Payment services: revised rules to improve consumer protection and competition in electronic payments

Brussels, 28 June 2023

Background

What is PSD2? Why is it being reviewed?

The second Payment Services Directive (PSD2), adopted in 2015, sets out the rules for all retail payments in the EU, euro and non-euro, domestic and cross-border. The first Payment Services Directive (PSD1), adopted in 2007, established a harmonised legal framework for the creation of an integrated EU payments market. PSD2 addressed barriers to new types of payment services and improved the level of consumer protection and security. It aimed to:

- ensure a level playing field between incumbent and new providers of card, internet and mobile payments;
- increase the efficiency, transparency and choice of payment instruments for payment service users (consumers and merchants);
- facilitate the provision of card, internet and mobile payment services across borders within the EU;
- help innovative payment services to reach a broader market; and
- ensure a high-level protection for payment service users across all Member States.

The Commission was required to evaluate PSD2, in particular on charges, scope, thresholds and access to payment systems. The evaluation took place in 2022, including advice from the European Banking Authority (EBA), a general and targeted public consultation and a report from an independent consultant. Following the evaluation the Commission decided to propose amendments to PSD2, accompanied by an impact assessment.

What are the main changes being proposed by this revision?

These amendments represent an evolution not a revolution of the EU payments framework. The amendments will improve the functioning of EU payment markets by:

- strengthening measures to combat payment fraud;
- allowing non-bank payment service providers (PSPs) access to all EU payment systems, with appropriate safeguards, and giving them a right to have a bank account;
- improving the functioning of open banking, especially as regards the performance of data interfaces, removing obstacles to open banking services and consumer control over their data access permissions;
- reinforcing the enforcement powers of national competent authorities and facilitating implementation of the rules clarifying various elements;
- further improving consumer information and rights;
- improving the availability of cash;
- merging the legal frameworks applicable to electronic money and to payment services.

Why are electronic retail payments important?

As highlighted in the Commission's Retail Payments Strategy of 2020, effective and efficient retail payment systems are essential for the smooth running of the economy and for private economic operations between individuals. They are equally important for the EU's open strategic autonomy. The retail payments sector is at the forefront of digital innovation in financial services and multiple developments (contactless payments, instant payments etc.) have taken place in recent years. Electronic payments in the EU are in constant growth, reaching €240 trillion in value in 2021 (compared with €184.2 trillion in 2017). The COVID-19 pandemic accelerated this trend. The

Strategy announced the launch of a comprehensive review of the application and impact of PSD2, "*which should include an overall assessment of whether it is still fit for purpose, taking into account market developments*".

What did the evaluation of the PSD2 find?

The evaluation concluded that PSD2 has had varying degrees of success in meeting its objectives. One area of clear positive impact has been that of fraud prevention, via the introduction of Strong Customer Authentication (SCA), which has already had a significant impact in reducing fraud. PSD2 has also been particularly effective in increasing the efficiency, transparency and choice of payment instruments for consumers, given the new means of payment that have sprung up since its introduction. However, the evaluation finds that there remains an unlevel playing field between payment service providers, due partly to the lack of direct access by non-bank Payment Service Providers (PSPs) to certain key systems that are necessary to finalise payments. Open banking (i.e. the secure sharing of financial data between banks and third-party service providers) was a major innovation of PSD2. In spite of the emergence of many new non-bank providers on the market offering open banking services, there has been mixed success in its uptake. Obstacles to data access by account information service providers (services which collect and consolidate information on the different bank accounts of a consumer in a single place) and payment initiation service providers (services which establish a payment link between the payer and the online merchant) still remain. While cross-border provision of payment services is increasing, many payment systems (especially debit card systems) remain largely national.

Fraud and liability

What is the Commission's approach on payment fraud?

The Commission accords utmost importance to the issue of payment fraud. It believes that any changes to the PSD2 liability framework should contribute to reducing fraud, without creating moral hazard (if the consumers believe that they will always be compensated).

New types of fraud have emerged for which PSD2 is not equipped. For example, PSD3 will go beyond the PSD2 tackling new types of fraud like "spoofing" (impersonation fraud), which blur the distinction between unauthorised and authorised transactions, since the consent given by the customer to authorise a transaction is subjected to manipulative techniques by the fraudster, who for example uses the telephone number of email address of the bank. Prevention mechanisms such as SCA have been insufficient to prevent such frauds until now. The IBAN/name check (where a payment is only completed after verification by the bank that the name on the account 'matches' the IBAN linked to that name) can help prevent these types of fraud.

Given the continued existence of social engineering fraud, in which fraudsters manipulate a victim to send funds to an illegitimate payee, the Commission is proposing additional anti-fraud measures regarding both fraud prevention and redress.

The new proposed prevention measures include:

- An extension to all credit transfers of IBAN/name matching verification services. These have been proposed by the Commission for instant payments in Euro. All consumers should benefit from them, for both regular and instant credit transfers;
- A legal basis for PSPs to share fraud-related information between themselves in full respect of GDPR (via dedicated IT platforms);
- The strengthening of transaction monitoring;
- An obligation by PSPs to carry out education actions to increase awareness of payments fraud among their customers and staff; and
- An extension of refund rights of consumers in certain situations.

Under what circumstances will victims of fraud be entitled to a refund?

The proposal enables the granting of refund rights in two situations: for consumers who suffered damages caused by the failure of the IBAN/name verification service to detect a mismatch between the name and IBAN of the payee, and for consumers falling victim of a "spoofing" fraud where the fraudster contacts the consumer pretending to be an employee of the consumer's bank, tricking the consumer into carrying out some actions causing financial damages to the consumer. Victims of "spoofing" fraud can be entitled to claim damages from their PSP for the full amount of the fraudulent transaction, subject to conditions including filing a police report and notification to their PSP without undue delay. Refund would not be allowed in cases of "gross negligence" by the victim, including falling victim more than once to the same kind of fraud, and the "spoofing" would have to be convincing, for example replicating the bank's exact email address or phone number.

How will the new IBAN/name verification service work?

The Commission proposal on instant payments proposed a new service which identifies, and signals to the payer before the completion of a payment order, of discrepancies between the name and unique identifier of a payee for instant credit transfers denominated in euro. To achieve a coherent framework for all credit transfers, the new proposal will extend this service to all credit transfers in the EU. This service will have to be provided free of charge to consumers. The PSP of the payee will be required, at the request of the PSP of the payer, to verify whether the unique identifier (IBAN number) and the name of the payee as provided by the payer match. Where these do not match, the PSP of the payer will be obliged to notify the payer of any such discrepancy before the payer finalises the payment order. The payer remains free to decide whether to authorise a credit transfer where a discrepancy was detected and notified. The payer will have the right to opt out of the service.

What is being done to improve Strong Customer Authentication?

PSD2 made payments safer for payers through the introduction of SCA, which involves at least a two-phase authentication of payer's identities. This proposal will:

- Clarify in which circumstances certain types of transactions, such as merchant-initiated transactions, or transactions for which payment orders are placed by the payer with modalities other than the use of electronic platforms or devices, may be exempt of the obligation to apply SCA, while also introducing safeguards to ensure that payers remain nevertheless protected from fraud.
- Clarify that, for remote payments, the specific amount and the payee must be explicitly linked to the transaction which is to be authenticated by the payer.
- Simplify the application of SCA in respect of payment account information services. Banks holding payment accounts will only apply SCA for the first access to payment account data by open banking account information service providers unless there are reasonable grounds to suspect fraud. Account information service providers will then be responsible for SCA for subsequent data accesses.
- Strengthen the use for payments of digital passthrough wallets (where a virtual payment card is stored on the wallet), by requiring that SCA must be performed at the moment of the enrolment of a payment instrument in the wallet under the responsibility of the PSPs that issued that instrument.
- Require payment services providers to ensure that all users can benefit from methods to perform SCA which are adapted to their needs and situations and, in particular, that those methods do not depend on one single technology, device or mechanism, for instance on the possession of a smartphone.

Consumer rights and information

What new information requirements is the Commission proposing for payment service providers?

There are three new requirements:

- **More transparency for credit transfers and money remittances from the EU to third countries:** For credit transfers and money remittances from the EU to third countries, the Commission is proposing an obligation to inform the payment service user about the estimated charges for currency conversion. The method of expressing these charges will be aligned with current information requirements for intra-EU transactions for card-based transactions, i.e. expressed as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the ECB. This provision will allow users to better compare currency conversion charges, which is necessary to take an informed decision when choosing their PSP. PSPs will also be required to provide an estimated time for the funds to be received by the payee's payment service provider in a third country.
- **More transparency for payment account statements:** PSD2 does not regulate whether the legal name or commercial name of a payee (such as a merchant) should be used on payment account statements. This can cause confusion among users who may not recognise the name which appears on their statement and incorrectly suspect a fraudulent transaction. The proposal stipulates that PSPs must include in payment account statements the information needed to unambiguously identify the payee, such as a reference to the payee's commercial trade name.
- **More transparency for ATM charges**: In order to increase the transparency of ATM charges for payment service users, PSPs will be obliged to provide users with information on all applicable charges made by other ATM operators in the same Member State, so that the user

knows in advance what total charges will be applied, regardless of the ATM used.

How will the Commission ensure that consumers are adequately protected when funds are blocked on a payment card?

When a payment card is used for a payment of an initial, estimated amount (for example at a petrol station, a hotel or a car rental), funds are normally blocked on the card by the payer's PSP after consent has been given by the payer. The blocked funds are unavailable to the user for spending until released, which can cause financial difficulties. Evidence collected by the Commission shows that the blocked funds may be disproportionate or unreasonably high compared with the final amount, when known. The release of unused blocked funds can take up to several weeks or even require an explicit request from the payer to be released. The Commission is proposing changes to speed up the pay-out of unused blocked funds and to require that the blocked amount be proportionate to the expected final amount.

What does the proposal do to improve the availability of cash?

Currently, a retailer may provide cash to a customer without being licensed and supervised as a PSP, but only in association with a purchase ("cashback"). In order to further increase access to cash, the proposal allows retailers, if they wish, to offer a cash provision service even in the absence of a purchase by a customer, without having to obtain a license or being an agent of a Payment Institution. This is associated with some conditions, such as a cap of €50 per withdrawal (to guarantee fair competition with ATMs and to ensure that shops do not rapidly run out of cash) and an obligation to disclose any possible fees charged.

The distribution of cash via ATMs generally requires a license, but there is an exclusion in PSD2 for certain ATM operators, which has proven difficult to apply in practice. It is therefore proposed to more explicitly allow certain ATM operators (those which do not service payment accounts) to operate ATMs without licensing. This should encourage more provision of ATMs. Transparency on fees will be required.

What does the initiative do to clarify the interaction between payments and General Data Protection Regulation?

The proposal introduces clarifications and changes aimed at ensuring consistency with GDPR, namely by:

- clarifying that, for payment services providers, the permission to access and process personal data of their customers is limited to the data necessary for the provision of the specific payment services which were contracted with the customers;
- strengthening the protection of payment service users' data in the context of Open Banking services, by limiting the data which can be accessed by Third-Party Providers to the minimum necessary for delivering the Payment Initiation or Account information services required by the user (data minimisation) and by requiring banks to provide a "dashboard" allowing users to visualize and manage all permissions that they grant to third-party providers for accessing their payment account data;
- clarifying that the processing of payment transactions may necessitate that payment service providers be able to process personal data related to the parties of a payment transactions, including personal data designated as "special categories of data" under GDPR.

Improvements to Open Banking

What is open banking, and what did PSD2 provide for in this area?

Open banking is the process by which account information service providers (AISPs) and payment initiation service providers (PISPs) offer (or enable other parties to provide) value added services to users by accessing – upon user request - their account data held by banks and other payment account providers. Although open banking existed before PSD2, it took place in a largely unregulated environment. PSD2 gave open banking a stable regulatory framework. It imposed an obligation on banks to facilitate access to payments data for AISPs and PISPs via a secure interface. The value-added services include, for example, services giving consumers a global view on their financial situation and an analysis of their spending patterns, expenses and financial needs.

What are the changes being made to the functioning of open banking?

This initiative makes a number of targeted amendments to the open banking framework to improve its functioning, while avoiding radical changes which might destabilise the market or generate significant further implementation costs. New substantial requirements for dedicated data access interfaces are proposed. A list of prohibited obstacles to data access is introduced. Banks will no

longer need to permanently maintain (unless where exempted) two data access interfaces (a dedicated one and its "fall-back"). Contingency data access possibilities will remain available to open banking providers in specific and temporary circumstances in order to secure their business continuity in case the primary interface is down. Banks and other payment account providers will be required to set up a "dashboard" allowing consumers of open banking services to see at a glance what data access rights they have granted and to whom, and to withdraw access via this tool.

What is done to protect the business continuity of open banking providers?

The Commission grants utmost importance to the continuous access by open banking providers (AISPs and PISPs) to the data which they need to service the clients having given them such data access permission. The Commission considers that open banking data access and exchange is best ensured through state-of-the-art dedicated interfaces. However, if a bank's open banking interface is down, causing providers potential harmful data access disruption, and if the bank cannot rapidly offer an effective alternative solution to the providers, they can then request their national authority to be allowed to use another interface (such as the one that banks use for their customers) until the provider's dedicated interface is restored to functioning. To ensure that there is no disruption in their business, the open banking providers can use the alternative interface as long as the authorities do not respond to their request to use it. The authority can set banks a deadline for this, with the possibility of penalties if the bank fails to restore the dedicated interface by the deadline. Open banking providers retain the right to claim damages from the bank for loss of business, in line with civil law.

How do these changes relate to the Commission's proposal on financial data access?

The Commission is also presenting a legislative proposal on financial data access (FIDA), extending the obligation to provide access to financial data beyond payment account data. The Commission examined the possibility of transferring the legal framework for account information service providers (AISPs) from PSD to the future FIDA framework. Although such a transfer would ultimately make sense, given the nature of AISPs' business, there would be a significant risk of disruption and data access rights interruptions for these market operators if such a transfer were carried out prematurely i.e. before the existence of a "scheme", which will be a pre-requisite for FIDA to take place. There is currently no such scheme in the market. Creation of a private contractual scheme in the payments sector (the SEPA Payment Account Access Scheme – SPAA) is currently being discussed by market participants, which is however outside the FIDA framework. It is therefore deemed preferable to have a staggered approach and provide for such transfer when the FIDA framework will be up and running and when conditions for a smooth transfer are considered appropriate.

Competition and level playing field

What competition issues have been encountered by non-bank Payment Service Providers?

Payment institutions and e-money institutions (PIs and EMIs) have grown in numbers and importance since the entry into force of PSD2. PIs and EMIs need to have an account with a commercial bank to obtain a license. Offering payment services also requires having access to key payment infrastructures that execute and settle payments. However, commercial banks often refuse to open an account for them or close their existing bank account because of concerns over matters such as anti-money laundering controls. Furthermore, the Settlement Finality Directive, as it stands, prevents access by PIs and EMIs to payment infrastructures which have been designated under that Directive, by not mentioning them as possible participants in such systems. This forces PIs and EMIs to rely even more on commercial banks, establishing a structural dependency on banks and an unlevel playing field, as banks are competitors of PIs and EMIs for the provision of payment services.

What does the initiative do to facilitate access of non-bank payment service providers to a bank account?

Requirements on banks regarding bank account services to non-bank PSPs will be considerably toughened, with a stronger requirement on banks to explain access refusal, covering also withdrawal of service. Justification for refusal must be based on the specific situation of that PI, including serious grounds to suspect illegal activities being pursued by or via the PI, or a business model or risk profile which causes serious risks to the credit institution. The latter will be able to appeal to a national authority against any decision of a bank not to open or to close an account. In addition to commercial banks, central banks will also be allowed to provide account services to non-bank PSPs, at their discretion.

How will payment institutions get better access to payment systems?

The proposal includes PIs as possible participants in designated payment systems. There will be reinforced rules on the admission of PIs as participants in payment systems, with an obligation on

payment system operators to carry out appropriate risk assessments. Given the urgency of introducing this indispensable level-playing-field measure, Member States are given 6 months to transpose it in their national law.

Simplification and enforcement

What is changing as regards e-money institutions?

The E-Money Directive (EMD) contains rules on authorisation and supervision of e-money institutions (EMIs). PSD2 contains rules on authorisation and supervision of payment institutions (PIs) and establishes conditions for the relationship between all payment service providers (including EMIs) and payment service users. The legal framework applicable to EMIs and PIs is already reasonably consistent. However, the licensing requirements and some other key concepts governing the e-money business, such as issuance of e-money, e-money distribution and redeemability, are quite distinct as compared to the services provided by payment institutions. Supervisory authorities have experienced practical difficulties in clearly delineating the two regimes and in distinguishing e-money products/services from payment services offered by payment institutions. Therefore, a merger of the two regimes is proposed, bringing them together in one single piece of legislation and harmonising them to the extent possible. This will ensure a higher degree of harmonisation, simplification and consistent application of the legal requirements for PIs and former EMIs.

What is being done to enhance enforcement of the rules?

Most of the payment rules applicable to PSPs will be contained in a directly applicable regulation. Multiple clarifications are introduced in the legislation on points which were previously unclear or ambiguous. They include the definition of "funds" "payment account" and "payment instrument" and detailed rules on how competent authorities must enforce the rules, including a list of breaches for which specific sanctions must be in place. Specific enforcement provisions for open banking rules are provided for, given the importance of national supervision for the smooth functioning of open banking. The European Banking Authority will be granted new intervention powers, providing extra protection for consumers.

Framework for Financial Data Access

Why is the framework for financial data access needed?

- Some data users are already accessing some types of customer data covered through technical interfaces that data holders have put in place for their customers. However, this way of accessing customers' data is neither regulated nor supervised, creating risks for customers.
- Customers currently do not have control over their data to access data-driven services beyond payments. In the absence of rules on who can access data and what they can do with it, customers are not sufficiently confident in permitting data sharing because of potential risks. Without tools to manage data sharing permissions, customers often feel they do not have sufficient control. They are therefore often reluctant to share their data.
- Even where customers want to share data, the rules governing such sharing are either absent or unclear.
- Data sharing can be costly as both the data itself and the technical infrastructure upon which it would rely are not standardised and hence differ significantly.

This initiative aims to address these problems in order to promote better access to consumers' and firms' financial data and hence make it possible for consumers and firms to realise the gains stemming from better financial products and services. Combining data from different data holders can enable innovative services for customers who are willing to grant such access.

What is the proposal about?

The proposal for a Regulation establishes a framework for responsible access to individual and business customer data across a wide range of financial services (also referred to as "open finance"). This builds on the already existing "open banking" provisions introduced by the Payment Services Directive (PSD2) that regulate access to customer data held by account-servicing payment service providers. The proposal takes a customer-centric approach. It aims to ensure that all consumers and firms have effective tools to control the use of their financial data. The proposal therefore provides additional tools to ensure personal data protection in line with the General Data Protection Regulation (GDPR) and applying the general principles of business-to-business data sharing in line with the Data Act proposal.

What type of data is in the scope of proposal?

The proposal covers customer data that financial institutions typically collect, store and process as

part of their normal interaction with customers who can be either natural persons or business customers. This includes data transmitted by the customers themselves (transmitted data) and transaction data arising from customers' interactions with their financial service providers (transaction data). The data covered by this proposal involves both personal data that relates to identified or identifiable individuals and non-personal data that relates to business entities or financial product (contract) features. In terms of specific types of customer data, the initiative covers loans, savings, investments, occupational and personal pensions, and non-life insurance. Input data collected for the purposes of carrying out an assessment of suitability and appropriateness as defined in Article 25(2) and Article 25(3) of Directive 2014/65/EU and input data collected for the purposes of creditworthiness assessment of firms are also covered.

The proposal does not cover some customer data where an overall cost benefits analysis found that risks of financial exclusion may outweigh potential benefits. This concerns in particular: creditworthiness assessments of natural persons; and life, sickness and health insurance.

How will the proposal enable effective access to customer data for customers and for firms acting as data users?

The proposal gives customers a right to access the data which financial institutions hold about them ("data holders") through electronic means without additional cost. It also gives customers a right to give access to these data to firms from whom they would like to obtain innovative services ("data users").

Today, customers of financial service providers can only ensure that third-party providers obtain access to their payment accounts data under PSD2. Although GDPR also gives consumers the right to share their personal data held by any financial service provider directly with third-party providers, this does not cover non-personal data related to business customers and is only applicable 'where technically feasible'. However, direct electronic access is necessary for data users to provide customers with digital financial services, if customers want their data to be used for that purpose. The proposal therefore introduces a general obligation for data holders to make customer data available to data users at customer request.

Enabling customer data aggregation and sharing at scale in the financial sector across the EU would require that both customer data and their sharing interfaces are standardised. This proposal will promote standardisation of customer data and access interfaces. Furthermore, it aims to ensure that data holders implement the developed standards and have sufficient economic incentives to provide high quality interfaces, by allocating the costs involved in implementing those standards and interfaces between data holders and data users. Moreover, as data reuse involves risks, such as data misuse, financial crime or fraud, it must be ensured that the liability in case of data misuse, financial crime or fraud is clear and predictable and liability risks do not act as a disincentive for data holders to make data available. This is why financial data sharing schemes will have to provide for a clear liability regime and corresponding dispute resolution mechanisms.

How will the proposal enhance customer trust in data sharing?

Customers must be able to decide who can use their financial data and how: they may either want to limit third-party access to their data for personal reasons, or they may wish to grant firms access to their data for the purposes of obtaining financial and information services. This proposal ensures a secure data-sharing framework that empowers customers by giving them meaningful and effective control over their data, providing additional safeguards in line with data protection rules and rules on digital operational resilience, as well as ensuring that the use of this data by the industry is beneficial to them.

First, life, sickness and health insurance data will be excluded from the scope of this proposal to guard against any unintended consequences and risks with respect to the processing of such sensitive data, e.g. risks of financial exclusion. Creditworthiness data of natural persons will also be excluded. Furthermore, EBA and EIOPA will be empowered to issue guidelines on the use of customer data (that is in the scope of this proposal) originating from other sources for the purposes of creditworthiness evaluation of natural persons as well as risk assessment and pricing of life, sickness and health insurance.

Second, any data sharing relationship will be strictly subject to customer permission, as has already been the case with respect to payment account data under PSD2. A particular challenge is when customers have relationships with multiple firms (both data holders and data users), which can make it cumbersome to track and revoke the respective permissions granted. This is why this proposal imposes a requirement on data holders to provide customers with dedicated permission dashboards as part of their customer interfaces.

Third, the proposal adds rules on who is eligible to access customer data to make sure that all data

users are subject to authorisation and supervision. For firms to be able to access customer data under this proposal, they will either have to be regulated financial firms or be authorised as Financial Information Service Providers (FISPs). FISPs will also be subject to the Digital Operational Resilience Act, which addresses cybersecurity risks. Account Information Service Providers (AISPs) duly authorised under the PSR/PSD3 regime will be eligible to access customer data in line with the modalities set out in this proposal, notably as members of financial data sharing schemes and subject to compensation to data holders.

How does this proposal relate to the broader policy framework on data?

This proposal contributes to the commitment set out in the EU Digital Finance Strategy to put in place a European financial data space. It builds on the lessons learned from 'open banking' as identified in the review of the revised Payment Services Directive (PSD2) and is fully consistent with the PSR/PSD3 proposals tabled today. Overall, this proposal fits into the broader European strategy for data and will builds upon the key principles for data access and processing set out in its accompanying initiatives, such as the Data Governance Act, the Digital Markets Act and the Data Act proposal.

How does this proposal relate to data sharing under PSD2?

The open banking provisions introduced under PSD2 concern customer data of only one type of product in the financial sector – payment account. Payment account data will remain subject to the regulatory framework under PSR/PSD3, which is already well established. This proposal in turn regulates access to customer data for all other types of financial products and services, excluding life and health/sickness insurance as well as data related to consumer creditworthiness assessment.

Furthermore, this proposal also differs in terms of the regulatory approach. While data sharing under PSR/PSD3 is based on non-contractual access at no cost, this proposal requires data holders and users to agree on financial data sharing schemes that contain the contractual terms for sharing data. It also entitles data holders to get reasonable compensation for the costs of making data available. This is fully in line with the Commission's Data Act proposal. Unlike PSR/PSD3, this proposal covers only information access services and excludes transaction initiation services, because the latter are not relevant for all types of financial services covered by this proposal.

How does this proposal interact with GDPR?

The proposed framework is coherent with and without prejudice to the GDPR, which provides for general rules on the processing of personal data to ensure their protection and free movement. Any legal obligation to disclose personal data must meet the requirements set by the GDPR. Giving consumers control over their personal data is one of the main objectives of the GDPR, which stipulates generally applicable requirements, including the requirement to ensure the security of data processing and the right to data portability. However, the latter is subject to practical limitations, which have led the Commission to propose a general framework for additional data access rights in the Data Act proposal, and the same approach is taken in this initiative.

Does the proposal respect the subsidiarity principle?

Financial services legislation is a shared competence between the EU and Member States. Member States cannot improve data sharing in the financial sector acting alone, given that the holders and potential users of customer data in finance often operate across several Member States in the single market for financial services, and they do so on the basis of EU financial services legislation. Therefore, a single customer may have data held by financial institutions in different Member States, and all these financial institutions would need to be subject to the same framework and the same technical standards to enhance trust and allow the integrated use of this data. Individual national initiatives would result in overlapping requirements and disproportionately high compliance costs for firms without providing most of the benefits due to a lack of interoperable standards, which are fragmented along national lines.

How and by whom will the standards be developed?

The proposal will require data holders and data users to become members of a financial data sharing scheme, which will be tasked with the development of standards for customer data and access interfaces. These standards will have to be subsequently implemented by all scheme members.

Will data holders be entitled to compensation?

Data access for customers themselves will be free of charge. The situation will be different for firms accessing data under permission by the customer. Data holders will be entitled to reasonable compensation from data users for making customer data available to them. In cases where the data user is an SME (e.g. a small FinTech firm), any compensation shall not exceed the costs directly

attributable to the individual data request.

These compensation principles fully reflect the general principle of compensation to data holders legally obliged to make data available introduced by the Data Act proposal. Thus, it can in no way be considered as a payment for the data itself, but rather as compensation for the costs of building and maintaining the technical infrastructure required for accessing high-quality data that can be used by data users to add further value for the financial sector customers.

For More Information

Press release

Factsheet

Legal texts

QANDA/23/3544

Press contacts:

Daniel FERRIE (+32 2 298 65 00)
Aikaterini APOSTOLA (+32 2 298 76 24)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email