate, the accessibility requirements under Directive (EU) 2019/882 of the European Parliament and of the Council[14]. When providing a permission dashboard, data holders could use a notified electronic identification and trust service, such as a European Digital Identity Wallet issued by a Member State as introduced by the proposal amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity[15]. Data holders may also rely on data intermediation service providers under Regulation (EU) 2022/868 of the

[14] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70–115)

[15] COM(2021) 281 final, 2021/0136(COD)

European Parliament and of the Council[16], to provide permission dashboards that fulfil the requirements of this Regulation.

(22) The permission dashboard should display the permissions given by a customer, including when personal data are shared based on consent or are necessary for the performance of a contract. The permission dashboard should warn a customer in a standard way of the risk of possible contractual consequences of the withdrawal of a permission, but the customer should remain responsible for managing such risk. The permission dashboard should be used to manage existing permissions. Data holders should inform data users in real-time of any withdrawal of a permission. The permission dashboard should include a record of permissions that have been withdrawn or have expired for a period of up to two years to allow the customer to keep track of their permissions in an informed and impartial manner. Data users should inform data holders in real-time of new and re-established permissions granted by customers, including the duration of validity of the permission and a short summary of the purpose of the permission. The information provided on the permission dashboard is without prejudice to the information requirements under Regulation (EU) 2016/679.

(23) To ensure proportionality, certain financial institutions are out of the scope of this Regulation for reasons associated with their size or the services they provide, which would make it too difficult to comply with this regulation. These include institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total, as well as insurance intermediaries who are microenterprises or small or medium-sized enterprises. In addition, small or medium-sized enterprises acting as data holders that are within the scope of this Regulation should be allowed to establish an application programming interface jointly, reducing the costs for each of them. They can also avail themselves of external technology providers which run application programming interfaces in a pooled manner for financial institutions and may charge them only a low fixed usage fee and work largely on a pay-per-call basis.

(24) This Regulation introduces a new legal obligation on financial institutions acting as data holders to share defined categories of data at request of the customer. The obligation on data holders to share data at the request of the customer should be specified by making available generally recognised standards to also ensure that the data shared is of a sufficiently high quality. The data holder should make customer data available continuously for the purposes and under the conditions for which the customer has granted permission to a data user. Continuous access could consist of multiple requests to make customer data available to fulfil the service agreed with the customer. It could also consist of a one-off access to customer data. While the data holder is responsible for the interface to be available and for the interface to be of adequate quality, the interface may be provided not only by the data holder but also by another financial institution, an external IT provider, an industry association or a group of financial institutions, or by a public body in a member state. For institutions for occupational retirement provisions, the interface can be integrated into pension

[16] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1).

dashboards that cover a broader range of information, as long as it complies with the requirements of this Regulation.

(25) In order to enable the contractual and technical interaction necessary for implementing data access between multiple financial institutions, data holders and data users should be required to be part of financial data sharing schemes. These schemes should develop data and interface standards, joint standardised contractual frameworks governing access to specific datasets, and governance rules related to data sharing. In order to ensure that schemes function effectively, it is necessary to establish general principles for the governance of these schemes, including rules on inclusive governance and participation of data holders, data users and customers (to ensure balanced representation in schemes), transparency requirements, and a well-functioning appeal and review procedure (notably around the decision-making of schemes). Financial data sharing schemes must comply with Union rules in the area of consumer protection and data protection, privacy, and competition. The participants in such schemes are also encouraged to draw up codes of conduct similar to those prepared by controllers and processors under Article 40 of Regulation (EU) 2016/679. While such schemes may build upon existing market initiatives, the requirements set out in this Regulation should be specific to financial data sharing schemes or parts thereof which market participants use to fulfil their obligations under this Regulation after the data of application of these obligations.

(26) A financial data sharing scheme should consist of a collective contractual agreement between data holders and data users with the objective of promoting efficiency and technical innovation in financial data sharing to the benefit of customers. In line with Union rules on competition, a financial data sharing scheme should only impose on its members restrictions which are necessary to achieve its objectives and which are proportionate to those objectives. It should not afford its members the possibility of preventing, restricting or distorting competition in respect of a substantial part of the relevant market.

(27) In order to ensure the effectiveness of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of specifying the modalities and characteristics of a financial data sharing scheme in case a scheme is not developed by the data holders and the data users. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[17]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(28) Data holders and data users should be allowed to use existing market standards when developing common standards for mandatory data sharing.

(29) To ensure that data holders have an interest in providing high quality interfaces for making data available to data users, data holders should be able to request reasonable compensation from data users for putting in place application programming interfaces. Facilitating data access against compensation would ensure a fair distribution of the

[17] OJ L 123, 12.5.2016, p. 1.

related costs between data holders and data users in the data value chain. In cases where the data user is an SME, proportionality for smaller market participants should be ensured by limiting compensation strictly to the costs incurred for facilitating data access. The model for determining the level of compensation should be defined as part of the financial data sharing schemes as provided in this Regulation.

(30) Customers should know what their rights are in case problems arise when data is shared and who to approach to seek compensation. Financial data sharing scheme members, including data holders and data users, should therefore be required to agree on the contractual liability for data breaches as well as how to resolve potential disputes between data holders and data users regarding liability. Those requirements should focus on establishing, as part of any contract, liability rules as well as clear obligations and rights to determine liability between the data holder and the data user. Liability issues related to the consumers as data subjects should be based on Regulation (EU) 2016/679, notably the right to compensation and liability under Article 82 of that Regulation.

(31) To promote consumer protection, enhance customer trust and ensure a level playing field, it is necessary to lay down rules on who is eligible to access customers' data. Such rules should ensure that all data users are authorised and supervised by competent authorities. This would ensure that data can be accessed only by regulated financial institutions or by firms subject to a dedicated authorisation as financial information service providers' ('FISPs') which is subject to this Regulation. Eligibility rules on FISPs, are needed to safeguard financial stability, market integrity and consumer protection, as FISPs would provide financial products and services to customers in the Union and would access data held by financial institutions and the integrity of which is essential to preserve the financial institutions' ability to continue providing financial services in a safe and sound manner. Such rules are also required to guarantee the proper supervision of FISPs by competent authorities in line with their mandate to safeguard financial stability and integrity in the Union, which would allow FISPs to provide throughout the Union the services for which they are authorised.

(32) Data users within the scope of this Regulation should be subject to the requirements of Regulation (EU) 2022/2554 of the European Parliament and of the Council[18] and therefore be obliged to have strong cyber resilience standards in place to carry out their activities. This includes having comprehensive capabilities to enable a strong and effective ICT risk management, as well as specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents. Data users authorised and supervised as financial information service providers under this Regulation should follow the same approach and the same principle-based rules when addressing ICT risks taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. Financial information service providers should therefore be included in the scope of Regulation (EU) 2022/2554.

[18] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

(33) In order to enable effective supervision and to eliminate the possibility of evading or circumventing supervision, financial information service providers must be either legally incorporated in the Union or in case they are incorporated in a third country appoint a legal representative in the Union. An effective supervision by the competent authorities is necessary for the enforcement of requirements under this Regulation to ensure integrity and stability of the financial system and to protect consumers. The requirement of legal incorporation of financial information service providers in the Union or the appointment of a legal representative in the Union does not amount to data localisation since this Regulation does not entail any further requirement on data processing including storage to be undertaken in Union.

(34) A financial information service provider should be authorised in the jurisdiction of the Member State where its main establishment is located, that is, where the financial information service provider has its head office or registered office within which the principal functions and operational control are exercised. In respect of financial information service providers that do not have an establishment in the Union but require access to data in the Union and therefore fall within the scope of this Regulation, the Member State where those financial information service providers have appointed their legal representative should have jurisdiction, considering the function of legal representatives under this Regulation.

(35) To facilitate transparency regarding data access and financial information service providers, EBA should establish a register of financial information service providers authorised under this Regulation, as well as financial data sharing schemes agreed between data holders and data users.

(36) Competent authorities should be conferred with the powers necessary to supervise the way the compliance of the obligation on data holders to provide access to customer data established by this Regulation is exercised by market participants, as well as to supervise financial information service providers. Access relevant data traffic records held by a telecommunications operator as well as the ability to seize relevant documents on premises are important and necessary powers to detect and prove the existence of breaches under this Regulation. Competent authorities should therefore have the power to require such records where they are relevant to an investigation, insofar as permitted under national law. Competent authorities should also cooperate with the supervisory authorities established under Regulation (EU) 2016/679 in the performance of their tasks and the exercise of their powers in accordance with that Regulation.

(37) Since financial institutions and financial information service providers can be established in different Member States and supervised by different competent authorities, the application of this Regulation should be facilitated by close cooperation among relevant competent authorities, through the mutual exchange of information and the provision of assistance in the context of the relevant supervisory activities.

(38) To ensure a level playing field in the area of sanctioning powers, Member States should be required to provide for effective, proportionate and dissuasive administrative sanctions, including periodic penalty payments, and administrative measures for the infringement of provisions of this Regulation. Those administrative sanctions, periodic penalty payments and administrative measures should meet certain minimum requirements, including the minimum powers that should be vested on competent authorities to be able to impose them, the criteria that competent authorities

should consider when imposing them, and the obligation to publish and report. Member States should lay down specific rules and effective mechanisms regarding the application of periodic penalty payments.

(39) In addition to administrative sanctions and administrative measures, competent authorities should be empowered to impose periodic penalty payments on financial information services providers and on those members of their management body who are identified as responsible for an ongoing infringement or who are required to comply with an order from an investigating competent authority. Since the purpose of the periodic penalty payments is to compel natural or legal persons to comply with an order from the competent authority to act, for example to accept to be interviewed or to provide information, or to terminate an ongoing breach, the application of periodic penalty payments should not prevent competent authorities from imposing subsequent administrative sanctions for the same infringement. Unless otherwise provided for by Member States, periodic penalty payments should be calculated on a daily basis.

(40) Irrespective of their denomination under national law, forms of expedited enforcement procedure or settlement agreements are to be found in many Member States and are used as an alternative to formal proceedings leading to imposing sanctions. An expedited enforcement procedure usually starts after an investigation has been concluded and the decision to start proceedings leading to imposing sanctions has been taken. An expedited enforcement procedure is characterised by being shorter than a formal one, due to simplified procedural steps. Under a settlement agreement usually the parties subject to the investigation by a competent authority agree to end that investigation early, in most cases by accepting liability for wrongdoing.

(41) While it does not appear appropriate to strive to harmonise at Union level such expedited enforcement procedures, which were introduced by many Member States, due to the varied legal approaches adopted at national level, it should be acknowledged that such methods allow competent authorities that can apply them, to handle infringement cases in a speedier, less costly and overall efficient way under certain circumstances, and should therefore be encouraged. However, Member States should not be obliged to introduce such enforcement methods in their legal framework nor should competent authorities be compelled to use them if they do not deem it appropriate. Where Member States choose to empower their competent authorities to use such enforcement methods, they should notify the Commission of such decision and of the relevant measures regulating such powers.

(42) National competent authorities should be empowered by Member States to impose such administrative sanctions and administrative measures to financial information service providers and other natural or legal persons where relevant to remedy the situation in the case of infringement. The range of sanctions and measures should be sufficiently broad to allow Member States and competent authorities to take account of the differences between financial information service providers, as regards their size, characteristics and the nature of their business.

(43) The publication of an administrative penalty or measure for infringement of provisions of this Regulation can have a strong dissuasive effect against repetition of such infringement. Publication also informs other entities of the risks associated with the sanctioned financial information service provider before entering into a business relationship and assists competent authorities in other Member States in relation to the risks associated with a financial information service provider when it operates in their Member States on a cross-border basis. For those reasons, the publication of decisions

on administrative penalties and administrative measures should, be allowed as long as it concerns legal persons. In taking a decision whether to publish an administrative penalty or administrative measure, competent authorities should take into account the gravity of the infringement and the dissuasive effect that the publication is likely to produce. However, any such publication referred to natural persons may impinge on their rights stemming from the Charter of Fundamental Rights and the applicable Union data protection legislation in a disproportionate manner. Publication should occur in an anonymised way unless the competent authority deems it necessary to publish decisions containing personal data for the effective enforcement of this Regulation, including in the case of public statements or temporary bans. In such cases the competent authority should justify its decision.

(44) The exchange of information and the provision of assistance between competent authorities of the Member States is essential for the purposes of this Regulation. Consequently, cooperation between authorities should not be subject to unreasonable restrictive conditions.

(45) The cross-border access to data by information service providers should be allowed pursuant to the freedom to provide services or the freedom of establishment. A financial information service provider wishing to have access to data held by a data holder in another Member State, should notify its intention to its competent authority, providing information on the type of data it wishes to access, the financial data sharing scheme of which it is a member and the Member States in which it intends to access the data.

(46) The objectives of this Regulation, namely giving effective control of data to the customer and addressing the lack of rights of access to customer data held by data holders, cannot be sufficiently achieved by the Member States given their cross-border nature but can rather be better achieved at Union level, by means of the creation of a framework through which a larger cross-border market with data access could be developed. The Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(47) The proposal for a Data Act [Regulation (EU) XX] establishes a horizontal framework for access to and use of data across the Union. This Regulation complements and specifies the rules laid down in the proposal for a Data Act [Regulation (EU) XX] Therefore those rules also apply to the sharing of data governed by this Regulation. This includes provisions on the conditions under which data holders make data available to data recipients, on compensation, dispute settlement bodies to facilitate agreements between data sharing parties, technical protection measures, international access and transfer of data and on authorised use or disclosure of data.

(48) Regulation (EU) 2016/679 applies when personal data are processed. It provides for the rights of a data subject, including the right of access and right to port personal data. This Regulation is without prejudice to the rights of a data subject provided under Regulation (EU) 2016/679, including the right of access and right to data portability. This Regulation creates a legal obligation to share customer personal and non-personal data upon customer's request and mandates the technical feasibility of access and sharing for all types of data within the scope of this Regulation. The granting of permission by a customer is without prejudice to the obligations of data users under Article 6 of Regulation (EU) 2016/679. Personal data that are made available and

shared with a data user should only be processed for services provided by a data user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, when applicable, where the requirements of Article 9 of that Regulation on the processing of special categories of data are met.

(49) This Regulation builds upon and complements the 'open banking' provisions under Directive (EU) 2015/2366 and is fully consistent with Regulation (EU) …/202.. of the European Parliament and of the Council on payment services and amending Regulation (EU) No 1093/2010[19] and Directive (EU) …/202.. of the European Parliament and of the Council on payment services and electronic money services amending Directives 2013/36/EU and 98/26/EC and repealing Directives 2015/2355/EU and 2009/110/EC[20]. The initiative complements the already existing 'open banking' provisions under Directive (EU) 2015/2366 that regulate access to payment account data held by account servicing payment service providers. It builds on the lessons learned on 'open banking' as identified in the review of Directive 2015/2366/EU.[21] This Regulation ensures coherence between financial data access and open banking where additional measures are necessary, including on permission dashboards, the legal obligations to grant direct access to customer data, and the requirement for data holders to put in place interfaces.

(50) This Regulation does not affect the provisions related to data access and data sharing in Union financial services legislation, namely the following: (i) the provisions on access to benchmarks and the access regime for exchange-traded derivatives between trading venues and Central Counterparties laid down in Regulation (EU) No 600/2014 of the European Parliament and of the Council[22]; (ii) the rules on access of creditors to the database under Directive 2014/17/EU of the European Parliament and of the Council[23]; (iii) the rules on access to securitisation repositories under Regulation (EU) 2017/2402 of the European Parliament and of the Council[24]; (iv) the rules on the right to request from the insurer a claims history statement and on the access to central repositories to basic data necessary for the settlement of claims under Directive 2009/103/EC of the European Parliament and of the Council[25]; (v) the right to access and transfer all necessary personal data to a new pan-European Personal Pension Product provider under Regulation (EU) 2019/1238 of the European Parliament and of

---

19 Regulation (EU) … (OJ ….)

20 Directive (EU) … (OJ…).

21 Report from the Commission on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market

22 Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173 12.6.2014, p. 84).

23 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 (OJ L 060 28.2.2014, p. 34).

24 Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012 (OJ L 347 28.12.2017, p. 35).

25 Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (OJ L 263, 7.10.2009, p. 11).

the Council[26]; and (vi) the provisions on outsourcing and reliance under Directive (EU) 2018/843 of the European Parliament and of the Council[27]. Furthermore, this Regulation does not affect the application of EU or national rules of competition of the Treaty on the Functioning of the European Union and any secondary Union acts. This Regulation is also without prejudice to accessing, sharing and using data without making use of the data access obligations established by this Regulation on a purely contractual basis.

(51) As the sharing of data related to payment accounts is regulated under a different regime set out in Directive (EU) 2015/2366, it is deemed appropriate to set, in this Regulation, a review clause for the Commission to examine whether the introduction of the rules under this Regulation impacts the way AISPs access data and whether it would be appropriate to streamline the rules governing the sharing of data applicable to AISPs.

(52) Given that EBA, EIOPA and ESMA should be mandated to make use of their powers in relation to financial information service providers, it is necessary to ensure that they are able to exercise all of their powers and tasks in order to fulfil their objectives of protecting the public interest by contributing to the short, medium and long-term stability and effectiveness of the financial system, for the Union economy, its citizens and businesses and to ensure that financial information service providers are covered by Regulations (EU) No 1093/2010[28], (EU) No 1094/2010[29] and (EU) No 1095/2010[30] of the European Parliament and of the Council. Those Regulations should therefore be amended accordingly.

(53) The date of application of this Regulation should be deferred by XX months in order to allow for the adoption of regulatory technical standards and delegated acts that are necessary to specify certain elements of this Regulation.

(54) The European Data Protection Supervisor was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[31] and delivered an opinion on […….]

---

26 Regulation (EU) 2019/1238 of the European Parliament and of the Council of 20 June 2019 on a pan-European Personal Pension Product (PEPP) (OJ L 198, 25.7.2019, p. 1).

27 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 (OJ L 156, 19.6.2018, p. 43).

28 Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

29 Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

30 Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

31 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions,

HAVE ADOPTED THIS REGULATION:

TITLE I
SUBJECT MATTER, SCOPE, AND DEFINITIONS

Article 1
Subject matter

This Regulation establishes rules on the access, sharing and use of certain categories of customer data in financial services.

This Regulation also establishes rules concerning the authorisation and operation of financial information service providers.

Article 2
Scope

1. This Regulation applies to the following categories of customer data on:

   (a) mortgage credit agreements, loans and accounts, except payment accounts as defined in the Payment Services Directive (EU) 2015/2366, including data on balance, conditions and transactions;

   (b) savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate and other related financial assets as well as the economic benefits derived from such assets; including data collected for the purposes of carrying out an assessment of suitability and appropriateness in accordance with Article 25 of Directive 2014/65/EU of the European Parliament and of the Council[32];

   (c) pension rights in occupational pension schemes, in accordance with Directive 2009/138/EC and Directive (EU) 2016/2341 of the European Parliament and of the Council[33] ;

   (d) pension rights on the provision of pan-European personal pension products, in accordance with Regulation (EU) 2019/1238;

   (e) non-life insurance products in accordance with Directive 2009/138/EC, with the exception of sickness and health insurance products; including data collected for the purposes of a demands and needs assessment in accordance with Article 20 of Directive (EU) 2016/97 of the European Parliament and

---

bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[32] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (OJ L 173, 12.6.2014, p. 349).

[33] Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (recast) (OJ L 354, 23.12.2016, p. 37).

Council[34], and data collected for the purposes of an appropriateness and suitability assessment in accordance with Article 30 of Directive (EU) 2016/97.

(f) data which forms part of a creditworthiness assessment of a firm which is collected as part of a loan application process or a request for a credit rating.

2. This Regulation applies to the following entities when acting as data holders or data users:

(a) credit institutions;

(b) payment institutions, including account information service providers and payment institutions exempted pursuant to Directive (EU) 2015/2366;

(c) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC of the European Parliament and of the Council[35];

(d) investment firms;

(e) crypto-asset service providers;

(f) issuers of asset-referenced tokens;

(g) managers of alternative investment funds;

(h) management companies of undertakings for collective investment in transferable securities;

(i) insurance and reinsurance undertakings;

(j) insurance intermediaries and ancillary insurance intermediaries;

(k) institutions for occupational retirement provision;

(l) credit rating agencies;

(m) crowdfunding service providers;

(n) PEPP providers;

(o) financial information service providers

3. This Regulation shall not apply to the entities referred to in Article 2(3), points (a) to (e), of Regulation (EU) 2022/2554.

4. This Regulation does not affect the application of other Union legal acts regarding access to and sharing of customer data referred to in paragraph 1, unless specifically provided for in this Regulation.

Article 3
Definitions

For the purposes of this Regulation, the following definitions apply:

[34] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast) (OJ L 26, 2.2.2016, p. 19–5)

[35] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

(1) ‘consumer’ means a natural person who is acting for purposes other than his or her trade, business or profession;

(2) ‘customer’ means a natural or a legal person who makes use of financial products and services;

(3) ‘customer data’ means personal and non-personal data that is collected, stored and otherwise processed by a financial institution as part of their normal course of business with customers which covers both data provided by a customer and data generated as a result of customer interaction with the financial institution;

(4) ‘competent authority’ means the authority designated by each Member State in accordance with Article 17 and for financial institutions it means any of the competent authorities listed in Article 46 of Regulation (EU) 2022/2554;

(5) ‘data holder’ means a financial institution other than an account information service provider that collects, stores and otherwise processes the data listed in Article 2(1) ;

(6) ‘data user’ means any of the entities listed in Article 2(2) who, following the permission of a customer, has lawful access to customer data listed in Article 2(1) ;

(7) ‘financial information service provider’ means a data user that is authorised under Article 14 to access the customer data listed in Article 2(1) for the provision of financial information services;

(8) ‘financial institution’ means the entities listed in Article 2(2) points (a) to (n), who are either data holders, data users or both for the purposes of this Regulation.

(9) ‘investment account’ means any register managed by an investment firm, credit institution or an insurance broker about the current holdings in financial instruments or insurance-based investment products of their client, including past transactions and other data points relating to lifecycle events of that instrument

(10) ‘non-personal data’ means data other than personal data as defined in Article 4(1) of Regulation (EU) 2016/679;

(11) ‘personal data’ means personal data as defined in Article 4(1) of Regulation 2016/679;

(12) ‘credit institution’ means a credit institution as defined in Article 4(1), point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council[36];

(13) ‘investment firm’ means an investment firm as defined in Article 4(1), point (1), of Directive 2014/65/EU;

(14) ‘crypto asset service provider’ means a crypto asset service providers as referred to in Article 3(1), point (15) of Regulation (EU) 2023/1114 of the European Parliament and of the Council[37];

---

[36] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

[37] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023, p. 40).

(15) ‘issuer of asset referenced tokens’ means an issuer of asset referenced tokens authorised under Article 21 of Regulation (EU) 2023/1114;

(16) ‘payment institution’ means a payment institution as defined in Article 4(4), of Directive (EU) 2015/2366;

(17) ‘account information service provider’ means an account information service provider as referred to in Article 33(1) of Directive (EU) 2015/2366;

(18) ‘electronic money institution’ means an electronic money institution as defined in Article 2(1), of Directive 2009/110/EC;

(19) ‘electronic money institution exempted pursuant to Directive 2009/110/EC’ means an electronic money institution benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC;

(20) ‘manager of alternative investment funds’ means a manager of alternative investment funds as defined in Article 4(1), point (b), of Directive 2011/61/EU of the European Parliament and of the Council[38];

(21) ‘management company of undertakings for collective investment in transferable securities’ means a management company as defined in Article 2(1), point (b), of Directive 2009/65/EC of the European Parliament and of the Council[39];

(22) ‘insurance undertaking’ means an insurance undertaking as defined in Article 13(1) of Directive 2009/138/EC;

(23) ‘reinsurance undertaking’ means a reinsurance undertaking as defined in Article 13(4) of Directive 2009/138/EC;

(24) ‘insurance intermediary’ means an insurance intermediary as defined in Article 2(1), point (3), of Directive (EU) 2016/97 of the European Parliament and of the Council[40];

(25) ‘ancillary insurance intermediary’ means an ancillary insurance intermediary as defined in Article 2(1), point (4), of Directive (EU) 2016/97;

(26) ‘institution for occupational retirement provision’ means an institution for occupational retirement provision as defined in Article 6(1), of Directive (EU) 2016/2341;

(27) ‘credit rating agency’ means a credit rating agency as defined in Article 3(1), point (b), of Regulation (EC) No 1060/2009 of the European Parliament and of the Council[41];

---

[38] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).

[39] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (recast) (OJ L 302, 17.11.2009, p. 32).

[40] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast) (OJ L 26, 2.2.2016, p. 19).

[41] Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies (OJ L 302, 17.11.2009, p. 1).

(28) "PEPP provider" means a PEPP provider as defined in Article 2, point (15) of Regulation (EU) 2019/1238 of the European Parliament and of the Council;

(29) 'legal representative' means a natural person domiciled in the Union or a legal person with its registered office in the Union, and which, expressly designated by a financial information service provider established in a third country, acts on behalf of such financial information service provider vis-à-vis the authorities, clients, bodies and counterparties to the financial information service provider in the Union with regard to the financial information service provider's obligations under this Regulation;

TITLE II
DATA ACCESS

Article 4
Obligation to make available data to the customer

The data holder shall, upon request from a customer submitted by electronic means, make the data listed in Article 2(1) available to the customer without undue delay, free of charge, continuously and in real-time.

Article 5
Obligations on a data holder to make customer data available to a data user

1. The data holder shall, upon request from a customer submitted by electronic means, make available to a data user the customer data listed in Article 2(1) for the purposes for which the customer has granted permission to the data user. The customer data shall be made available to the data user without undue delay, continuously and in real-time.

2. A data holder may claim compensation from a data user for making customer data available pursuant to paragraph 1 only if the customer data is made available to a data user in accordance with the rules and modalities of a financial data sharing scheme, as provided in Articles 9 and 10, or if it is made available pursuant to Article 11.

3. When making data available pursuant to paragraph 1, the data holder shall:

   (a) make customer data available to the data user in a format based on generally recognised standards and at least in the same quality available to the data holder;

   (b) communicate securely with the data user by ensuring an appropriate level of security for the processing and transmission of customer data;

   (c) request data users to demonstrate that they have obtained the permission of the customer to access the customer data held by the data holder;

   (d) provide the customer with a permission dashboard to monitor and manage permissions in accordance with Article 8.

   (e) respect the confidentiality of trade secrets and intellectual property rights when customer data is accessed in accordance with Article 5(1).

Article 6
Obligations on a data user receiving customer data

1. A data user shall only be eligible to access customer data pursuant to Article 5(1) if that data user is subject to prior authorisation by a competent authority as a financial institution or is a financial information service provider pursuant to Article 14.

2. A data user shall only access customer data made available under Article 5(1) for the purposes and under the conditions for which the customer has granted its permission. A data user shall delete customer data when it is no longer necessary for the purposes for which the permission has been granted by a customer.

3. A customer may withdraw the permission it has granted to a data user. When processing is necessary for the performance of a contract, a customer may withdraw the permission it has granted to make customer data available to a data user according to the contractual obligations to which it is subject.

4. To ensure the effective management of customer data, a data user shall:

   (a) not process any customer data for purposes other than for performing the service explicitly requested by the customer;

   (b) respect the confidentiality of trade secrets and intellectual property rights when customer data is accessed in accordance with Article 5(1);

   (c) put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal customer data that is unlawful under Union law or the national law of a Member State;

   (d) take necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal customer data;

   (e) not process customer data for advertising purposes, except for direct marketing in accordance with Union and national law;

   (f) where the data user is part of a group of companies, customer data listed in Article 2(1) shall only be accessed and processed by the entity of the group that acts as a data user.

TITLE III
RESPONSIBLE DATA USE AND PERMISSION DASHBOARDS

Article 7
Data use perimeter

1. The processing of customer data referred to in Article 2(1) of this Regulation that constitutes personal data shall be limited to what is necessary in relation to the purposes for which they are processed.

2. In accordance with Article 16 of Regulation (EU) No 1093/2010, the European Banking Authority (EBA) shall develop guidelines on the implementation of paragraph 1 of this Article for products and services related to the credit score of the consumer.

3. In accordance with Article 16 of Regulation (EU) No 1094/2010, the European Insurance and Occupational Pensions Authority (EIOPA) shall develop guidelines on the implementation of paragraph 1 of this Article for products and services related to

risk assessment and pricing of a consumer in the case of life, health and sickness insurance products.

4. When preparing the guidelines referred to in paragraphs 2 and 3 of this Article, EIOPA and EBA shall closely cooperate with the European Data Protection Board established by Regulation (EU) 2016/679.

Article 8
Financial Data Access permission dashboards

1. A data holder shall provide the customer with a permission dashboard to monitor and manage the permissions a customer has provided to data users.

2. A permission dashboard shall:

   (a) provide the customer with an overview of each ongoing permission given to data users, including:

      (i) the name of the data user to which access has been granted

      (ii) the customer account, financial product or financial service to which access has been granted;

      (iii) the purpose of the permission;

      (iv) the categories of data being shared;

      (v) the period of validity of the permission;

   (b) allow the customer to withdraw a permission given to a data user;

   (c) allow the customer to re-establish any permission withdrawn;

   (d) include a record of permissions that have been withdrawn or have expired for a duration of two years.

3. The data holder shall ensure that the permission dashboard is easy to find in its user interface and that information displayed on the dashboard is clear, accurate and easily understandable for the customer.

4. The data holder and the data user for which permission has been granted by a customer shall cooperate to make information available to the customer via the dashboard in real-time. To fulfil the obligations in paragraph 2 points (a), (b), (c) and (d) of this Article:

   (a) The data holder shall inform the data user of changes made to a permission concerning that data user made by a customer via the dashboard.

   (b) A data user shall inform the data holder of a new permission granted by a customer regarding customer data held by that data holder, including:

      (i) the purpose of the permission granted by the customer;

      (ii) the period of validity of the permission

      (iii) the categories of data concerned.

TITLE IV
FINANCIAL DATA SHARING SCHEMES

Article 9
Financial data sharing scheme membership

1. Within 18 months from the entry into force of this Regulation, data holders and data users shall become members of a financial data sharing scheme governing access to the customer data in compliance with Article 10.

2. Data holders and data users may become members of more than one financial data sharing schemes.

   Any sharing of data shall be made in accordance with the rules and modalities of a financial data sharing scheme of which both the data user and the data holder are members.

Article 10
Financial data sharing scheme governance and content

1. A financial data sharing scheme shall include the following elements:

   (a) the members of a financial data sharing scheme shall include:

      (i) data holders and data users representing a significant proportion of the market of the product or service concerned, with each side having fair and equal representation in the internal decision-making processes of the scheme as well as equal weight in any voting procedures; where a member is both a data holder and data user, its membership shall be counted equally towards both sides;

      (ii) customer organisations and consumer associations.

   (b) the rules applicable to the financial data sharing scheme members shall apply equally to all the members and there shall be no unjustified favourable or differentiated treatment between members;

   (c) the membership rules of a financial data sharing scheme shall ensure that the scheme is open to participation by any data holder and data user based on objective criteria and that all members shall be treated in a fair and equal manner;

   (d) a financial data sharing scheme shall not impose any controls or additional conditions for the sharing of data other than those provided in this Regulation or under other applicable Union law;

   (e) a financial data sharing scheme shall include a mechanism through which its rules can be amended, following an impact analysis and the agreement of the majority of each community of data holders and data users respectively;

   (f) a financial data sharing scheme shall include rules on transparency and where necessary, reporting to its members;

   (g) a financial data sharing scheme shall include the common standards for the data and the technical interfaces to allow customers to request data sharing in accordance with Article 5(1). The common standards for the data and technical

interfaces that scheme members agree to use may be developed by scheme members or by other parties or bodies;

(h) a financial data sharing scheme shall establish a model to determine the maximum compensation that a data holder is entitled to charge for making data available through an appropriate technical interface for data sharing with data users in line with the common standards developed under point (g). The model shall be based on the following principles:

(i) it should be limited to reasonable compensation directly related to making the data available to the data user and which is attributable to the request;

(ii) it should be based on an objective, transparent and non-discriminatory methodology agreed by the scheme members;

(iii) it should be based on comprehensive market data collected from data users and data holders on each of the cost elements to be considered, clearly identified in line with the model;

(iv) it should be periodically reviewed and monitored to take account of technological progress;

(v) it should be devised to gear compensation towards the lowest levels prevalent on the market; and

(vi) it should be limited to the requests for customer data under Article 2(1) or proportionate to the related datasets in the scope of that Article in the case of combined data requests.

Where the data user is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC of 6 May 2003[42], any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request.

(i) a financial data sharing scheme shall determine the contractual liability of its members, including in case the data is inaccurate, or of inadequate quality, or data security is compromised or the data are misused. In case of personal data, the liability provisions of the financial data sharing scheme shall be in accordance with the provisions in Regulation (EU) 2016/679;

(j) a financial data sharing scheme shall provide for an independent, impartial, transparent and effective dispute resolution system to resolve disputes among scheme members and membership issues, in accordance with the quality requirements laid down by Directive 2013/11/EU of the European Parliament and of the Council[43].

---

42 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) OJ L 124, 20.5.2003, p. 36.

43 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) (OJ L 165, 18.6.2013, p. 63).

2. Membership in financial data sharing schemes shall remain open to new members on the same terms and conditions as those for existing members at any time.

3. A data holder shall communicate to the competent authority of the Member State of its establishment the financial data sharing schemes it is part of, within one month of joining a scheme.

4. A financial data sharing scheme set up in accordance with this Article shall be notified to the competent authority of establishment of the three most significant data holders which are members of that scheme at the time of establishment of the scheme. Where the three most significant data holders are established in different Member States, or where there is more than one competent authority in the Member State of establishment of the three most significant data holders, the scheme shall be notified to all of these authorities which shall agree among themselves which authority shall carry out the assessment referred to in paragraph 6.

5. The notification in accordance with paragraph 4 shall take place within 1 month of setting up the financial data sharing scheme and shall include its governance modalities and characteristics in accordance with paragraph 1.

6. Within 1 month of receipt of the notification pursuant to paragraph 4, the competent authority shall assess whether the financial data sharing scheme's governance modalities and characteristics are in compliance with paragraph 1. When assessing the compliance of the financial data sharing scheme with paragraph 1, the competent authority may consult other competent authorities.

   Upon completion of its assessment, the competent authority shall inform EBA of a notified financial data sharing scheme that satisfies the provisions of paragraph 1. A scheme notified to EBA in accordance with this paragraph shall be recognised in all the Member States for the purpose of accessing data pursuant to Article 5(1) and shall not require further notification in any other Member State.

Article 11

Empowerment for Delegated Act in the event of absence of a financial data sharing scheme

In the event that a financial data sharing scheme is not developed for one or more categories of customer data listed in Article 2(1) and there is no realistic prospect of such a scheme being set up within a reasonable amount of time, the Commission is empowered to adopt a delegated act in accordance with Article 30 to supplement this Regulation by specifying the following modalities under which a data holder shall make available customer data pursuant to Article 5(1) for that category of data:

(a) common standards for the data and, where appropriate, the technical interfaces to allow customers to request data sharing under Article 5(1);

(b) a model to determine the maximum compensation that a data holder is entitled to charge for making data available;

(c) the liability of the entities involved in making the customer data available.

TITLE V
ELIGIBILITY FOR DATA ACCESS AND ORGANISATION

Article 12
Application for authorisation of financial information service providers

1. A financial information service provider shall be eligible to access customer data under Article 5(1) if it is authorised by the competent authority of a Member State.

2. A financial information service provider shall submit an application for authorisation to the competent authority of the Member State of establishment of its registered office, together with the following:

   (a) a programme of operations setting out in particular the type of access to data envisaged;

   (b) a business plan including a forecast budget calculation for the first 3 financial years which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;

   (c) a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures, as well as arrangements for the use of ICT services in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council, which demonstrates that those governance arrangements, control mechanisms and procedures are proportionate, appropriate, sound and adequate;

   (d) a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incident reporting mechanism which takes account of the notification obligations laid down in Chapter III of Regulation (EU) 2022/2554;

   (e) a description of business continuity arrangements including a clear identification of the critical operations, effective ICT business continuity policy and plans and ICT response and recovery plans, and a procedure to regularly test and review the adequacy and efficiency of such plans in accordance with Regulation (EU) 2022/2554;

   (f) a security policy document, including a detailed risk assessment in relation to its operations and a description of security control and mitigation measures taken to adequately protect its customers against the risks identified, including fraud;

   (g) a description of the applicant's structural organisation, as well as a description of outsourcing arrangements;

   (h) the identity of directors and persons responsible for the management of the applicant and, where relevant, persons responsible for the management of the data access activities of the applicant, as well as evidence that they are of good repute and possess appropriate knowledge and experience to access data as determined in this Regulation;

   (i) the applicant's legal status and articles of association;

   (j) the address of the applicant's head office;

(k) where applicable, the written agreement between the financial information service provider and the legal representative evidencing the appointment, the extent of liability and the tasks to be carried out by the legal representative in accordance with Article 13.

For the purposes of the first subparagraph, points (c), (d) and (g) the applicant shall provide a description of its audit arrangements and the organizational arrangements it has set up with a view to taking all reasonable steps to protect the interests of its customers and to ensure continuity and reliability in the performance of its activities.

The security control and mitigation measures referred to in the first subparagraph, point (f), shall indicate how the applicant will ensure a high level of digital operational resilience in accordance with Chapter II of Regulation (EU) 2022/2554, in particular in relation to technical security and data protection, including for the software and ICT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations.

3. Financial information service providers shall hold a professional indemnity insurance covering the territories in which they access data, or some other comparable guarantee, and shall ensure the following:

(a) an ability to cover their liability resulting from non-authorised or fraudulent access to or non-authorised or fraudulent use of data;

(b) an ability to cover the value of any excess, threshold or deductible from the insurance or comparable guarantee;

(c) monitoring of the coverage of the insurance or comparable guarantee on an ongoing basis.

As an alternative to holding a professional indemnity insurance or other comparable guarantee as required in the first sub-paragraph, the undertaking as referred in the previous subparagraph shall hold initial capital of EUR 50 000, which can be replaced by a professional indemnity insurance or other comparable guarantee after it commences its activity as financial information service provider, without undue delay.

4. EBA in cooperation with ESMA and EIOPA shall, after consulting all relevant stakeholders, develop draft regulatory technical standards specifying:

(a) the information to be provided to the competent authority in the application for the authorisation of financial information service providers, including the requirements laid down in paragraph 1, points (a) to (l);

(b) a common assessment methodology for granting authorisation as a financial information service provider, under this Regulation;

(c) what is a comparable guarantee, as referred in paragraph 2, which should be interchangeable with a professional indemnity insurance;

(d) the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee referred to in paragraph 2.

In developing these regulatory technical standards, EBA shall take account of the following:

(a) the risk profile of the undertaking;

(b) whether the undertaking provides other types of services or is engaged in other business;

(c) the size of the activity;

(d) the specific characteristics of comparable guarantees and the criteria for their implementation.

EBA, shall submit those draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date = 9 months after entry into force of this Regulation].

Power is conferred to the Commission to adopt the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation 1093/2015.

In accordance with Article 10 of Regulation (EU 1093/2010, EBA shall review and if appropriate, update these regulatory technical standards.

Article 13
Legal representatives

1. Financial information service providers that do not have an establishment in the Union but that require access to financial data in the Union shall designate, in writing, a legal or natural person as their legal representative in one of the Member States from where the financial information service provider intends to access financial data.

2. Financial information service providers shall mandate their legal representatives to be addressed in addition to or instead of the financial information service provider by the competent authorities on all issues necessary for the receipt of, compliance with and enforcement of this Regulation. Financial information service providers shall provide their legal representative with the necessary powers and resources to enable them to cooperate with the competent authorities and ensure compliance with their decisions.

3. The designated legal representative may be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the financial information service provider.

4. Financial information service providers shall notify the name, address, the electronic mail address and telephone number of their legal representative to the competent authority in the Member State where that legal representative resides or is established. They shall ensure that that information is up to date.

5. The designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union.

Article 14
Granting and withdrawal of authorisation of financial information service providers

1. The competent authority shall grant an authorisation if the information and evidence accompanying the application complies with of the requirements laid down in Article 11(1) and (2). Before granting an authorisation, the competent authority may, where relevant, consult other relevant public authorities.

2. The competent authority shall authorise a third country financial information service provider provided that all the following conditions are met:

   (a) the third country financial information service provider has complied with all conditions laid down in Article 12 and 16;

   (b) the third country financial information service provider has designated a legal representative pursuant to Article 13;

   (c) where the third country financial information service provider is subject to supervision, the competent authority shall seek to put in place an appropriate cooperation arrangement with the relevant competent authority of the third country where the financial information service provider is established, to ensure an efficient exchange of information;

   (d) the third country where the financial information service provider is established is not listed as a non-cooperative jurisdiction for tax purposes under the relevant Union policy or as a high-risk third-country jurisdiction that presents deficiencies in accordance with Commission Delegated Regulation (EU) 2016/1675.[44]

3. The competent authority shall grant an authorisation only if, taking into account the need to ensure the sound and prudent management of a financial information service provider, the financial information service provider has robust governance arrangements for its information service business. This includes a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective procedures to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures. Those arrangements, procedures and mechanisms shall be comprehensive and proportionate to the nature, scale and complexity of the information services provided by the financial information service provider.

4. The competent authority shall grant an authorisation only if the laws, regulations or administrative provisions governing one or more natural or legal persons with which the financial information service provider has close links, or difficulties involved in the enforcement of those laws, regulations or administrative provisions, do not prevent the effective exercise of its supervisory functions.

5. The competent authority shall grant an authorisation only if it is satisfied that any outsourcing arrangements will not render the financial information service provider a letterbox entity or that they are not undertaken as a means to circumvent the provisions of this Regulation.

6. Within 3 months of receipt of an application or, if the application is incomplete, of all of the information required for the decision, the competent authority shall inform the applicant whether the authorisation is granted or refused. The competent authority shall give reasons where it refuses an authorisation.

7. The competent authority may withdraw an authorisation issued to a financial information service provider only if the provider:

---

[44] Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies

(a) does not make use of the authorisation within 12 months, expressly renounces the authorisation or has ceased to engage in business for more than 6 months;

(b) has obtained the authorisation through false statements or any other irregular means;

(c) no longer meets the conditions for granting the authorisation or fails to inform the competent authority on major developments in this respect;

(d) would constitute a risk to consumer protection and the security of data.

The competent authority shall give reasons for any withdrawal of an authorisation and shall inform those concerned accordingly. The competent authority shall make public the withdrawal of an authorisation, in an anonymised version.

Article 15
Register

1. EBA shall develop, operate and maintain an electronic central register which contains the following information:

(a) the authorised financial information service providers.

(b) the financial information service providers that have notified their intention to access data in a Member State other than their home Member State.

(c) the financial data sharing schemes agreed between data holders and data users.

2. The register referred to in paragraph 1 shall only contain anonymised data.

3. The register shall be publicly available on EBA's website and shall allow for easy searching and accessing the information listed.

4. EBA shall enter in the register referred to in paragraph 1 any withdrawal of authorisation of financial information service providers or termination of a financial data sharing scheme.

5. The competent authorities of Member States shall communicate without delay to EBA the information necessary to fulfil its tasks pursuant to paragraphs 1 and 3. Competent authorities shall be responsible for the accuracy of the information specified in paragraphs 1 and 3 and for keeping that information up to date. They shall, where technically possible, transmit this information to EBA in an automated way.

Article 16

Organisational requirements for financial information service providers

A financial information service provider shall comply with the following organisational requirements:

(a) it shall establish policies and procedures sufficient to ensure its compliance, including its managers and employees with its obligations under this Regulation;

(b) it shall take reasonable steps to ensure continuity and regularity in the performance of its activities. To that end the financial information service provider shall employ appropriate and proportionate systems, resources and procedures to ensure the continuity of its critical operations, have in place contingency plans and a procedure to test and review regularly the adequacy and efficiency of such plans;

(c) when relying on a third party for the performance of functions which are critical for the provision of continuous and satisfactory service to customers and the performance of activities on a continuous and satisfactory basis, that it takes reasonable steps to avoid undue additional operational risk. Outsourcing of important operational functions may not be undertaken in such a way as to impair materially the quality of its internal control and the ability of the supervisor to monitor the financial information service provider's compliance with all obligations;

(d) it shall have sound governance, administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment and management, and effective control and safeguard arrangements for information processing systems;

(e) its directors and persons responsible for its management as well as the persons responsible for the management of the data access activities of the financial information service provider are of good repute and possess appropriate knowledge, skills and experience, both individually and collectively, to perform their duties;

(f) it shall establish and maintain effective and transparent procedures for the prompt, fair and consistent monitoring, handling and follow up of a security incident and security related customer complaints, including a reporting mechanism which takes account of the notification obligations laid down in Chapter III of Regulation (EU) 2022/2554;

TITLE VI
COMPETENT AUTHORITIES AND SUPERVISION FRAMEWORK

Article 17
Competent authorities

1. Member States shall designate the competent authorities responsible for carrying out the functions and duties provided for in this Regulation. Member States shall notify those competent authorities to the Commission.

2. Member States shall ensure that the competent authorities designated under paragraph 1 possess all the powers necessary for the performance of their duties.

   Member States shall ensure that those competent authorities have the necessary resources, notably in terms of dedicated staff, in order to comply with their tasks as per the obligations under this Regulation.

3. Member States who have appointed within their jurisdiction more than one competent authority for matters covered by this Regulation shall ensure that those authorities cooperate closely so that they can discharge their respective duties effectively.

4. For financial institutions, compliance with this Regulation shall be ensured by the competent authorities specified in Article 46 of Regulation (EU) 2022/2554 in accordance with the powers granted by the respective legal acts listed in that Article, and by this Regulation.

Article 18
Powers of competent authorities

1. Competent authorities shall have all the investigatory powers necessary for the exercise of their functions. Those powers shall include:

(a) the power to require any natural or legal persons to provide all information that is necessary in order to carry out the tasks of the competent authorities, including information to be provided at recurrent intervals and in specified formats for supervisory and related statistical purposes;

(b) the power to conduct all necessary investigations of any person referred to in point (a) established or located in the Member State concerned where necessary to carry out the tasks of the competent authorities, including the power to:

(i) require the submission of documents;

(ii) examine the data in any form, including the books and records of the persons referred to in point (a) and take copies or extracts from such documents;

(iii) obtain written or oral explanations from any person referred to in point (a) or their representatives or staff, and, if necessary, to summon and question any such person with a view to obtaining information;

(iv) interview any other natural person who agrees to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;

(v) subject to other conditions set out in Union law or in national law, the power to conduct necessary inspections at the premises of the legal persons and at sites other than the private residence of natural persons referred to in point (a), as well as of any other legal person included in consolidated supervision where a competent authority is the consolidating supervisor, subject to prior notification of the competent authorities concerned.

(vi) to enter the premises of natural and legal persons, in line with national law, in order to seize documents and data in any form where a reasonable suspicion exists that documents or data relating to the subject matter of the inspection or investigation may be necessary and relevant to prove a case of breach of provisions of this Regulation;

(vii) to require, insofar as permitted by national law, existing data traffic records held by a telecommunications operator, where there is a reasonable suspicion of a breach and where such records may be relevant to the investigation of a breach of this Regulation;

(viii) to request the freezing or sequestration of assets, or both;

(ix) to refer matters for criminal investigation;

(c) in the absence of other available means to bring about the cessation or the prevention of any breach of this Regulation and in order to avoid the risk of serious harm to the interests of consumers, competent authorities shall be entitled to take any of the following measures, including by requesting a third party or other public authority to implement them:

(i) to remove content or to restrict access to an online interface or to order that a warning is explicitly displayed to customers when they access an online interface;

(ii) to order a hosting service provider to remove, disable or restrict access to an online interface;

(iii) to order domain registries or registrars to delete a fully qualified domain name and to allow the competent authority concerned to record such deletion.

The implementation of this paragraph and the exercise of powers set out therein shall be proportionate and comply with Union and national law, including with applicable procedural safeguards and with the principles of the Charter of Fundamental Rights of the European Union. The investigation and enforcement measures adopted pursuant to this Regulation shall be appropriate to the nature and the overall actual or potential harm of the infringement.

2. Competent authorities shall exercise their powers to investigate potential breaches of this Regulation, and impose administrative penalties and other administrative measures provided for in this Regulation, in any of the following ways:

(a) directly;

(b) in collaboration with other authorities;

(c) by delegating powers to other authorities or bodies;

(d) by having recourse to the competent judicial authorities of a Member State.

Where competent authorities exercise their powers by delegating to other authorities or bodies in accordance withpoint (c), the delegation of power shall specify the delegated tasks, the conditions under which they are to be carried out, and the conditions under which the delegated powers may be revoked. The authorities or bodies to which the powers are delegated shall be organised in such a manner that conflicts of interest are avoided. Competent authorities shall oversee the activity of the authorities or bodies to which the powers are delegated.

3. In the exercise of their investigatory and sanctioning powers, including in cross border cases, competent authorities shall cooperate effectively with each other and with the authorities from any sector concerned as applicable to each case and in accordance with national and Union law, to ensure the exchange of information and the mutual assistance necessary for the effective enforcement of administrative sanctions and administrative measures.

Article 19

Settlement agreements and expedited enforcement procedures

1. Without prejudice to Article 20, Member States may lay down rules enabling their competent authorities to close an investigation concerning an alleged breach of this Regulation, following a settlement agreement in order to put an end to the alleged breach and its consequences before formal sanctioning proceedings are started.

2. Member States may lay down rules enabling their competent authorities to close an investigation concerning an established breach through an expedited enforcement procedure in order to achieve a swift adoption of a decision aiming at imposing an administrative sanction or administrative measure.

The empowerment of competent authorities to settle or open expedite enforcement procedures does not affect the obligations upon Member States under Article 20.

3. Where Member States lay down the rules referred to in paragraph 1, they shall notify the Commission of the relevant laws, regulations and administrative provisions regulating the exercise of powers referred to in that paragraph and shall notify it of any subsequent amendments affecting those rules.

Article 20
Administrative penalties and other administrative measures

1. Without prejudice to the supervisory and investigative powers of competent authorities listed in Article 18, Member States shall, in accordance with national law, provide for competent authorities to have the power to take appropriate administrative penalties and to take other administrative measures in relation to the following infringements:

   (a) infringements of Articles 4, 5 and 6;

   (b) infringements of Articles 7 and 8;

   (c) infringements of Article 9 and 10;

   (d) infringements of Articles 13 and 16;

   (e) infringements of Article 28.

2. Member States may decide not to lay down rules on administrative sanctions and administrative measures applicable to breaches of this Regulation which are subject to sanctions under national criminal law. In such a case, Member States shall notify the Commission of the relevant criminal law provisions and any subsequent amendments thereto.

3. Member States shall, in accordance with national law, ensure that competent authorities have the power to impose the following administrative penalties and other administrative measures in relation to the infringements referred to in paragraph 1:

   (a) a public statement indicating the natural or legal person responsible and the nature of the infringement;

   (b) an order requiring the natural or legal person responsible to cease the conduct constituting the infringement and to desist from a repetition of that conduct;

   (c) the disgorgement of the profits gained or losses avoided due to the infringement insofar as they can be determined;

   (d) a temporary suspension of the authorisation of a financial information service provider;

   (e) a maximum administrative fine of at least twice the amount of the profits gained or losses avoided because of the infringement where those can be determined, even if such fine exceeds the maximum amounts set out in this paragraph, point (f), as regards natural persons, or in paragraph 4 as regards legal persons;

   (f) in the case of a natural person, maximum administrative fines of up to EUR 25 000 per infringement and up to a total of EUR 250 000 per year, or, in the Member States whose official currency is not the euro, the corresponding value in the official currency of that Member State on ... [OP please insert the date of entry into force of this Regulation].

(g) a temporary ban of any member of the management body of the financial information service provider**,** or any other natural person who is held responsible for the infringement, from exercising management functions in financial information service providers;

(h) in the event of a repeated infringement of the articles referred to in paragraph 1, a ban of at least 10 years for any member of the management body of a financial information service provider**,** or any other natural person who is held responsible for the infringement, from exercising management functions in a financial information service provider.

4. Member States shall, in accordance with national law, ensure that competent authorities have the power to impose, in relation to the infringements referred to in paragraph 1 committed by legal persons, maximum administrative fines of:

(a) up to EUR 50 000 per infringement and up to a total of EUR 500 000 per year, or, in the Member States whose official currency is not the euro, the corresponding value in the official currency of that Member State on ... [OP please insert the date of entry into force of this Regulation];

(b) 2% of the total annual turnover of the legal person according to the last available financial statements approved by the management body;

Where the legal person referred to in the first subparagraph is a parent undertaking or a subsidiary of a parent undertaking which is required to prepare consolidated financial statements in accordance with Article 22 of Directive 2013/34/EU of the European Parliament and of the Council[45], the relevant total annual turnover shall be the net turnover or the revenue to be determined in accordance with the relevant accounting standards, according to the consolidated financial statements of the ultimate parent undertaking available for the latest balance sheet date, for which the members of the administrative, management and supervisory body of the ultimate undertaking have responsibility.

5. Member States may empower competent authorities to impose other types of administrative penalties and other administrative measures in addition to those referred to in paragraphs 3 and 4 and may provide for higher amounts of administrative pecuniary fines than those laid down in those paragraphs.

Member States shall notify to the Commission the level of such higher penalties, and any subsequent amendments thereto.

Article 21
Periodic penalty payments

1. Competent authorities shall be entitled to impose periodic penalty payments on legal or natural persons for an ongoing failure to comply with any decision, order, interim

[45] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

measure, request, obligation or other administrative measure adopted in accordance with this Regulation.

A periodic penalty payment referred to in the first subparagraph shall be effective and proportionate and shall consist of a daily amount to be paid until compliance is restored. They shall be imposed for a period not exceeding 6 months from the date indicated in the decision imposing the periodic penalty payments.

Competent authorities shall be entitled to impose the following periodic penalty payments which may be adjusted depending on the seriousness of the breach and the needs of the sector:

(a) 3% of the average daily turnover in the case of a legal person;

(b) EUR 30 000 in the case of a natural person.

2. The average daily turnover referred to in paragraph 1, third subparagraph, point (a), shall be the total annual turnover, divided by 365.

3. Member States may provide for higher amounts of periodic penalty payments than those laid down in paragraph 1, third subparagraph.

Article 22

Circumstances to be considered when determining administrative penalties and other administrative measures

1. Competent authorities, when determining the type and level of administrative penalties or other administrative measure, shall take into account all relevant circumstances in order to ensure that such sanctions or measures are effective and proportionate. Those circumstances shall include, where appropriate:

(a) the gravity and the duration of the breach;

(b) the degree of responsibility of the legal or natural person responsible for the breach;

(c) the financial strength of the legal or natural person responsible for the breach, as indicated, among other things, by the total annual turnover of the legal person, or the annual income of the natural person responsible for the breach;

(d) the level of profits gained or losses avoided by the legal or natural person responsible for the breach, if such profits or losses can be determined;

(e) the losses for third parties caused by the breach, if such losses can be determined;

(f) the disadvantage resulting to the legal or natural person responsible for the breach from the duplication of criminal and administrative proceedings and penalties for the same conduct;

(g) the impact of the breach on the interests of customers;.

(h) any actual or potential systemic negative consequences of the breach;

(i) the complicity or organised participation of more than one legal or natural person in the breach;

(j) previous breaches committed by the legal or natural person responsible for the breach;

(k) the level of cooperation of the legal or natural person, responsible for the breach, with the competent authority;

(l) any remedial action or measure undertaken by the legal or natural person responsible for the breach to prevent its repetition.

2. Competent authorities that use settlement agreements or expedited enforcement procedures pursuant to Article 19 shall adapt the relevant administrative penalties and other administrative measures provided for in Article 20 to the case concerned to ensure the proportionality thereof, in particular by considering the circumstances listed in paragraph 1.

Article 23
Professional secrecy

1. All persons who work or who have worked for the competent authorities, as well as experts acting on behalf of the competent authorities, are bound by the obligation of professional secrecy.

2. The information exchanged in accordance with Article 26 shall be subject to the obligation of professional secrecy by both the sharing and recipient authority to ensure the protection of individual and business rights.

Article 24
Right of appeal

1. Decisions taken by the competent authorities pursuant to this Regulation, may be contested before the courts.

2. Paragraph 1 shall apply also in respect of a failure to act.

Article 25
Publication of decisions of competent authorities

1. Competent authorities shall publish on their website all decisions imposing an administrative penalty or administrative measure on legal and natural persons, for breaches of this Regulation, and where applicable, all settlement agreements. The publication shall include, a short description of the breach, the administrative penalty or other administrative measure imposed, or, where applicable, a statement about the settlement agreement. The identity of the natural person subject to the decision imposing an administrative penalty or administrative measure shall not be published.

Competent authorities shall publish the decision and the statement referred to in paragraph 1 immediately after the legal or natural person subject to the decision has been notified of that decision or the settlement agreement has been signed.

2. By derogation from paragraph 1, where the publication of the identity or other personal data of the natural person is deemed necessary by the national competent authority to protect the stability of the financial markets or, to ensure the effective enforcement of this Regulation, including in the case of public statements referred to in Article 20(3) point (a), or temporary bans referred to in Article 20(3) point (g), the national competent authority may publish also the identity of the persons or personal data, provided that it justifies such a decision and that the publication is limited to the personal data that is strictly necessary to protect the stability of the financial markets or to ensure the effective enforcement of this Regulation.

3. Where the decision imposing an administrative penalty or other administrative measure is subject to appeal before the relevant judicial or other authority, competent authorities shall also publish on their official website, without delay, information on the appeal and any subsequent information on the outcome of such an appeal insofar as it concerns legal persons. Where the appealed decision concerns natural persons and the derogation under paragraph 2 is not applied, competent authorities shall publish information on the appeal only in an anonymised version.

4. Competent authorities shall ensure that any publication made in accordance with this Article remains on their official website for a period of at least 5 years. Personal data contained in the publication shall be kept on the official website of the competent authority only if an annual review shows the continued need to publish that data to protect the stability of the financial markets or to ensure the effective enforcement of this Regulation, and in any event for no longer than 5 years.

Article 26

Cooperation and exchange of information between competent authorities

1. Competent authorities shall cooperate with each other and with other relevant competent authorities designated under Union or national law applicable to financial institutions for the purposes of this Regulation carrying out the duties of the competent authorities.

2. The exchange of information between competent authorities and the competent authorities of other Member States responsible for the authorisation and supervision of financial information service providers shall be allowed for the purposes of carrying out their duties under this Regulation.

3. Competent authorities exchanging information with other competent authorities under this Regulation may indicate at the time of communication that such information must not be disclosed without their express agreement, in which case such information may be exchanged solely for the purposes for which those authorities gave their agreement.

4. The competent authority shall not transmit information shared by other competent authorities to other bodies or natural or legal persons without the express agreement of the competent authorities which disclosed it and solely for the purposes for which those authorities gave their agreement, except in duly justified circumstances. In this last case, the contact point shall immediately inform the contact point that sent the information.

5. Where obligations under this Regulation concern the processing of personal data, competent authorities shall cooperate with the supervisory authorities established pursuant to Regulation (EU) 2016/679.

Article 27

Settlement of disagreements between competent authorities

1. Where a competent authority of a Member State considers that, in a particular matter, cross-border cooperation with competent authorities of another Member State as referred to in Articles 28 or 29 of this Regulation does not comply with the relevant conditions set out in those provisions, it may refer the matter to EBA and may request its assistance in accordance with Article 19 of Regulation (EU) No 1093/2010.

2. Where EBA has been requested to provide assistance pursuant to paragraph 1, it shall take a decision under Article 19(3) of Regulation (EU) No 1093/2010 without undue delay. EBA may also, on its own initiative, assist the competent authorities in reaching an agreement in accordance with Article 19(1), second subparagraph of that Regulation. In either case, the competent authorities involved shall defer their decisions pending resolution of the disagreement pursuant to Article 19 of Regulation (EU) No 1093/2010.

TITLE VII
CROSS BORDER ACCESS TO DATA

Article 28
Cross-border access to data by financial information service providers

1. Financial information service providers and financial institutions shall be allowed to have access to the data listed in Article 2(1) of Union customers held by data holders established in the Union, pursuant to the freedom to provide services or the freedom of establishment.

2. A financial information service provider wishing to have access to the data listed in Article 2(1) of this Regulation for the first time in a Member State other than its home Member State, in the exercise of the right of establishment or the freedom to provide services, shall communicate the following information to the competent authorities in its home Member State:

   (a) the name, the address and, where applicable, the authorisation number of the financial information service provider;

   (b) the Member State(s) in which it intends to have access to the data listed in Article 2(1);

   (c) the type of data it wishes to have access to;

   (d) the financial data sharing schemes it is a member.

   Where the financial information service provider intends to outsource operational functions of data access to other entities in the host Member State, it shall inform the competent authorities of its home Member State accordingly.

3. Within 1 month of receipt of all of the information referred to in paragraph 1 the competent authorities of the home Member State shall send it to the competent authorities of the host Member State.

4. The financial information service provider shall communicate to the competent authorities of the home Member State without undue delay any relevant change regarding the information communicated in accordance with paragraph 1, including additional entities to which activities are outsourced in the host Member States in which it operates. The procedure provided for under paragraphs 2 and 3 shall apply.

Article 29
Reasons and communication

Any measure taken by the competent authorities pursuant to Article 18 or Article 28 involving penalties or restrictions on the exercise of the freedom to provide services or the freedom of establishment shall be properly justified and communicated to the financial information service provider concerned.

TITLE VIII

FINAL PROVISIONS

Article 30
Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt the delegated act referred to in Article 11, shall be conferred on the Commission for a period of XX months from … [OP please insert: date of entry into force of this Regulation]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the XX-month period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of powers referred to in Article 11, may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts signated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 11, shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months on the initiative of the European Parliament or of the Council.

Article 31
Evaluation of this Regulation and report on access to financial data

1. By [OP please insert the date = 4 years after the date of entry into application of this Regulation, the Commission shall carry out an evaluation of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee. That evaluation shall assess, in particular:

   (a) other categories or sets of data to be made accessible;

   (b) the exclusion from the scope of certain categories of data and entities;

   (c) changes in contractual practices of data holders and data users and the operation of financial data sharing schemes;

(d) the inclusion of other types of entities to those entities granted the right of access to data.

(e) the impact of compensation on the ability of data users to participate in financial data sharing schemes and access data from data holders.

2. By [OP please insert the date = 4 years after the date of entry into force of this Regulation, the Commission shall submit a report to the European Parliament and the Council assessing the conditions for access to financial data applicable to account information service providers under this Regulation and under Directive (EU) 2015/2366. The report can be accompanied, if deemed appropriate, by a legislative proposal.

Article 32
Amendment to Regulation (EU) No 1093/2010

In Article 1(2) of Regulation (EU) No 1093/2010, the first subparagraph is replaced by the following:
'The Authority shall act within the powers conferred by this Regulation and within the scope of Directive 2002/87/EC, Directive 2008/48/EC*, Directive 2009/110/EC, Regulation (EU) No 575/2013**, Directive 2013/36/EU***, Directive 2014/49/EU****, Directive 2014/92/EU*****, Directive (EU) 2015/2366******, Regulation (EU) 2023/1114 (*******), Regulation (EU) 2024/…/EU (********) of the European Parliament and of the Council and, to the extent that those acts apply to credit and financial institutions and the competent authorities that supervise them, within the relevant parts of Directive 2002/65/EC, including all directives, regulations, and decisions based on those acts, and of any further legally binding Union act which confers tasks on the Authority. The Authority shall also act in accordance with Council Regulation (EU) No 1024/2013*********.

* Directive 2008/48/EC Of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ L 133, 22.5.2008, p. 66).

** Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

*** Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

**** Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes (OJ L 173, 12.6.2014, p. 149).

***** Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (OJ L 257, 28.8.2014, p. 214).

****** Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

******* Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023, p. 40).

******** Regulation (EU) 2024/… of the European Parliament and of the Council of … on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) 1095/2010 and (EU) 2022/2554 and Directive (EU) 2019/1937 (OJ L ..., ..., p.).

********* Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).'

Article 33
Amendment to Regulation (EU) No 1094/2010

In Article 1(2) of Regulation (EU) No 1094/2010, the first subparagraph is replaced by the following:

'The Authority shall act within the powers conferred by this Regulation and within the scope of Regulation (EU) 2024/…/EU (*), of Directive 2009/138/EC with the exception of Title IV thereof, of Directive 2002/87/EC, Directive (EU) 2016/97 (**) and Directive (EU) 2016/2341 (***) of the European Parliament and of the Council, and, to the extent that those acts apply to financial information services providers, insurance undertakings, reinsurance undertakings, institutions for occupational retirement provision and insurance intermediaries, within the relevant parts of Directive 2002/65/EC, including all directives, regulations, and decisions based on those acts, and of any further legally binding Union act which confers tasks on the Authority.'

---

* Regulation (EU) 2024/… of the European Parliament and of the Council of … on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010, (EU) 1094/2010 and (EU) 2022/2554 and Directive (EU) 2019/1937 (OJ L …, ..., p.).

** Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26, 2.2.2016, p. 19).

*** Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (OJ L 354, 23.12.2016, p. 37).

Article 34
Amendment to Regulation (EU) No 1095/2010

In Article 1(2) of Regulation (EU) No 1095/2010, the first subparagraph is replaced by the following:
'The Authority shall act within the powers conferred by this Regulation and within the scope of Directives 97/9/EC, 98/26/EC, 2001/34/EC, 2002/47/EC, 2004/109/EC, 2009/65/EC, Directive 2011/61/EU of the European Parliament and of the Council*, Regulation (EC) No 1060/2009 and Directive 2014/65/EU of the European Parliament and of the Council**, Regulation (EU) 2017/1129 of the European Parliament and of the Council***, Regulation (EU) 2023/1114of the European Parliament and of the Council**** Regulation (EU) 2024/… of the European Parliament and of the Council***** and to the extent that those acts apply to firms providing investment services or to collective investment undertakings marketing their units or shares, issuers or offerors of crypto-assets, persons seeking admission to trading or crypto-asset service providers, financial information service providers and the competent authorities that supervise them, within the relevant parts of, Directives 2002/87/EC and

2002/65/EC, including all directives, regulations, and decisions based on those acts, and of any further legally binding Union act which confers tasks on the Authority.

---

* Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).

** Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

*** Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC (OJ L 168, 30.6.2017, p. 12).

**** Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023, p.40).'

***** Regulation (EU) 2024/… of the European Parliament and of the Council of … on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010 and (EU) 2022/2554 and Directive (EU) 2019/1937 (OJ L ..., ..., p.).

Article 35
Amendment to Regulation (EU) 2022/2554

Article 2(1) of Regulation (EU) 2022/2554 is amended as follows:

(1) In point (u), the punctuation mark "."is replaced by ";"

(2) the following point (v) is added:

""(v) financial information service providers.""

Article 36
Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [OP please insert the date = 24 months after the date of entry into force of this Regulation]. However, Articles 9 to 13 shall apply from [OP please insert the date = 18 months after the date of entry into force of this Regulation].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*