EU Financial Data Access Regulation (FIDA)

Summary of proposals across Commission, Parliament and Council texts.

Trilogues have just recently commenced so there is no final agreed version of the text at this date. Links to the texts are as follows:

- Commission proposals (28 June 2023)
- Parliament proposals (30 April 2024)
- Council proposals (2 December 2024)
- Commission simplification non-paper (17 May 2025) ("**Simplification proposal**")
- 2nd Trilogue (17 June 2025) – Parliament and Council (under Polish Presidency) ("**2nd trilogue**")

This Table was originally prepared 22 April 2025, with subsequent updates as highlighted.

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
Definitions	**Data in scope** (a.2(1))	A.2(1)(a)-(f) list Simplification proposals: • Impose a time limit on data - allow Financial Data Sharing Schemes to exclude data collected more than 10 years prior to the data request (where not readily available in digital form, and not part of contractual conditions) • Exclude data on terminated contracts (no longer active)	Significant amends: • Amends scope of (a), (b), (c), (f). • Adds new (fa) (non-sensitive categories of data used by data holders to meet KYC requirements for business customers) 2nd trilogue: • Time limit on data - 10 years is excessive, 3 years should be enough; and there is a need to distinguish between terminated -v- fulfilled contracts here	Significant amends: • Amends scope of (a), (b), (d), (e) • Deletes (f) • Deletes (c) but adds new A.2(1)(1a) to allow member states discretion to include occupational pension schemes • Adds new A.2(1)(1b) allowing FDSS to limit the customer data made available, to data collected 10 years prior to the data request, if the customer data is not readily available in digital format or it is not part of the contractual conditions of the product/service 2nd trilogue: • Time limit on data - there is a need to distinguish between terminated -v- fulfilled contracts here (benefit in keeping terminated contracts in scope as some record of these transactions could be beneficial to e.g. allow year-on-year comparisons.
	Consumer (a.3(1))	A natural person who is acting for purposes other than his or her trade, business or profession	Defined by reference to Article 2, point (1), of Consumer Rights Directive (2011/83): any natural person who, in contracts covered by this Directive, is acting for purposes ~~other than~~ which are outside his or her trade, business, craft or profession	[Same as Commission version]
	Data Holder (a.3(5)) (a.2(2))	A Financial Institution, defined as those listed in A.2(2)(a)-(n) Simplification proposals: • Exclude credit rating agencies and reinsurance undertakings 2nd trilogue: Does not agree with the exclusion of IORPs (asked Parliament and Council to reconsider IORP exclusion – perhaps consider other ways to ensure proportionality for smaller sized entities (and not whole sectors)	Some tweaks but effectively a Financial Institution, defined as those listed in A.2(2)(a)-(n) – but with significant amends as follows: • Amends to (b), (c), (i), (k), (m) • Deletes (l) • Adds new (oa) (operators of payment schemes) • Remainder aligns with Commission 2nd trilogue: • Exclusion of IORPs, credit rating agencies and reinsurance undertakings (and possibly ancillary insurance intermediaries) is important	Some tweaks but effectively a Financial Institution, defined as those listed in A.2(2)(a)-(n) – but with significant amends as follows: • Aligns with Parliament on amends to (b), (c) • Amends to (k), (m) • Remainder aligns with Commission 2nd trilogue: • Exclusion of IORPs, credit rating agencies and reinsurance undertakings (and possibly other entities for which FiDA-eligible activities only represent a marginal part of their total business) is important

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
	Data User (a.3(6))	Any entity listed in A.2(2) who, following permission of a customer, has lawful access to customer data listed in A.2(1) *[Financial Institution or Financial Information Service Provider (FISP)]*	Same as Commission version, but note amended scope of A.2(2) above	Same as Commission version, but note amended scope of A.2(2) above
	Customer (a.3(2))	A natural or a legal person who makes use of financial products and services Simplification proposals: - Narrow the 'customer' definition to only include natural persons and SMEs (retail-centric), excluding all others	A natural person resident in the Union or a legal person established in the Union who ~~makes~~ is a consumer or a micro, small or medium-sized enterprise that is party to or has applied to an agreement for the use of financial products and services 2nd trilogue: - Likes the Commission simplification proposal (as it aligns more closely to the above), but notes the need to define also by reference to establishment and EU residence requirements	A natural or a legal person who makes use of financial products and services, and in the case of insurance, it means insured persons or policyholders, excluding third-party beneficiaries 2nd trilogue: - Open to the Commission simplification proposal to exclude large corporates
	Customer Data (a.3(3))	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	Personal and non-personal data in digital form that is collected, stored and ~~otherwise processed~~ managed by a financial institution as part of ~~their~~ its normal course of business in connection with ~~customers~~ a relationship between a customer and the financial institution as the data holder for the provision of such services, which covers both data provided by a customer and transaction data ~~generated~~ related to a customer held by a financial institution and which excludes data created as a result of ~~customer interaction with the financial institution~~ profiling as defined in Article 4(4) of Regulation (EU) 2016/679 and trade secrets as defined in Article 2, point (1), of Directive (EU) 2016/943 2nd trilogue: - Need to discuss definition of 'raw data'	Personal and non-personal data in digital form that is collected, stored and ~~otherwise processed~~ managed 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~~ transaction data related to the use a that results from the of the financial product or service by a customer ~~interaction with held by a that financial institution~~, as well as data on the contractual conditions of the product or service held by a customer, excluding any confidential business data or trade secrets [recital (9): The personal and non-personal customer data included in the scope of this Regulation only refers to ~~should be considered as~~ raw data that occurs as a result of normal course of business between data holders and customers. It should not include confidential business data or trade secrets, nor data enriched internally by the data holder]
	Financial Institution (a.3(8))	A.2(2)(a)-(n) definition	Same as Commission definition, but note significantly amended scope of A.2(2) above	Same as Commission definition, but note significantly amended scope of A.2(2) above
	Financial Information Service Provider (a.3(7))	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	An entity providing a ~~data user~~ financial information service that is established in the Union and authorised under Article 14 to access the customer data listed in Article 2(1) for the provision of financial information services "Financial information service" (new a.3(6a)): the online service provided by a data user of collecting and consolidating customer data to customers and does not include the provision of services regulated under existing Union financial services legislation and reserved for financial institutions authorised under Union law	~~a~~ An entity ~~data user~~ that is authorised under Article 14 as a data user to access the customer data listed in Article 2(1) for the provision of financial information services "Financial information service" (new a.3(6a)): an online service provided by an entity who has access to customer data made available by one or several data holders upon permission of the customer with the purpose of providing a service of collecting, processing and consolidating customer data and does not include any provision of regulated and reserved activities and services under Union law
	Gatekeeper	[No position]	(Defined throughout the Regulation) by reference to A.3 of Digital Markets Act (Reg 2022/1925)	(New A.3(28c)): An undertaking providing core platform services, designed pursuant to A.3 of Digital Markets Act (Reg 2022/1925)
	Non-Personal Data (a.3(10))	Data other than Personal Data as defined in Article 4(1) of GDPR	Data other than personal data as defined in Article 4(1) of Regulation (EU) 2016/679	[Same as Commission version]
	Personal Data (a.3(11))	Personal data as defined in Article 4(1) of GDPR	[Same as Commission version]	[Same as Commission version]

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
Excluded from FIDA (a.2(3))		FIDA does not apply to entities in A.2(3)(a)-(e) DORA Simplification proposals: - Narrow the 'customer' definition to only include natural persons and SMEs (retail-centric), excluding all others - Impose a time limit on data - allow Financial Data Sharing Schemes to exclude data collected more than 10 years prior to the data request (where not readily available in digital form, and not part of contractual conditions) - Exclude data on terminated contracts (no longer active) - Exclude from the 'Data Holder' definition, credit rating agencies and reinsurance undertakings 2nd trilogue: - Does not agree with the exclusion of IORPs (asked Parliament and Council to reconsider IORP exclusion – perhaps consider other ways to ensure proportionality for smaller sized entities (and not whole sectors)	- Aligns with Commission on excluding A.2(3)(a)-(e) DORA entities – but adds that entities under (e) (cryptoasset service providers) can opt in. - Brings into scope of FIDA small enterprises defined in Commission Recommendation 2003/361/EC from 12 months of FIDA application - Expands exclusion to also cover: ○ Small and non-interconnected investment firms under A.12 IFR ○ Entities under A.2(5)(4)-(23) CRD6 ○ Sensitive data referred to in A.9(1) GDPR (unless A.9(2) GDPR is complied with) 2nd trilogue: - Likes the Commission simplification proposal for 'customer' (as it aligns more closely to the Parliament proposal), but notes the need to define also by reference to establishment and EU residence requirements - Exclusion of IORPs, credit rating agencies and reinsurance undertakings (and possibly ancillary insurance intermediaries) is important - Time limit on data - 10 years is excessive, 3 years should be enough; and there is a need to distinguish between terminated -v- fulfilled contracts here	- Aligns with Commission on excluding A.2(3)(a)-(e) DORA entities - Expands exclusion to also cover: ○ Entities under A.2(5)(4)-(23) CRD6 adding wording "*that are located within their respective territories*" ○ Entities under A.32 PSD ○ Sensitive data referred to in A.9 GDPR (unless A.9(2) complied with) and A.10 GDPR ○ Data collected as part of a credit worthiness assessment ○ Existing national pension tracking systems ○ Customer data associated with fulfilled or terminated contracts ○ Sickness and health insurance products; and data on personal ○ Social security insurance ○ Small IORPs under A.5 IORP2 2nd trilogue: - Open to the Commission simplification proposal to exclude large corporates from 'customer' to give retail focus - Exclusion of IORPs, credit rating agencies and reinsurance undertakings (and possibly other entities for which FiDA-eligible activities only represent a marginal part of their total business) is important - Time limit on data - there is a need to distinguish between terminated -v- fulfilled contracts here (benefit in keeping terminated contracts in scope as some record of these transactions could be beneficial to e.g. allow year-on-year comparisons.
Data made available to customer (a.4)		Data Holder to make available, upon request from Customer submitted by electronic means, to the Customer the Data without: - undue delay - free of charge - continuously - in real-time	- Replaces the request from the Customer by 'electronic means' with "*through a dedicated online or mobile customer interface*' - Adds that the Data is made available to the customer "*via that customer interface in an easily readable format reflecting the state in which those Data are readily available to the Data Holder at the time that access is requested by a Customer*" - Otherwise same as Commission version	[Same as Commission version]
Data made available to Data User (a.5 and a.6)	General (a.5(1))	Data Holder to make available, upon request from Customer submitted by electronic means, the Data (for the purpose for which the customer has granted permission) to the Data User without: - undue delay - continuously - in real-time	- Requires request from Customer to be '*explicit*' and made through a '*dedicated online or mobile customer interface'* - Otherwise broadly aligned with Commission version	- Allows requests from Customer *or the Data User acting on behalf of the Customer* - Otherwise broadly aligned with Commission version
	Compensation (a.5(2))	Data Holder may claim compensation from the Data User only if the Data is made available: - under a Financial Sharing Data Scheme (a. 9, 10); or - under a.11	[Aligned with Commission version]	[Aligned with Commission version]
	Obligations on Data Holder (a.5(3))	- Provide Data in format based on "generally recognised standards" and at least in same quality as available to Data Holder - Communicated securely - Request Data Users to show they have obtained permission from Customer to access Data	- Aligned with Commission version on (a), (b), (c) and (d) - Adds a new (ba) that where Personal Data is processed, the Data Holder requests Data Users to demonstrate they have a valid legal basis under A.6(1)(a) or (b) GDPR - On (e) replaces 'respect' with 'protect', and deletes reference to A.5(1) simply applying the provision to the trade secrets and IP rights of the Data Holder	- Aligned with Commission version on (b) and (d) - On (a) replaces "generally recognised standards" with "common standards" - On (c) adds that the Data Holder may prompt the Customer to confirm their permission via the Permission Dashboard - On (e) replaces 'respect' with 'protect'

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
		• Provide Customer with a Permission Dashboard to monitor and manage permissions • Respect confidentiality of trade secrets and IP rights when customer data is access in accordance with A.5(1)		
	Obligations on Data User (a.6(1), (2) and (4))	**Eligibility of Data User:** Requires prior authorisation by regulator as a Financial Institution or Financial Information Service Provider	**Eligibility of Data User:** Broadly aligned with Commission version but requires Financial Information Service Provider to be a legal person.	**Eligibility of Data User:** Broadly aligned with Commission version but adds additional criteria: ○ that Customer Data is made available to the Data User in accordance with the relevant FDSS rules ○ that before operating as a Data User Financial Institutions must notify the regulator of their intention to operate as a Data User
		Permission-limited: Access limited to that for which permission has been granted by Customer	**Permission-limited**: Broadly aligned with Commission but makes clearer the Data requested/accessed is limited to what is e.g. necessary for the purpose given, only relating to the specific service to which permission is given etc.	**Permission-limited**: Significant amends: • Requires that permission is to be freely given, limited in time, separated from possible other declarations/text and clearly state the purposes for which permission is given • Sets out a detailed (non-exhaustive) list of required information to be included in the permission
		Data deletion: Deleted when no longer necessary for the purposes for which permission was granted	**Data deletion:** Aligns with Commission version but also applies deletion requirement also to *all backups*, and *without undue delay*	**Data deletion:** • Aligns with Commission version but also applies deletion requirement also to *all backups*, and *without undue delay* • Also adds deletion required where permission is withdrawn and not re-established by Customer within 48 hours
		Management of Data: a) Only process Data for performing the service explicitly requested by Customer b) Respect confidentiality of trade secrets and IP rights c) Put in place technical, legal and organisational measure to prevent transfer or access to non-personal customer data *[a.4(1) GDPR]* that is unlawful under EU or national law d) Necessary measures to ensure appropriate level of security for storage, processing and transmission of non-personal data*[a.4(1) GDPR]* e) Not process customer data for advertising purposes, except for direct marketing in accordance with EU or national law f) Where Data User is part of a group, Data shall only be accessed and processed by the entity that acts as Data User.	**Management of Data:** • Aligned with Commission version but adds at the end *'in the best interest of the Customer'* • Broadly in line with Commission version but replaces 'respect' with 'protect' • Aligned with Commission version but deletes reference to 'non-personal' • Aligned with Commission version but deletes reference to 'non-personal' • Amends requirement to only allow contacting of Customers for direct marketing purposes subject to their prior consent or with offers for products/services similar to those for which they have accessed customer data and under the conditions provided in A.13(2) ePrivacy Directive (2002/58) • Aligned with Commission version but also applies the provision to where on of the entities of the group has been designated a Gatekeeper under A.3 Digital Markets Act (Reg 2022/1925) New (aa) Requirement not to transfer customer data to any third party, including an in outsourcing scheme, without the Customer's explicit permission New (ba) Requirement to *respect* data protection rights of *Consumers* and the level of protection guaranteed by GDPR	**Management of Data:** • Aligned with Commission version but requires the Data User to act professionally in accordance with the best interests of its Customers and must be able to demonstrate that the use of the Data is in the best interest of the Customer • Replaces 'respect' with 'protect'. Also provides that the protection of confidentiality/IP includes not combining and analysing the accumulated customer data with respect to a given Data Holder for the purpose of reverse-engineering in compliance with the data minimization principle in A.6 and A.7 • Aligned with Commission version but deletes reference to 'non-personal' • Aligned with Commission version but deletes reference to 'non-personal' • Aligned with Commission version but adds 'except for direct marketing in accordance with EU or national law *with prior consent of the Consumer'* • Aligned with Commission version New (fb) Requirement not to transfer customer data to any third party New (ba) Requirement to put in place technical, legal and organisational measure to *protect* data protection rights of *Consumers* and the level of protection guaranteed by GDPR New (g) Requirement for each communication session, to identify itself to the Data Holder and securely communicate with the Data Holder and Customer using secure electronic identification and authentication methods (technicalities to be determined by the FDSS)

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
		Where no permission given: [No position]	**(New) Where no permission given** (new a.6(1a)): Additional requirement that Consumers shall not be prevented accessing a financial product solely because they did not give permission under A.5(1). The burden of proof is on the Data User to show permission was given.	**Where no permission given:** [No position]
		Data access request: [No position]	**(New) Data access request**: • Access request must not be designed in a way to encourage or unduly influence the Customer to grant access • Access request must provide the Customer with fair, transparent and adequate information that is easily understandable for the Customer, including the types of customer data to which the Data User seeks access	**(New) Data access request**: Access request must not be designed in a way to encourage or unduly influence the Customer to grant access
		Gatekeepers: [No position]	**(New) Gatekeepers** (new a.6(4b)): Data Users that are owned/controlled by an undertaking designated as a Gatekeeper are prohibited from combining customer data in A.2(1) with other data relating to the Customer that the Gatekeeper may already collect, store or otherwise possess for purposes outside of FIDA	**(New) Gatekeepers** (new a.6(4a)): Data Users designated as a Gatekeeper or that are owned/controlled by an undertaking designated as a Gatekeeper are prohibited from combining customer data in A.2(1) with other data relating to the Customer that the Gatekeeper may already collect, store or otherwise possess for purposes outside of FIDA
		Place of Data processing: [No position]	**(New) Place of Data processing** (a.6(4a)): Personal data must be processed in the Union unless the conditions in Chapter V of GDPR are complied with	**Place of Data processing:** [No position]
		RTS: [No position]	**(New) RTS**: RTS may be developed on specific practices for implementation of A.6, including pre-ticked boxes and behavioural nudges	**RTS**: [No position]
		FDSS: [No position]	**FDSS:** [No position]	**(New) FDSS (new a.6(2a))**: When Data User and Data Holder are not members of the same FDSS, Data User must join the FDSS of which the Data Holder is a member
	Withdrawal of permission by Customer (a.6(3))	Customer can withdraw permission to a Data User. When processing necessary for performance of a contract, withdrawal be made according to the contractual obligations	Broadly aligned with Commission version but: • Makes clear withdrawal can be made *at any time*; and • Where access is based on consent in accordance with GDPR, *free of charge*	Broadly aligned with Commission version but: • Makes clear withdrawal can be made *at any time* and *free of charge*; and • The right to withdraw consent under A.7(3) GDPR remains unaffected
Perimeter Obligation (a.7)	Obligation (a.7(1))	Processing of Data is limited to what is necessary for the purpose for which it is processed	Aligns with Commission version, but adds that Customers that refuse to grant permission to access their Data shall not be refused access to financial products solely for this reason *[note similar obligation included also in new A.6(1a) above]*	Aligns with Commission version, but adds that Customers that refuse to grant permission to access their Data shall not be refused access to financial products solely for this reason
	Guidelines (a.7(2) and (3))	**EBA** (in co-operation with European Data Protection Board) to prepare Guidelines on the implementation of the Perimeter Obligation for products and services related to the credit score of the consumer	**EBA:** • Aligns with the Commission's call for Guidelines but extends the scope to be covered under the Guidelines to include mortgage credit agreements, accounts including credit card accounts, and investment products. • The EBA should take into account relevant provisions of Dir 2023/2225 (and subsequent iterations).	**EBA:** • Aligns with the Commission's call for Guidelines but replaces reference to 'credit score' with 'creditworthiness assessment'. • It also requires the Guidelines to be elaborated within the framework of Dir 2023/2225 and the Mortgage Credit Directive. • Additionally the EBA is permitted to develop Guidelines on the implementation of the Perimeter Obligation for products/services other than those related to creditworthiness assessment, where it concludes this to be necessary.
		EIOPA (in co-operation with European Data Protection Board) to prepare Guidelines on the implementation of the Perimeter Obligation for products and services related to risk assessment and pricing of a consumer in the case of life, health and sickness insurance products	**EIOPA:** • Amends requirement to require RTS (not Guidelines) and expands scope to be covered to include motor and home insurance products. • The RTS must also include provisions on how data may be used to avoid excessive granularity that undermines the "risk sharing" principle of insurance.	**EIOPA:** • Aligns with the Commission's call for Guidelines but removes 'health and sickness' references, replacing them with 'insurance products and non-life' insurance products. It also requires the Guidelines to be elaborated within the framework of IDD, Solvency II, MiFID2.

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
			• The RTS must also address how the 'right to be forgotten' of survivors of cancer or other chronic diseases and mental conditions shall be applicable to non-credit related insurance policies, including life and health insurance	• The Guidelines must also include provisions on how data may be used to avoid excessive granularity that undermines the "risk sharing" principle of insurance. • EIOPA is tasked, within 2 years of entry into force of FIDA, to prepare an impact assessment report of climate risk and natural disaster-related data on the insurance sector, after which the Guidelines may be amended
		ESMA: [No position]	**ESMA**: [No position]	**ESMA:** (New) May develop Guidelines on the implementation of the Perimeter Obligation, where necessary
		ESA Guidelines on A.2(1)(fa): n/a *[A.2(1)(fa) only exists in Parliament version]*	**ESA Guidelines on A.2(1)(fa): (New A.7(4a))** ESAs to develop Guidelines on the processing of customer data referred to in A.2(1)(fa) (non-sensitive categories of data used by data holders to meet KYC requirements for business customers) that constitutes Non-Sensitive Data	**ESA Guidelines on A.2(1)(fa):** n/a *[A.2(1)(fa) only exists in Parliament version]*
Permission Dashboard (a.8)	General (a.8(1))	Data Holder to provide Customer with a Permission Dashboard to monitor and manage permissions it has provided to Data Users	Aligns with Commission version but requires the permission dashboard to be *integrated into its user interface*	[Aligns with Commission version]
	Content (a.8(2))	**Overview**: Overview of each ongoing permission (including Data User name, customer account, financial product/service to which access has been granted, purpose of permission, categories of data shared, period of validity of permission)	**Overview**: Aligns with Commission version but: • adds that the information should be available *at any time and in a format that is easy to understand, to the extent that information if in the possession of the Data Holder* • adds to the list of information to be included in the Dashboard, *the dates on which the Data was accessed*	**Overview**: Aligns with Commission version but: • adds that the information should be available *at any time* • adds that the period of validity of permission should include the *date on which the Customer gave the permission*, and the dates on which the *Data was accessed*
		Withdrawal: Allow Customer to withdraw permission to a Data User	**Withdrawal**: Aligns with Commission version but adds that it can take place *at any time and free of charge*	**Withdrawal**: Aligns with Commission version but adds that it can take place *at any time and free of charge*. Also requires the Data User to cease accessing the Data and, without undue delay, erase all Data received as a result of the Data access permission granted by the Customer
		Re-establishment: Allow Customer to re-establish permission withdrawn	**Re-establishment**: [Deleted]	**Re-establishment:** Allows re-establishment of permission but only *within 48 hours from withdrawal*
		Records: Include a record of permissions withdrawn or expired for a duration of 2 years	**Records**: [Aligns with Commission version]	**Records**: [Aligns with Commission version]
		Opt-out: [No position]	**Opt-out (New A.8(2)(ca):** Allow Customer to opt-out from Data access with third parties in a general way for all present and future Data access permission requests	**Opt-out:** [No position]
		PSR Consistency: [No position] Simplification proposals: • Ensure alignment of permission dashboards under FIDA and PSR.	**PSR Consistency (New A.8(2)(da)):** Be consistent with the Payment Services Regulation (PSR) dashboards and allow Data Holders to manage Data permissions pursuant to PSR through a single dashboard upon the request of the user *[S&S note: meaning Customer?]*	**PSR Consistency (New A.8(2)(da)):** Be consistent with the Payment Services Regulation (PSR) dashboards and allow Data Holders to manage Data permissions pursuant to PSR through a single dashboard upon the request of the *Customer*
	Access (a.8(3))	• Data Holder to ensure Permission Dashboard in easy to find in its user interface • Information displayed is clear, accurate and easily understandable for the Customer	Aligned with Commission version but: • Adds that the Dashboard is also *neutral* • that the information is exclusively limited to information provided by the Data User	Aligned with Commission version but: • adds that the Dashboard is also *neutral* • Data Holder shall not prompt the Customer to withdraw a permission given to a Data User. Data Holders are prohibited from designing, organising, or operating their permission Dashboard interfaces in a manner that deceives, manipulates or directs Customer behaviour towards permissions that are not in the Customer's best interest, or that materially distorts or impairs the ability of Customers to make free and informed decisions

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
	Co-operation between Data Holder and Data User (a.8(4))	**General:** Data Holder and Data User to cooperate to make information available via the dashboard in real time	**General:** [Aligns with Commission version]	**General:** [Aligns with Commission version]
		Changes to permission: Data Holder inform Data User of changes made to permission	**Changes to permission:** • Aligned with Commission version but adds Data Holder to inform Data User *in real time.* • Also makes clear that "changes" to a permission includes *withdrawal* of permission	**Changes to permission:** • Changes obligation for Data Holder to 'inform' Data User, to 'notify' the Data User *without undue delay.* • Also makes clear that "changes" to a permission includes *withdrawal* of permission
		New permission: Data User inform Data Holder of new permission granted (including purpose of permission, period of validity, categories of data concerned)	**New permission:** • Adds Data Holder to inform Data User *in real time* • Requires information on the purpose of permission to be provided in *clear and comprehensible manner for the user* • Adds a requirement to provide information on the legal basis under A.6(1) GDPR and, where relevant, the exception under A.9(2) GDPR that the Data User intends to rely on to access Personal Data contained in the customer data	**New permission:** [Aligned with Commission version]
		Responsibility for accuracy: [no position]	**Responsibility for accuracy (New A.8(4)(ba):** Data User is responsible for the accuracy of the data provided to the Data Holder	**Responsibility for accuracy**: [no position]
		Guidelines: [no position]	**Guidelines**: [no position]	**Guidelines (New A.8(4a):** ESAs to develop Guidelines on the application of A.8
		More than one Data Holder (New A.8(4a)): [no position]	**More than one Data Holder (New A.8(4a)):** More than one Data Holder may, collectively, provide a single permission Dashboard to customers, provided that the Dashboard fulfils that criteria in A.8(1)-(4)	**More than one Data Holder (New A.8(4a)):** [no position]
Financial Data Sharing Schemes (FDSS) (a.9-11)	Membership	**Name:** Financial Data Sharing Schemes (FDSS)	**Name**: Changes name of FDSS to Financial Data *Access* Scheme (FDAS)	**Name:** [Same as Commission version]
		Timeline: Data Holders and Data Users (within 18 months of FIDA entering into force) shall become members of a FDSS	**Timeline:** Same as Commission version but timeline changed to within *30 months*	**Timeline:** [Timeline deleted]
		Multiple memberships: It is possible to become members of more than one FDSS	**Multiple memberships:** Broadly aligns with Commission version	**Multiple memberships:** [Same as Commission version]
		Data sharing: Data sharing shall be made in accordance with the rules of the relevant FDSS	**Data sharing**: [Broadly aligns with Commission version]	**Data sharing:** [Same as Commission version]
		Member types: Membership made up of: • Data Holders and Data Users representing a significant proportion of the market of the product/service concerned • Customer organisations • Consumer associations	**Member types:** Same as Commission version but qualifies customer organisations and customer associations as being those "*with expertise in financial services*"	**Member types:** Same as Commission version but limits the role of customer organisations and customer associations to "*an advisory role in particular matters that are related to the protection of customers*"
		Guidelines: [no position]	**Guidelines:** [no position]	**Guidelines:** Provides that the ESAs will adopt guidelines on the calculation of the *significant proportion of the market*, within 3 months of FIDA entering into force.
	Governance and content (a.10(1))	**Representation**: Fair and equal representation as between Data Holders and Data Users members – in internal decision making processes and equal weight in voting	**Representation:** Same as Commission version but amends as follows: 'fair and equal representation. Also clarifies that *every member [within the Data Holders and Dara Users groups] is to have equal voting weight within their side*	**Representation:** [Same as Commission version]

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
		Double counting: Where a member is both Data Holder and Data User, its membership shall be counted equally towards both sides	**Double counting**: [Same as Commission version]	**Double counting**: [Same as Commission version]
		Treatment and Admission: Equal treatment and fair admission of members	**Treatment and Admission:** [Same as Commission version]	**Treatment and Admission:** [Same as Commission version]
		Same terms: New members to get same terms as existing members	**Same terms**: [Same as Commission version]	**Same terms**: [Same as Commission version]
		Amendments: Rules can be amended, after impact analysis, by a majority of each community of Data Holders and Data Users	**Amendments**: [Same as Commission version]	**Amendments**: [Same as Commission version]
		Transparency and reporting: Rules on transparency and reporting to members	**Transparency and reporting**: [Same as Commission version]	**Transparency and reporting**: [Same as Commission version]
		- **Common standards:** To be agreed by members, for the data and technical interfaces (APIs) to allow customers to request data sharing in accordance with A.5(1). These may be developed by scheme members or by other parties or bodies - Simplification proposals: - Rather than a market-driven consensus to create common standards, follow instead a similar procedure to a.33 Data Act i.e. establish a common level of functionality for data and technical interfaces (APIs) based on harmonised standards developed by European standardisation organisations (ESOs) - Measures on customer authentication could be streamlined by proposing voluntary use of European Digital Identity (EuID) Wallets to enable authentication and identification in a harmonised manner 2nd trilogue: - Focus of Commission simplification paper was on drawing from existing EU law (to give market operators a better understanding of what is expected – keeps costs down). E.g. minimum standards, following the logic of the Data Act, would provide consistency and decrease burdens for the schemes - Re-iterated the Commission simplification paper proposal to voluntarily use EuID Wallet for authentication – reduce burden	**Common standards:** Broadly aligns with Commission version but adds that the common standards *shall draw on existing international or industry-recognised standards* or be developed by scheme members or by other parties or bodies. It also adds a new provision that the FDAS will include minimum technical and organisational measures the FDAS members will implement to ensure an appropriate level of security for exchanged data (including security measures to prevent and mitigate the risk of fraud). 2nd trilogue: - Standards should be developed by members – but agrees with Commission simplification proposals that EU bodies might be able to assist to establish standards - Supports Commission simplification proposals for voluntary use of EuID Wallets	**Common standards:** Broadly aligns with Commission but adds that the FDSS will agree on the level of standardisation of data points at a level accepted and implemented by its members. Technicalities to be determined by FDSS in relation to the requirement under A.6 (management of data) that for each communication session, the Data User should identify itself to the Data Holder and securely communicate with the Data Holder and customer using secure electronic identification and authentication methods. 2nd trilogue: - Open to Commission simplification proposals to establish common functionality for data and APIs, and to involve ESOs to harmonise standards - Concerned about Commission simplification proposal to include explicit reference to EuID Wallet, as this could be overly restrictive. Other authentication methods could be considered
		Compensation (general): Establish a model to determine max. compensation to which Data Holder is entitled based on these principles: - Reasonable compensation directly related to making the data available - Based on objective, transparent, non-discriminatory methodology agreed by members - Based on comprehensive market data - Periodically reviewed and monitored to take account of technical progress - Gear compensation towards the lowest level prevalent in the market	**Compensation (general)**: Aligns with Commission version but adds to the principles: - Compensation should be reasonable *and proportionate* and related to the *costs incurred in* making the data available. It also provides that compensation agreements shall ensure the members take into account the costs of formatting the data, dissemination via electronic means and storage, as well as investments in the collection and production of data where applicable, taking into account whether other parties contributed to obtaining/generating/collecting the data, as well as the format and nature of the data - Compensation may include a margin - Gear compensation towards the *lower* levels prevalent in the market (while ensuring there are sufficient incentives to foster market adoption and effective competition)	**Compensation (general):** Aligns with Commission version but adds to the principles that compensation may include a margin

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
		Compensation (micro/SME): Where Data User is a micro or SME *[A.2 Comm Recommendation 2004/361/EC, Annex]* any compensation agreed shall not exceed the costs directly related to making the data available	**Compensation (micro/SME):** [Aligns with Commission version]	**Compensation (micro/SME):** Aligns with Commission version but qualifies the application to micro/SME to *exclude* those that have partner enterprises or are part of linked enterprises that do not qualify as micro/SME
		Compensation Guidelines: [no position]	**Compensation Guidelines:** The guidelines on reasonable compensation adopted by the Commission under a.9(5) of Regulation 2023/2854 (Data Act) should be also be taken into account.	**Compensation Guidelines:** The guidelines on reasonable compensation adopted by the Commission under a.9(5) of Regulation 2023/2854 (Data Act) should be also be taken into account.
		Liability: Determine the contractual liability of its members – including if data is inaccurate, inadequate quality, security compromised, misuse of data. For personal data, liability provision shall be in line with GDPR.	**Liability**: [Aligns with Commission version]	**Liability**: [Aligns with Commission version]
		DR: Provide for an independent, impartial , transparent and effective dispute resolution system (in line with requirements in Consumer ADR Directive)	**DR**: [Aligns with Commission version]	**DR**: [Aligns with Commission version]
		Compensation for loss: [no position]	**Compensation for loss**: Provide a mechanism of financial compensation to customers for any loss of data, damage or fraud suffered	**Compensation for loss**: Provide a mechanism of financial compensation to customers for any loss of data, damage or fraud suffered
		Security: [no position]	**Security**: [no position]	**Security**: Adds a requirement for common technical and organisational measures that FDSS members shall implement to communicate securely (in order to show an appropriate level of security for the processing and transmission of customer data
		Service levels: [no position]	**Service levels**: [no position]	**Service levels**: Adequate service levels for technical interfaces (re: availability and performance)
		Limited data option: [no position]	**Limited data option**: [no position]	**Limited data option:** The possibility to agree on a limit under a.2(1)(1b) [i.e. under which FDSS can limit the customer data made available, to data collected 10 years prior to the data request, if the customer data is not readily available in digital format or it is not part of the contractual conditions of the product/service where appropriate]
		Proof of permission: [no position]	**Proof of permission**: [no position]	**Proof of permission:** Requirements to demonstrate that a data user has obtained permission of the customer to access the data
		FDSS implementation timetable: [no position]	**FDAS implementation timetable**: • (new a.9(1a) Imposes the following timelines on FDAS implementation: ○ **Development phase**: Within 12 months of FIDA entering into force, members must agree on the general rules applicable for a FDAS (in accordance with a.10(1)(a)-(f) and (i)-(j) – 'development phase') ○ **Implementation phase**: Within 26 months of FIDA entering into force, members must agree common standards and a model to determine compensation (in accordance with a.10(1)(g)-(h). Members shall also notify a FDAS in accordance with a.10(4). ○ **Operationalisation phase**: Within 30 months of FIDA entering into force, members must ensure all elements of a FDAS are fully operational.	**FDSS implementation timetable**: [no position]
	Regulatory notifications on joining a FDSS	Data Holder must communicate, with national regulator of its establishment, the FDSS it is part of, within 1 month of joining the scheme	Broadly aligns with Commission version but adds that the national regulator must also communicate the notification to the ESAs (e.g. ESMA, EIOPA, EBA, as applicable)	[Broadly aligns with Commission version]

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
	Regulatory notifications on setting up a FDSS	- A FDSS set up must be notified to the national regulator of establishment of the 3 most significant Data Holders which are members of that scheme at the time of its establishment. Where this means different member states, or more than one regulator, the FDSS must be notified to all of these regulators who will agree which authority should be responsible for regulator assessment. Notification must be made within 1 month of setting up the FDSS and include its governance details. - Within 1 month of receipt of the notification, the regulator will assess the FDSS. Upon completion it will inform the EBA that it satisfies the required conditions - Once notified to the EBA the FDSS will be recognised in all member states (no further notifications required to other member states)	- Requires that a FDAS set up must be notified *directly to the ESAs* (e.g. ESMA, EIOPA, EBA, as applicable), which will carry out the assessment of the FDAS. However where the FDAS is developed by scheme members established in the same member state, the FDAS must [also?] be notified to the national regulator of that member state, which will carry out the assessment of the FDAS. - Where the FDAS membership changes due to additional Data Holders and Data Users established in another member state, the FDAS shall notify the ESA concerned. However, if membership changes remain within the same member state, the FDAS shall notify the national regulator of that member state. - Deletes the requirement for the regulator to inform the EBA of its FDSS assessment (as the assessment under the Parliament version requires the ESAs to already have the necessary information – per above) - The ESAs must undertake regular comprehensive reviews of FDAS' governance and content arrangements under A.10(1)	Broadly aligns with Commission version but: - Sets out specifics on what information the notification should include in order for the national regulator to determine whether the FDSS represents a significant proportion of the market. - Extends the timeline from receipt of the notification within which the national regulator will assess the FDSS, from 1 month to *3 months* - Significant amendments to the functioning of an existing FDSS (governance modalities/characteristics, products/services covered, geographic scope, 3 most significant members) must be notified to the national regulator without undue delay, which will assess whether the governance and content requirements under A.10(1) remain satisfied. The national regulator must notify the EBA if the FDSS no longer so satisfies.
	Absence of FDSS	- If a FDSS is not developed for one or more of the categories of Data listed in A.2(1) (and no realistic prospect of one being set up within a reasonable amount of time) the Commission can adopt a delegated act specifying, for that category of data, the common standards, max. compensation, and liability provisions.	[Broadly aligns with Commission version]	Broadly aligns with Commission version, but provides that this provision will apply if *6 months after the relevant application of FiDA under A.26(2)* a FDSS has not been notified to the EBA
Financial Information Service Provider (FISP) (a.12-16)	FISP	**Authorisation:** Needs to be authorised by the regulator as a FISP Simplification proposals: - Re: AISPs, there could be a simplified authorisation process for AISPs as part of the FISP authorisation process (legally valid information held on an entity registered as an AISP would not need to be re-submitted, and other core requirements for authorisation like professional indemnity insurance could be re-used)	**Authorisation:** Broadly aligns with Commission version but: - Requires a FISP to be a legal person - An account information service provider (AISP) under PSD may only access customer data if authorised as a FISP.	**Authorisation:** Broadly aligns with Commission version but: - Requires a FISP to be a legal person, and provides that undertakings that are not legal persons shall only provide financial information services if their legal form ensures a level of protection for third parties' interests equivalent to that of a legal person and they are subject to equivalent prudential supervision - Adds to the authorisation requirements, providing that it will only be granted if the national regulator is satisfied that the governance arrangement of the FISP show that it intends to carry out at least part of its business activities in the member state where it has its registered office. - An account information service provider (AISP) under PSD may only access customer data if authorised as a FISP.
		Insurance: Must hold professional indemnity insurance for territories in which they access data, or some other comparable guarantee, or hold initial capital of EUR50k	**Insurance**: [Aligns with Commission version]	**Insurance:** Deletes the alternative options to professional indemnity insurance of or some other comparable guarantee, or hold initial capital of EUR50k *[although later provisions suggest the comparable guarantee alternative may be included in the ESAs' RTS – below]*
		RTS: EBA (in co-operation with ESMA/EIOPA) will produce RTS on details of authorisation requirements and process	**RTS**: [Aligns with Commission version]	**RTS**: RTS will be produced by the ESAs through joint committee
		Gatekeepers: [no position] Simplification proposals: - Align with Data Act by excluding gatekeepers (defined under A.3 Digital Markets Act) from obtaining a FISP license - Rely on Digital Markets Act provisions to regulate licensed financial institutions that are owned and controlled by gatekeepers 2nd trilogue:	**Gatekeepers:** The A.12 requirements do not apply to services by undertakings for which they are designated as a gatekeeper, or to any entity owned/controlled by such undertaking. In that case new A.18a authorisation process will be applied by the national regulator of its registered office. Details of the assessment are set out in A.18a 2nd trilogue: - Internal divergence. EPP does not want full exclusion. S&D/ECR seek full ban	**Gatekeepers:** Where the FISP is a gatekeeper (or owned/controlled by a gatekeeper) additional assessments under (new) A.18 will be performed in order to obtain authorisation as a FISP. A.18 provides that within 6 months of FIDA entering into force. A Data User that is a gatekeeper (or owned/controlled by a gatekeeper) will be subject to a specific assessment by the competent authority of its establishment authorisation. That same assessment must be carried out when such undertaking submits an application to be a FISP, or if an existing Data User becomes a gatekeeper (or is owned/controlled by a gatekeeper). Details of the assessment are set out in A.18. 2nd trilogue:

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
		• Criticised the Parliament and Council proposals for an additional assessment for Gatekeepers. Pushed the Commission simplification proposal to align with the Data Act		• Considers the Commission simplification proposal as a good starting point
		Outsourcing: Authorisation will be granted only if any outsourcing arrangement will not refer the FISP a letter box entity	**Outsourcing:** [Aligns with Commission version]	**Outsourcing**: Deletes reference to letter box entities, providing that authorisation will be granted only if any outsourcing arrangement will not render the FISP *unable to meet its obligations under FIDA*
		Timing: The national regulator will have 3 months from receipt of an application to grant/refuse it	**Timing**: *2 months* (not 3 months)	**Timing**: [Same as Commission version]
		Register: EBA will maintain a public register of authorised FISPs on its website	**Register:** [Broadly aligns with Commission version]	**Register:** [Broadly aligns with Commission version]
		Org requirements: Organisational requirements for FISPs listed in A.16	**Org requirements**: Broadly aligns with Commission version, with some tweaks to provisions on critical operations and management responsibility	**Org requirements**: Broadly aligns with Commission version, with some tweaks to provisions on critical operations and outsourcing
		Review: [no position]	**Review:** The ESAs or national regulators of any host member state can request the national regulator of the home member state to examine whether the FISP still complies with the conditions of authorisation	**Review:** National regulators of any host member state can request the national regulator of the home member state to examine whether the FISP still complies with the conditions of authorisation
	Legal Representatives	• Third country FISPs (no establishment in the EU): They shall designate, in writing, a legal or natural person as their legal rep in one of the member states from where the FISP intends to access data • The legal rep must be mandated to be addressed in addition to, or instead of, the FISP by regulators on all issues relating to FIDA. • FISPs shall provide the legal rep with the powers and resources necessary to enable them to co-operate with regulators and ensure compliance • Legal reps may be liable for non-compliance (without prejudice to any liability of the FISP) • FISPs must notify to the regulator of the member state in which the legal rep resides or is established, details of the legal rep, and ensure the information is up to date • Designating a legal rep will not constitute an establishment of the FISP in the EU.	[Deletes Commission version]	[Deletes Commission version]
Cross Border Access to Data (a.28)	Financial Institutions	Allowed to access Data of EU customers held by Data Holders in the EU	[Broadly aligns with Commission version]	[Broadly aligns with Commission version]
	FISPs	• Allowed to access Data of EU customers held by Data Holders in the EU, but if wish to access Data for the 1st time in a member state other than its home member state, must communicate information for its home regulator: ○ Name, address ○ Member state in which it intends to access Data ○ Type of data ○ FDSS of which is it a member ○ Any outsourcing of operational functions • The home regulator will send the data to the host regulator within 1 month	Broadly aligns with Commission version with some tweaks, and adds that where the host regulator has reasonable grounds to live the FISP acting in its territory, infringes the provisions of FIDA re: the use of the data of customers located in the host member state, it has the power to temporarily suspend transmission of data of those customers from Data Holders to that FISP, until the home regulator has taken necessary measures to end the infringement	Broadly aligns with Commission version with some tweaks, and adds that the ESAs will develop RTS specifying the framework for cooperation and exchange of information between host and home state regulators
Regulator powers (a.17-27)		Various powers assigned to be assigned to national regulators	Broadly aligns with Commission version but:	Broadly aligns with Commission version but adds:

Topic	Sub-topic	Commission proposals	Parliament proposals	Council proposals
			• Qualifies the ability to request freezing/sequestration of assess *in accordance with national law* • Increases the max. administrative fines applicable to natural persons from EUR25k per infringement or EUR250k per year to EUR35k per infringement or EUR350k per year • Increases the max. administrative fines applicable to legal persons from EUR50k per infringement, EUR500k per year and 2% of total annual turnover, to EUR160k per infringement, EUR1.6million per year and 4.5% of total annual turnover • Includes a consideration of whether or not the breach was notified to it by the controlled or processor, when competent authorities are considering the type and level of penalties to apply	• Power to require FISPs to remove members of the management body when they fail to comply with A.12(2)(h) [good repute, possess appropriate knowledge and experience] • Qualifies the ability to request freezing/sequestration of assess *insofar as permitted by national law* • Increases the max. administrative fines applicable to natural persons to up to EUR5million • Deletes the power, in relation to repeated infringements, to ban for at least 10 years any member of the management body of a FISP • Increases the max. administrative fines applicable to legal persons from EUR50k per infringement, EUR500k per year and 2% of total annual turnover, to EUR5million and 10% of total annual turnover
Application of FIDA (a.36)		Provisions will apply 24 months after FIDA enters into force	Provisions will apply *32 months* after FIDA enters into force (but A.9-13 will apply *30 months* after FIDA enters into force. However application to entities when acting as Data Holders or Data Users, the provisions will apply *38 months* after FIDA enters into force (with A.9-13 applying *36 months* after FIDA enters into force)	• For tranche 1 types of customer data provisions will apply 24 months after FIDA enters into force (with A.9-11 applying after 18 months) • For tranche 2 provisions will apply 36 months after FIDA enters into force (with A.9-11 applying after 30 months) • For tranche 2 provisions will apply 48 months after FIDA enters into force (with A.9-11 applying after 42 months)