Consultation Response

European Commission - Data Act

3 September 2021

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the European Commission Consultation Paper on the **DATA ACT**. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate for stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

For completeness, please find below the multiple choice and short form answers included in our Data Act EU Survey response, followed in most cases by additional explanation, rationale and/or detail. We look forward to continuing to support the European Commission in this important initiative.

Consultation Response Sections

Section 1. Business-to-government data sharing for the public interest

1.1a. Have you or has your organisation experienced difficulties/encountered issues when requesting or responding to requests for access to data, in the context of B2G data sharing for the public interest?

- **Yes**
- No
- I don't know / no opinion

1.1b. Please specify. 200 characters max

Short form answer:

Association for Financial Markets in Europe
London Office: 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 788 3971
Frankfurt Office: Bürohaus an der Alten Oper, Neue Mainzer Straße 75, 60311 Frankfurt am Main, Germany
T: +49 (0)69 153 258 963
www.afme.eu

Increased data requests from public authorities during COVID19 have created difficulties where they result in multiple or duplicative requests. Additional requests should be prioritised based on need.

Financial services have seen an increased number of data requests during the COVID19 pandemic from public sector authorities (e.g. financial regulators and supervisors). AFME members have noted that this created difficulties where it resulted in multiple or duplicative requests from national and regional public sector authorities (e.g. additional resourcing required to respond to requests in parallel to all other business as usual data requests and reporting). We believe that additional requests for B2G data sharing should be prioritised, wherever possible, on their need, leveraging previously generated data, and be standardised.

1.2. Should the EU take additional action so that public sector bodies can access and re-use private sector data when this data is needed for them to carry out their tasks in the public interest purpose?

- EU level action is needed
- Action at Member State level only is needed
- No action is needed
- **I don't know / no opinion**

1.3a. To what extent do you believe that the following factors impede B2G data sharing for the public interest in the EU?

	Strongly agree	**Somewhat agree**	**Neutral**	**Somewhat disagree**	**Strongly disagree**	**I don't know/no opinion**
Legal uncertainty due to different rules across Member States		**X**				
Legal barriers to the use of business data for the public interest (e.g. on what data can be shared, in what form, conditions for re-use), including competition rules			**X**			
Commercial disincentives or lack of incentives/interest/ willingness		**X**				
Lack of skilled professionals (public and/or private sector)						**X**
Lack of bodies to help bring together supply and demand for data, and to promote, support and oversee B2G data sharing (e.g. provide best practice, legal advice)		**X**				
Lack of safeguards ensuring that the data will be used only for the public interest purpose for which it was requested		**X**				
Lack of appropriate infrastructures and cost of providing or processing such data (e.g. interoperability issues)		**X**				

Lack of awareness (benefits, datasets available)		**X**				
Insufficient quality of public authorities' privacy and data protection tools		**X**				
Other						**X**

1.3b. Please specify. 200 characters max

Short form answer:

It will be important to clarify whether the Data Act will take precedence over local laws regarding client confidentiality and secrecy, which could create conflicting requirements and impede sharing.

It will be important to clarify whether the Data Act will take precedence over local laws regarding client confidentiality and secrecy laws. This could result in conflicting laws or requirements and act to impede B2G data sharing. For instance, existing rules relating to data sharing in the Market Abuse Directive, Takeover Directive and Transparency Directive could conflict with various requirements proposed in this Data Act.

AFME members have also highlighted other factors which can impede B2G data sharing. These include:

- A lack of harmonised B2G transfer mechanisms with corresponding APIs,
- Technical limitations for public authorities to read and capture unstructured data,
- The absence of consistent data descriptions or data taxonomies, including how the data has been gathered that allows data collection to be comparable,
- A lack of standardisation (i.e. which questions can be answered with the same data/information), and
- A lack of prioritisation of data requests.

We also note that no proposals have been included regarding government-to-business (G2B) data sharing. We believe there are considerable benefits in creating a two-way data-sharing mechanism to facilitate greater efficiencies and collaboration between the public and private sector.

1.4a. In which of the following areas do you think that, for specific use-cases with a clear public interest, B2G data sharing should be compulsory, with appropriate safeguards?

	Yes, it should be compulsory	No, it should not be compulsory	I don't know/no opinion
Data (e.g. mobility data from Telecom operators, loss data from insurance companies) for emergencies and crisis management, prevention and resilience			**X**
Data (e.g. price data from supermarkets) for official statistics			**X**
Data (e.g. emissions data from manufacturing plants) for protecting the environment			**X**
Data (e.g. fuel consumption data from transport operators) for a healthier society			**X**
Data for better public education services			**X**
Data (e.g. employment data from companies) for a socially inclusive society		**X**	

Data for evidence-based public service delivery and policymaking		**X**	
Other			**X**

1.4b. Please specify. 200 characters max

Short form answer:

We recommend more granular definitions of 'public interest' and 'the common good', minimising use cases for personal data sharing and clarifying how individual data subject rights will be enforced.

AFME members support data sharing for the public interest in full respect of data protection rights. However, the terms '*public interest*' and *'the common good',* as stated in this consultation, are broad and without limitation. Therefore, we believe that a more granular definition of public interest, and a supporting framework for data sharing in this regard, should be the first step before identifying potential use-cases and the required data. This would also provide greater legal certainty to businesses in the scope of this initiative. This approach will also address other important considerations such as data standardisation and quality, minimum expected protection needs, cost and commercial sensitivities, personal data protection, ethics and security (e.g. potential data breaches).

Regarding the B2G sharing of personal data, it is our view that there should be minimal use cases for the sharing of personal data, and that in all cases, personal data should only be shared at an aggregated level and anonymised as necessary.

Regarding data protection, more generally, existing legislative frameworks should be leveraged wherever possible. For example, any sharing should meet requirements set out in the data protection framework. It should be clear why the sharing is necessary/proportionate to the purpose.

Regarding the protection of data subjects, particularly in the context of wholesale sharing with multiple entities, any future legislation must be clear in how individual rights will be enforced. Furthermore, data sharing between entities will need to be carefully documented; for instance, it should be clear to the data subject which entities in the data value chain to approach to enforce their rights.

Regarding specific use-cases, we are of the view that existing processes for data sharing relating to fraud detection, Anti-Money Laundering/Counter-Terrorist Financing (AML/CFT) or cybersecurity could be enhanced within the B2G data sharing framework.

1.5a. When sharing data with public bodies, businesses should provide it:

- For free
- At a preferential rate/ below market price (marginal cost or other)
- At market price
- **Depending on the purpose it may be provided at market price, preferential rate or for free**
- I don't know/ no opinion

1.5b. Please provide an example(s) of when public sector bodies should be able to obtain data for the public interest at a preferential rate. (no character limit)

AFME members believe that the provision and monetisation of data for the public interest will be dependent on the data being shared and the specific use case (see the answer to Q1.4b). For example, it may be appropriate to provide data free at the point of delivery where there is a universally agreed public interest within an industry sector. However, where

data is requested by public sectors bodies and shared for a commercial benefit (e.g. profit) a fee may be appropriate for the investment required by the relevant organisations to supply the data.

However, it is complex to determine the *market price* or a *preferential rate* for data due to multiple data sources and the different interpretations of value that could be applied. It is important to consider how essential the data is for the provision of services, as well as the business time, effort and knowledge required to provide this data. Ultimately, we believe this will depend on the specific use-case and the nature of the data required on a case-by-case basis.

1.6a. What safeguards for B2G data sharing would be appropriate? (select all that apply)

- **Data security measures including protection of commercially sensitive information**
- **Specific rules on proportionality and reasonableness of the request**
- **Transparent reporting on how the public authority has used the data**
- **Limitations regarding how long public bodies may use or store specific datasets before having to destroy them**
- **Other**

1.6b. Please specify. 200 characters max

Short form answer:

We believe that confidentiality, transfer mechanisms, consistent descriptions, trust, and personal data protection with limited use cases must also be considered.

AFME members agree with the safeguards listed and believe that the following items must also be considered for B2G data sharing:

- Confidentiality: Limitations on how the data can be used, and requirements for the data (or specific fields or attributes) to be anonymised where necessary,
- Transfer mechanisms: Harmonised transfer mechanisms, with corresponding API standards, for the secure and efficient transit of data,
- Consistent descriptions: Standards for the consolidation of different data types across (and within) industry sectors,
- Trust: Appropriate checks on the quality of data submitted to provide assurances on the suitability of its use, and
- Personal data protection: as stated in our response to Q1.4b, personal data should be anonymised or aggregated before sharing. This should be limited to specific use cases where clear value-add has been identified.

1.7. Which of the following types of financial compensation would incentivise you to engage in a B2G data-sharing collaboration for the public interest (select all that apply):

- Marginal costs for dissemination
- Marginal costs for dissemination + fair return on investment (ROI)
- Market price

AFME has not responded to this question.

1.8a. Which of the following types of non-monetary compensation would incentivise you to engage in a B2G data-sharing collaboration for the public interest (select all that apply):

- Tax incentives

- **Increased know-how and innovation through co-creation with public bodies**
- **Reputation/ public recognition programmes (e.g. corporate social responsibility)**
- **Investment of public funds to support the development of trusted technical tools for B2G data sharing**
- I don't know / no opinion
- **Other**

1.8b. Please specify. 200 characters max

Short form answer:

Non-monetary compensation could include public-private collaboration on non-public interest initiatives (e.g. initiatives to improve the efficiency of existing reporting obligations).

We note that financial institutions already share data to public authorities for specific initiatives to inform policymaking. We welcome EU authorities in further developing additional channels and safeguards for B2G data sharing to support a data-driven approach to policymaking.

AFME members agree that non-monetary compensation could be helpful for incentivising collaboration and sharing data with public bodies where there is a clear public interest. Financial institutions make significant investments in the safe and secure management of data and incur costs for data sharing to public bodies in this regard (e.g. technical and resourcing requirements). Therefore, non-monetary compensation benefits could be a mechanism to increase the benefits and success of B2G data-sharing initiatives.

Non-monetary compensation could include public bodies and financial institutions collaborating on non-public interest initiatives (e.g. policy initiatives such as improvements to the efficiency of existing reporting obligations). The recent EBA Integrated Reporting Consultation is an example where financial institutions and public bodies can collaborate to improve how existing data is shared (e.g. exploring the use of machine-readable solutions and the development of globally consistent standards).

Other types of non-monetary compensation not listed include mutual benefits, such as increased financial stability, enhanced consumer/investor protection, and the greater availability of public data for business use.

Section 2. Business-to-business data sharing

2.1. Does your company share data with other companies? (This includes providing data to other companies and accessing data from other companies)

- **Yes**
- No
- I don't know / no opinion

2.2. Are you:

- Data holder
- Data user
- **Both data holder and user**
- Other

2.3a. In the last five years, how often has your company shared data with other companies?

- **Many times**
- Only a few times
- Don't know

2.3b. Please describe the type of data shared, and the type of businesses with whom it is shared.

Short form answer:

Most data sharing occurs for specific mandatory requirements (e.g. market data, transaction data, or reporting). which varies in purpose (e.g. regulatory, commercial, innovation).

The financial services sector is one of the most data-intensive sectors in the economy, with the creation, use and transfer of data underpinning almost all aspects of the industry (e.g., the collation and dissemination of market data, or the submission of transaction or regulatory reports).

Within capital markets, data sharing is a mature and fundamental aspect of how the industry operates. Much of the data sharing occurs for specific mandatory requirements (e.g., sharing market data, transaction data, or regulatory reporting) to satisfy regulatory or compliance obligations. However, there is a wide variation in the purposes for data sharing (e.g. regulatory, commercial, innovation).

Data sharing is complex and involves a wide range of industry participants performing different roles (e.g. banks, financial market infrastructures, public bodies, industry utilities). Moreover, the sharing of data takes place bilaterally (e.g. bank to bank, bank to the regulator, bank to non-bank) and via multilateral platforms (e.g. industry utilities, financial market infrastructures, exchanges). Therefore, the types of data shared (e.g. personal and non-personal), and types of businesses with whom it is shared, is extensive both within the EU and globally (e.g. cross-border). There is also a wide variation in the purposes for data sharing (e.g., regulatory, commercial, innovation). For and across commercial, regulatory, and innovative purposes, the pricing and contractual arrangements will vary, depending on the negotiating conditions of these arrangements. It is important to consider these complex dynamics, as well as existing laws and regulations restricting data sharing, when considering regulatory intervention to business-to-business data sharing.

2.4. On what basis does your company share data with other companies?

- Voluntary

- Mandatory
- **Both voluntary and mandatory**
- I don't know / No opinion

2.5a. Why does your company share data with other companies? (select all that apply)

- Optimisation of the supply chain
- Predictive maintenance
- Precision farming
- Moving to circular production
- Training algorithms for AI
- Design of innovative solutions/products
- **Other**

2.5b. Please specify. 200 characters max

Short form answer:

For mandatory (e.g. compliance) or voluntary (e.g. industry efficiency in the form of shared trading platforms or commercial obligations) reasons.

AFME members share a wide range of data with other companies (e.g. banks and non-banks) for a wide variety of reasons. This data sharing may be mandatory (e.g. for regulatory compliance) or voluntary (e.g. for industry efficiency in the form of shared trading platforms or commercial obligations such as using a third party to provide data or application services).

2.6. Which services/products based on data sharing exist/are under development in your sector and what type of data are needed for these purposes? 300 characters max

Short form answer:

Capital markets examples include: EU consolidated tape (CT) for post-trade data under MiFID II/R to increase the transparency, availability, and efficiency of aggregated market data, and the ISDA Common Domain Model (CDM) to develop shared data standards.

There are many mature examples of services/products based on data sharing in the capital markets sector, for example, the use of Financial Market Infrastructures (FMIs) that provide trade settlement and clearing services (e.g. the sharing of securities data). More broadly, within the payments industry, data sharing involves multiple parties.

There are also initiatives underway within the capital markets industry, both regulatory and non-regulatory led, that focus on increasing data sharing. For example:

- The European Commission regulatory initiative to establish a consolidated tape (CT) for post-trade data under MiFID II/R, to increase the transparency, availability, and efficiency of aggregated market data, and
- The ISDA industry initiative to develop a Common Domain Model (CDM), and shared data standards, to improve the efficiency of the trade lifecycle efficiency clients and regulators.

Data sharing in capital markets impacts and benefits market participants in different ways; for example, what data and format are helpful for a bank will differ from that of an investor. In addition, data sharing can be focused on a specific asset class (e.g. equities trading) or apply horizontally (e.g. data sharing for improving anti-money laundering for all asset classes).

2.7. What benefits from data sharing do you expect to be reaped in your sector? 300 characters max

Short form answer:

Improved client products and services, operational and cost efficiencies, innovation and sustainability, and improvements in regulatory and compliance requirements (e.g. sharing cybersecurity incident data to increase industry resilience, or public financial disclosures to develop ESG products).

Increased data sharing could benefit to European capital markets for improved client products and services, operational and cost efficiencies, innovation and sustainability, and improvements in regulatory and compliance requirements. For example:

- The sharing of cybersecurity incident data between financial institutions within trusted networks on a near real-time basis to increase the overall resilience of the industry to disruption, or
- The sharing of public financial disclosures to develop new sustainable financial products.

The benefits and use cases derived from data sharing will be enhanced when cross-border and cross-sectoral data flows are enabled. Some of these benefits include enabling centralised risk management and screening to improve financial crime detection or improving decisions on credit allocation to provide improved client service and returns and improved knowledge of cyber threats.

Many of the benefits from data sharing derive from the use of new technologies such as Artificial Intelligence (AI), Machine Learning (ML) or Cloud Computing (e.g. using AI/ML to develop machine-readable reporting capabilities). Combining data sharing and new technologies will be essential for enabling capital markets financial institutions to adapt to an increasingly digital world. These benefits and opportunities from data sharing in the capital markets will ultimately support the development of an EU Single Market for Data and further enhance the value of the European data economy.

2.8. Has your company experienced difficulties/encountered issues when requesting access to other companies' data?

- **Yes**
- No
- I don't know / no opinion

2.9. How often did such difficulties occur in the last 5 years?

- Very often
- Often
- Sometimes
- Rarely
- **I don't know / no opinion**

2.10a. What was the nature of such difficulties/issues? (select all that apply)

- The data holder refused to give data on the basis of competition law concerns
- The data holder refused to give access to data for reasons other than competition law concerns
- The data holder is prevented by law to give access to data
- There is no legal basis for the data holder to give access to data
- The data holder gave access to data at unreasonable conditions, e.g. unilateral change of contractual terms, disproportionate restriction of use of data, limitations in the termination of contract
- The data holder gave access to data at an unreasonable price
- Technical reasons like the data was not in usable format or quality or lacks shared vocabularies or metadata or the data holder doesn't support standards for enforce data usage controls (connector)
- **Other**
- I don't know / no opinion

2.10b. Please indicate the type of difficulties / issues. 200 characters max

Short form answer:

A lack of effective mechanisms to allow secure sharing. A lack of robust and sound governance in third party data management. Difficulties accessing where there is an imbalance of bargaining power.

There is a wide range of difficulties that can be encountered when requesting access to other companies' data. However, AFME members wish to highlight:

- A lack of effective mechanisms to allow financial institutions or other organisations to share and reuse data safely. Some financial institutions have faced difficulties using data from other non-financial organisations, either because data is unavailable or access is denied or a lack of technical interoperability, transfer mechanisms or appropriate security measures,
- Difficulties faced by financial institutions accessing certain data types where other organisations have greater bargaining power (where other valued data can be offered in return in full compliance with GDPR). In some cases, access to data held by non-financial organisations, such as technology platform providers, has been sought as part of bilateral arrangements but with limited success, and
- A lack of robust and sound governance in data management from third parties has resulted in regulators and supervisors advising against the use of shared data for certain banking use cases.

AFME members believe that data sharing must be driven across multiple sectors and not just within sectors (e.g. financial services), subject to the appropriate protections being in place. Increased standardisation of data types, and formats, across sectors, will be essential to facilitate this effective data sharing. European supervisory authorities and standards-setting bodies and global organisations will have an important coordinating role to play in achieving greater data sharing.

2.11. Do you agree that the application of a 'fairness test', to prevent unilateral imposition by one party of unfair contractual terms on another, could contribute to increasing data sharing between businesses (including for example co-generated non-personal IoT data in professional use)?

- **Yes**
- No
- I don't know / no opinion

2.12. Do you agree that model contract terms for voluntary use in B2B data sharing contracts could contribute to increasing data sharing between businesses (including for example co-generated non-personal IoT data in professional use)?

- **Yes**
- No
- I don't know/ no opinion

2.13. Do you agree that horizontal access modalities based on variations of fair, reasonable and non-discriminatory conditions applicable to data access rights, established in specific sectors, could contribute to increasing data sharing between businesses (including for example co-generated non-personal IoT data in professional use)?

- **Yes**
- No
- I don't know / no opinion

2.14. What, in you view, could be the benefits or risks of the options mentioned in the three previous questions, for example in relation to incentives for data collection, competitiveness and administrative burden. 300 characters max

Short form answer:

Further info on the criteria to determine fairness, who will perform the test, and whether the results could be challenged, is needed. It is unclear how enforcement of excesses in contractual clauses will be addressed. Any horizontal data modalities should be principles-based and voluntary.

AFME members welcome the Commission's efforts to increase B2B data sharing, bringing a range of opportunities within and across industry sectors and ensuring that the EU economy can remain competitive through its ambitions of a single market for data. However, for this objective to be achieved, any measures taken must:

- Apply across multiple sectors,
- Facilitate access to personal and non-personal data,
- Ensure the secure transmission and interoperability of data, and
- Based on a robust legal framework consistent with existing legal and regulatory obligations.

We recommend that any measures taken should complement other global frameworks to ensure the cross-border flow of data within and outside of Europe.

To support innovation and ensure a level playing field, any tools to incentivise data sharing must appropriately safeguard the freedom of contract and be fully compliant with competition law. While voluntary mechanisms are welcomed, we caution against the introduction of tools that may, in effect, lead to mandatory sharing of data that is the intellectual property of the contracting party. Such tools can have the effect of disincentivising innovation within firms if the benefits or insight from this work must be shared under mandatory requirements.

We want to raise the following considerations for the three policy options presented in this consultation for increasing B2B data sharing:

A legislative fairness test

A minimum, non-binding, harmonisation measure for B2B data sharing contracts could provide a valuable baseline for organisations establishing such arrangements (e.g. providing general contractual guidance consistent with other legislation, such as GDPR). A non-binding fairness test would also allow organisations to contract data sharing arrangements based on their specific legal, compliance, commercial, and technical requirements, unique to each use case.

We welcome more information on what criteria will be used to determine fairness, who will perform the test, whether the results could be challenged, and what the consequences are, if any, from the result. Criteria could, for example, consider characteristics of "unfair" behaviour (e.g. unreasonable and excessive payments terms, unfair or prohibitive restrictions around rights of use/aggregation). This principles-based approach may be more effective to implement across different relationships/sectors.

In addition, it is unclear how any enforcement of excesses in contractual clauses would be addressed under this arrangement (e.g. responsible bodies for managing dispute resolution, enforcement of remediating actions, subsequent penalties or punitive action, exclusions and limitations of liability, term and termination provisions). It is also unclear how *excessive clauses* would be identified for developing the general boundaries where the fairness test would apply due to the wide range of B2B data sharing arrangements and data types where it could apply. It will be essential to ensure that any fairness test or general contractual boundaries for data sharing contracts do not inadvertently create price regulation or impact competition. For example, a fairness test should not determine the *market price* or a *preferential rate* for data due to the multiple data sources that may exist and the different interpretations of value that could be applied.

A fairness test may also need to consider how it is applied to different types of data (e.g. data sharing for compliance or regulatory purposes, or business as usual service provision and innovation). Further, a fairness test must also consider how to balance being prescriptive versus proportionate in how it is applied to different data types, and more broadly.

A fairness test should leverage existing legislative frameworks, such as the competition law requirements, to reduce legal uncertainty and help ensure fair treatment and a level playing field. We welcome further detail from the European Commission in what the fairness test would entail.

Model contract terms

Model contractual clauses could provide helpful guidance for organisations to determine the practical compliance and legal aspects required for B2B data sharing contracts, provided that the terms used are proportionate, fair and reasonable.

We believe that model contractual terms are best where they are voluntary, in the form of a compliance tool, rather than providing prescriptive terms. This is because no one-size-fits-all approach to B2B data sharing arrangements will exist, and flexibility is required to ensure appropriate contracts for both parties (e.g., the commercial, technical, legal and compliance requirements specific to the use case). This approach will also limit the potential administrative burden for parties engaging in contractual discussions based on a specific dataset or use case (e.g., allowing a risk-based approach).

Further clarity is also needed on how any model contract clauses would be introduced, the proposed terms, and any potential governance mechanisms (e.g., ongoing monitoring or updates of the clauses). In addition, for any model contractual clauses to be practical, they must compliment and harmonise existing EU data contract frameworks and regulations (e.g. GDPR).

Horizontal access modalities

Horizontal access modalities for data sharing will help ensure that data sharing is viewed from an end-to-end use-case perspective rather than within a specific sector (e.g. financial services only). Data sharing must be driven across multiple sectors, particularly as new entrants emerge. Any requirements (where they are mandatory) must be applied equally to market participants to maintain a level playing field. Horizontal modalities could also help increase the standardisation of data types and formats across sectors which will be essential to facilitate effective data sharing (and alignment to other horizontal data legislation such as GDPR).

It will be vital that any sectoral data access initiatives or legislation are consistent with the horizontal access modalities to prevent introducing greater complexity or fragmentation for B2B data sharing within sectors. Further clarity is required on the terms of *fair, reasonable, proportionate, transparent* and *non-discriminatory*, and how they will be consistent with existing horizontal (e.g. GDPR) and sectoral legislation.

Finally, it is unclear which data types and B2B use cases the horizontal modalities would apply. For example, what constitutes *commercially sensitive data* or data *strategic for competition*, as stated in the consultation. There is a risk that any horizontal modalities could be too specific in their focus or approach (e.g. not including personal data sharing use-cases), increasing the burden on organisations to comply.

We believe that any introduction of horizontal data modalities should be principles-based, voluntary, and apply to the broadest data types and use-cases. This approach will provide flexibility for organisations to ensure the objectives of the modalities can be satisfied on a case-by-case basis and provide flexibility for any sector-specific initiatives or legislation to be developed.

2.15a. Regarding data access at fair, reasonable, proportionate, transparent, and non-discriminatory conditions, which of the following elements do you consider most relevant to increase data sharing? (maximum of 3 choices)

- **The party sharing data obtains a reasonable yield on investment and the party requesting access to data pays a reasonable fee**
- **Distinctions can be made depending on the type of data or the purpose of its use**
- **Availability of standards for interoperability that would allow data sharing and exploitation at a low marginal cost (in terms of time and money)**

- Structures enabling the use of data for computation without actually disclosing the data
- Availability of an impartial dispute settlement mechanism
- None of the above
- **Other**
- I don't know / no opinion

2.15b. Please explain. 200 characters max

Short form answer:

Determining the market price or a preferential rate for data should be done on a case-by-case basis. This will depend on the specific use-case and nature of the data required.

We find the following areas relevant to increase data-sharing:

- Reciprocal data sharing arrangements, to ensure alignment of incentives,
- Enhanced interoperability and standards (such as standardisation of APIs), which could include for example maximum API response times, minimum API uptimes, and the removal of artificial barriers during the user journey, and
- Standardisation of data definitions.

Regarding the sharing of data with "a reasonable yield on investment and the party requesting access to data pays a reasonable fee" we note that there are certain instances where monetisation would be appropriate, for instance for elaborated/inferred data, including validated data, where costs were incurred for the collection and processing of the data. It must be considered that it is complex to determine the *market price* or a *preferential rate* for data due to multiple data sources and the different interpretations of value that could be applied. It is important to consider how essential the data is for the provision of services, as well as the business time, effort and knowledge required to provide this data. Ultimately, we believe this will depend on the specific use-case and nature of the data required on a case-by-case basis.

Section 3. Tools for data sharing: smart contracts

3.1a. Are you using smart contracts or have you been involved in proofs of concept or pilots for Distributed Ledger Technologies that make use of smart contracts?

- **Yes**
- No

3.1b. Please briefly explain the use case(s) you tested. 200 characters max

Short form answer:

Use cases include using DLT and smart contracts to increase the efficiency and reduce the transaction time for the trade lifecycle (such as conducting equity swaps between counterparties).

The financial services sector continues to explore and adopt a wide range of use-cases for Distributed Ledger Technology (DLT) and smart contract functionality. For example, using both DLT and smart contracts to increase the efficiency and reduce the transaction time for the trade lifecycle (such as conducting equity swaps between counterparties).

3.2a. Do you consider that smart contracts could be an effective tool to technically implement the data access and use in the context of co-generated IoT data, in particular where the transfer is not only one-off but would involve some form of continuous data sharing?

- Yes
- No

AFME has not responded to this question.

3.2b. Please explain your answer.

AFME has not responded to this question.

3.3a. Do you consider that when individuals request data portability from businesses, smart contracts could be an effective tool to technically implement data transfers, in particular where the transmission is not only one-off but would involve some form of continuous data sharing?

- **Yes**
- No

3.3b. Please explain your answer. 200 characters max

Short form answer:

Benefits include enhanced transparency and traceability, increased trust, reduced need for a central operator. However, some legal and technical issues must be addressed (please see attachment).

We note that smart contracts technology could potentially bring a wide range of benefits to the financial services sector, such as:

- Enhanced transparency and traceability,
- Increased trust in the contracting process (e.g., decisions agreed and codified by all parties), and
- Reduced need for a central operator or external enforcement mechanism, reducing costs and the need for intermediaries.

However, there are also areas that need to be considered for smart contracts to be used as an effective tool for data transfers. These include:

- Ensuring the legal validity of the contract, particularly across jurisdictions,
- Determining the form of the smart contract (code, written English, written other, or a hybrid),
- Interpreting terms, particularly if written in code, to confirm that the terms reflect the parties' intentions,
- Enforceability of terms in cases of ambiguity,
- Determining who is a party to the contract,
- Maintaining a user or organisations control over their data once codified, and
- Managing inflexibility of the current technological capability in which changes may be needed on an ongoing basis.

3.4a. In your experience, what are the primary challenges for scaling smart contracts across blockchains and/or across ecosystems? Are these challenges related to: (0 lowest, 10 highest)

	1	2	3	4	5	6	7	8	9	10
Legal uncertainty					**X**					
Lack of interoperability									**X**	
Difficulties with governance							**X**			
Data protection issues								**X**		

Competition law					**X**					
Compliance concerns					**X**					
Other – Blockchain issues								**X**		

3.4b. Other: Please specify (no limit)

We note there are challenges to storing large volumes of data on a blockchain (e.g. relating to latency and data processing) due to how transactions are used to store data (e.g. data stored is either 'scarce' or a reference to external data).

We also note that smart contracts would be useful for controlling shared data, keeping an audit trail of data sharing and activity, and for verifying the authenticity of the data sources, however due to immutability of blockchain no personal information could be stored.

3.5. If interoperability is an issue for scaling smart contracts, which requirements should inform standardisation to scale smart contracts across blockchains and/or across ecosystems? Should such standards determine in particular minimum safeguards for cyber security? If so, which best practices would you consider relevant. 300 characters max

Short form answer:

General: the scope/features of smart contracts by sector and use-case, technology neutrality, existing global standards, consistency with sector-specific legislation.
Blockchain-specific: network capabilities, governance, inter-network identities and securities, need for a common meta-data language.

Requirements to inform the standardisation of smart contracts should consider:

- The scope and features of smart contracts to be included by industry sector and use-case,
- Technology neutrality to allow flexibility in the development of smart contracts (e.g. natural language and code vs only code),
- Harmonisation with existing global standards to ensure consistency and reduced fragmentation, and
- Consistency with existing sector specific legislation to prevent duplication or barriers for adoption.

Regarding standardisation of smart contracts across blockchains specifically, requirements should consider:

- Network capabilities (e.g. privacy, channels),
- Governance (e.g. how are smart contracts maintained and updated),
- Inter-network identities and security (e.g. network access control), and
- The various programming languages employed in different blockchain networks, in which a common meta-language would be needed to ensure smart contracts can interact.

Further clarity would be welcomed on whether the Data Act intends to legislate any specific future data-sharing arrangements via smart contract technology.

Section 4. Clarifying rights on non-personal Internet-of-Things data [Out of scope]

Section 5. Improving portability for business users of cloud services

5.1. Was your organisation aware of the SWIPO Codes of Conduct prior to filling in this questionnaire?

- **Yes**
- No
- I don't know /no opinion

5.2a. In your opinion, do the self-regulatory SWIPO codes of conduct on data portability developed by the cloud stakeholders represent a suitable approach to address cloud service portability?

- **Yes**
- No
- I don't know /no opinion

5.2b. Please explain. 200 characters max

Short form answer:

Self-regulatory approaches allow for a flexible adaption to technologies and services, such as cloud computing, noting that SWIPO CoCs may require further changes as the membership increases.

AFME is supportive of self-regulatory approaches as a useful means to address some of the industry challenges faced with cloud service portability (such as managing exits from cloud service providers under different scenarios). This is because self-regulatory approaches allow for a flexible adaption to technologies and services, such as cloud computing, which is continuing to mature and develop at a pace. We also recognise that this was the opinion supported in the recent public consultation on a European Strategy for Data.[1]

Self-regulatory measures can be more easily amended to ensure they remain fit for purpose over time. However, we recognise that the SWIPO CoCs have only been adopted since 2020 as a tool for addressing cloud service portability. Additional time is needed to assess their effectiveness and any changes required as the cloud services market and adoption continue to develop in financial services. We also note that the SWIPO CoCs were originally developed by a limited number of members, which may necessitate further changes as the current membership and the CoC usage increases.

Finally, we believe that attention will need to be paid to the auditability and enforceability of CoCs, such as SWIPO, to reinforce their use and effectiveness (such as independence assurance). Independent assurances could provide further testing, and evidence of compliance of a third-party service provider, to the CoC.

5.2c. In your opinion, could the self-regulatory SWIPO codes of conduct represent a suitable approach to address cloud portability if?

- The principles formulated in the self-regulatory SWIPO codes of conduct would be binding for all cloud services offered in Europe
- The codes of conduct would be supplemented by Standard Contractual Clauses translating the Codes' requirement into contractual elements
- Both
- **Other**

AFME believes that any approaches to address cloud service portability should remain voluntary. This is because a voluntary approach will limit any further compliance obligations being introduced for financial institutions that could

[1] https://www.afme.eu/Portals/0/DispatchFeaturedImages/2020%2005%2029%20AFME%20EC%20European%20Strategy%20for%20Data%20response%20(FINAL)_CLEAN.pdf

directly or inadvertently impact technical, commercial, or contractual elements of cloud service adoption. However, we recognise that the uptake of the SWIPO CoC is limited at this early stage of their adoption and further uptake will be important to identify and address challenges for cloud service portability.

Further, the SWIPO CoCs and legal entity (SWIPO AISBL) were only introduced to the market in 2020. We strongly believe that 12 months is too short a period for gathering industry feedback on the impact of the CoCs. We recommend that the European Commission continues to gather feedback on the CoCs via a public consultation to assess their effectiveness and any potential changes required. This consultation should inform any introduction of further binding or legal requirements for both cloud service providers (CSPs) and cloud service customers (CSC).

AFME has actively supported the European Commission's work as part of the 2018 Fintech Action plan initiative to develop Standard Contractual Clauses (SCCs) for cloud services. We believe that SCCs for cloud services could provide value where they are applied consistently throughout the EU and reduce regulatory fragmentation across the Member States. Further, SCCs could, to some degree, address challenges some firms face in contract negotiation with CSPs. However, whilst SCCs should provide a valuable tool to comply with existing regulatory obligations, such as the 2019 EBA Guidelines on Outsourcing, they should not become an additional compliance obligation for financial institutions. SCCs which become an additional compliance layer would likely contribute to additional cost and complexity for financial institutions and could inadvertently limit or restrict cloud use (and innovation). Further, the intents of both SCCs and the European Commission initiative were broader than data portability. For example, SCCs were considered for areas such as access and audit rights. We believe that any further work or the introduction of SCCs should continue to consider and support the broader range of existing regulatory requirements on financial institutions for cloud adoption. Finally, we continue to strongly advise that further consultation is taken with the industry on any draft SCCs before introducing them to the cloud services market. This further consultation will ensure that the SCCs can provide practical and beneficial outcomes for financial institutions and do not introduce further barriers to cloud adoption in the EU.

5.3a. Do you consider there is a need to establish a right to portability for business users of cloud computing services in EU legislation?

- Yes
- **No**
- I don't know / no opinion

5.3b. Please explain your answer, detailing as much as possible what this right should entail. 200 characters max

Short form answer:

Establishing portability right for cloud services in legislation at this stage could create additional barriers for smaller market providers or reduce the flexibility/ service offerings available.

AFME members welcome the intent of the European Commission to encourage and increase cloud services portability. In our response to the European Data Strategy public consultation,[2] we recognised that financial institutions can face issues with the portability of cloud services (such as variations in the time provided by CSPs for the effective migration of data between providers or to in-house developments). Conversely, we also acknowledged that some portability challenges may always be present (such as for Software as a Service offerings – SaaS – which may have no suitable market alternative).

However, we caution against establishing a right to portability for cloud services in legislation at this stage of cloud adoption in the EU. This is because further engagement with the financial services industry and cloud service providers (CSPs) is required to validate whether such a measure would actively support cloud adoption and innovation within the

[2] https://www.afme.eu/Portals/0/DispatchFeaturedImages/2020%2005%2029%20AFME%20EC%20European%20Strategy%20for%20Data%20response%20(FINAL)_CLEAN.pdf

EU. For example, legislating for cloud services portability could inadvertently reduce competition for cloud services by creating additional barriers for smaller market providers or reduce the flexibility and service offerings available for financial institutions.

We recommend further engagement with the financial services industry and CSPs to assess the options for supporting cloud services portability and the potential duplication of other measures such as the SWIPO codes of conduct (CoCs) or anticipated requirements within the digital finance package (such as the Digital Operational Resilience Act (DORA)). For example, exploring other possible non-legislative approaches for increasing the level of adherence and assurance of a CSPs compliance to the SWIPO CoC (such as independent testing and evidence of compliance).

5.4a. What legislative approach would be the most suitable in your opinion, if the data portability right for cloud users would be laid down in an EU legislation? (select all that apply)

1. High-level principle(s) recognising the right for cloud service portability (for example, a provision stipulating that the cloud user has the right to have its data ported in a structured, widely used and machine-readable format to another provider or proprietary servers, against minimum thresholds)
2. More specific set of conditions of contractual, technical, commercial and economic nature, including specification of the necessary elements to enable data portability
3. **Other solution**
4. I don't know / no opinion

5.4b. Please explain. 200 characters max

Short form answer:
Further engagement with the financial services industry, and CSPs, is needed to assess options for supporting portability to avoid reducing the unique arrangements and offerings of FIs and CSPs.

AFME members welcome the intent of the European Commission to encourage and increase cloud services portability (recognising the benefits of approaches such as the SWIPO CoCs and SCCs). We recommend that further engagement with the financial services industry, and CSPs, is needed to assess options for supporting cloud services portability. We believe that stipulating set conditions (such as contractual requirements) or technical standards (such as set formats for data extraction) could, to some degree, address challenges some firms face in contract negotiation with CSPs. However, we recognise that legislating such approaches, rather than continuing to focus on voluntary mechanisms, would be a highly complex task and could directly, or inadvertently, limit cloud services adoption in the EU. For example, legislating portability requirements may reduce the flexibility, or unique arrangements and offerings, of financial institutions and CSPs. Further, granular principles or contractual requirements could become obsolete very quickly as cloud technology and its use continues to mature (such as advances in machine-readable tools and data formats).

We also acknowledge the wide range of cloud service offerings and deployment models that need to be considered from a portability aspect. This variation could result in any legislative proposal (such as high-level principles) having a limited impact or duplicating existing industry measures (such as the SWIPO codes of conduct).

5.5a. Would the self-regulatory SWIPO codes of conduct on data portability developed by the cloud stakeholders in your opinion represent a suitable baseline for the development of such a legislative cloud service portability right?

- Yes
- Yes, but further elements would have to be considered (please be as specific as possible on which elements are currently not/insufficiently addressed in those codes of conduct – optional)
- No
- **No opinion**

- I am not familiar with SWIPO codes of conduct

5.5b. Please explain. 200 characters max

Short form answer:

Using the CoCs for any future cloud services portability legislation would be a complex undertaking and we caution against establishing a right to portability for cloud services in EU legislation.

We recognise the significant efforts of the European Commission, and SWIPO AISBL, to develop robust codes of conduct (CoC) on IaaS and SaaS cloud service portability. The CoCs are a fair and representative baseline of requirements for portability. They will be important tools for improving transparency and collaboration between cloud service providers (CSPs) and cloud service customers (CSCs). We recognise that further, attention will need to be paid to the auditability and enforceability of CoCs, such as SWIPO to reinforce their use and effectiveness (such as independence assurance). Independent assurances could provide further testing, and evidence of compliance of a third-party service provider to the CoC.

However, we stress that using the CoCs for any future cloud services portability legislation would be a complex undertaking, as identified in previous answers. For example, needing to cover the wide range of cloud service offerings and deployment models that exist and potentially becoming obsolete over time as cloud services technology and use continue to mature.

We caution against establishing a right to portability for cloud services in EU legislation. We believe that in maintaining a self-regulatory approach to cloud services data portability, however we recognise that more could be done to encourage portability (such as possible independent assurances as mentioned above). We encourage further engagement with the financial services industry and CSPs to determine what additional measures, if any, are required to support data portability for cloud services.

5.6a. Would it be suitable to develop – as a part of legislative approach to cloud service portability - standard APIs, open standards and interoperable data formats, timeframes and potentially other technical elements?

- Yes
- **No**
- I don't know / no opinion

5.6b. Can you be more specific about which standards should be developed in this regard? 200 characters max

Short form answer:

There is a risk that any standards developed will become quickly obsolete as the cloud service market and technical approaches (such as APIs) continue to mature at a pace.

AFME members welcome the intent of the European Commission to encourage and increase cloud services portability (recognising the benefits of approaches such as the SWIPO CoC and SCCs). We believe it is important to recognise the distinction between the approach and value of self-regulatory measures, such as CoC and SCCs, and exploring further options to strengthen their adoption and enforceability; in comparison to adopting these measures in their current form in legislation.

In line with our responses above, we caution against legislating specific and granular technical requirements for cloud services portability. Legislating specific technical requirements (such as data formats) could limit the flexibility required by financial institutions to adopt cloud services based on their individual needs and could also limit the services made available from cloud service providers (CSPs). For example, legislative technical requirements could overly standardise offerings and reduce the potential differentiation offered to each customer's unique needs. Further, legislating timelines for data portability could increase operational risk if they reduce the flexibility needed for individual use-cases or

situations (such as allowing cloud service customers to take a risk-based approach when there is a need for data portability).

We also recognise the significant effort and industry involvement in standards exercises, such as creating new open standards or API specifications. There is a risk that any standards developed will become quickly obsolete as the cloud service market and technical approaches (such as APIs) continue to mature at a pace. We encourage the European Commission to continue fostering alignment with existing regional and global cloud service-related standards. This is because alignment will reduce fragmentation and duplication, which limits the effectiveness of standards and their adoption in the industry.

Finally, we recommend further engagement with the financial services industry and CSPs to identity the standards and technical elements which could be of value to the industry for portability, through inclusion in non-legislative approaches such as existing CoCs or future SCCs initiatives.

5.7a. Do you consider that formally requesting European standardisation development organisations to design such standards or the necessary APIs would be an appropriate solution?

- Yes
- No
- **I don't know / no opinion**

5.7b. Please specify how such standards should be identified / developed. 200 characters max

Short form answer:

We encourage the Commission to continue fostering alignment with existing regional and global cloud service-related standards to reduce fragmentation and duplication.

We encourage the European Commission to continue fostering alignment with existing regional and global cloud service-related standards. This is because aligning with existing standards will reduce fragmentation and duplication, limiting the effectiveness of standards and their adoption in the industry.

5.8. Would it be necessary in your opinion to develop Standard Contractual Clauses for cloud service portability to improve negotiating position of the cloud users?

- Yes, it would be necessary and sufficient as a standalone solution
- Yes, it would be necessary but in addition to a legislative right of data portability
- **It would not be necessary but it would simplify the data portability and/or harmonise its aspects across the EU**
- No, it would not be necessary
- No opinion

5.9. Do you have any other comments you would like to address with respect to cloud service portability, which were not addressed above? 300 characters max

Short form answer:

Cloud services portability is often overly simplified as a technical and commercial concept (e.g. “switching”). This challenges the formulation of effective policy options to address cloud services competition or operational risk and risks limiting the different service offerings available.

AFME members believe that SCCs for cloud services could provide value where they are applied consistently throughout the EU and reduce regulatory fragmentation across the Member States. However, whilst SCCs should provide a useful

tool to comply with existing regulatory obligations, such as the 2019 EBA Guidelines on Outsourcing,[3] they should not become an additional compliance obligation for financial institutions. SCCs, which become an additional compliance layer, would likely contribute to additional cost and complexity for financial institutions and could inadvertently limit or restrict cloud use (and innovation). Further, SCCs and the intent of the European Commission initiative was broader than data portability. For example, SCCs were considered for areas such as access and audit rights.

We believe that any further work or the introduction of SCCs should continue to consider the wide range of potential requirements on financial institutions in adopting cloud services. Finally, we continue to strongly advise that further consultation is taken with the industry on any draft SCCs before introducing them to the cloud services market. This further consultation will ensure that the SCCs will provide practical and beneficial outcomes for firms and do not introduce further barriers to cloud adoption in the EU.

AFME members wish to raise an overall concern that cloud services portability is often overly simplified as a technical and commercial concept (e.g., "switching"). We believe this simplification presents a challenge for formulating effective policy options to address cloud services competition or operational risk (such as addressing potential asymmetry of power between cloud service providers and customers).

For example, a policy that would place more significant restrictions on cloud service portability could limit the differentiating service offerings available to financial institutions. This is because comparable cloud services that offer greater portability tend to be more foundational (i.e. compute and storage). Further, mandating high levels of portability could significantly increase the investment required by financial institutions (i.e. technical skills and infrastructure) to architecture solutions; restricting financial institutions from taking a risk-based approach (i.e. assessing where there is a greater need for portability, rather than having requirements mandated across all cloud service use). Finally, as with existing IT applications and infrastructure, there are often limitations in cloud services that could allow a financial institution to achieve high levels of portability (particularly for SaaS offerings, which can also provide the greatest competitive or unique benefits for financial institutions and customers).

Financial institutions strongly recognise the need to promote resilience within cloud services and acknowledge the potential benefits of portability in certain situations. This is recognised by most financial institutions adopting multi-cloud strategies and assessing which workloads are suitable for moving to the cloud (based on many factors, such as portability). However, portability is highly complex and should not be seen as a default solution in future policy measures. An overly simplified approach, or blanket set of requirements, will introduce a significant barrier to cloud services adoption in the EU and could limit digital transformation encouraged by the EU digital finance strategy.

We welcome further discussion on cloud services portability and supporting the European Commission on introducing any future requirements which can achieve greater competition, resilience, and innovation in financial markets.

[3] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

Section 6. Complementing the portability right under Article 20 GDPR

6.1. To what extent do you agree with the following statement: "Individual owners of a smart connected object (e.g. wearable or household appliance) should be able to permit whomever they choose to easily use the data generated by their use of that object."

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly disagree
- **I don't know / no opinion**

6.2 To what extent do you agree with the following statement: "The device manufacturer of a smart connected object (e.g. wearable or household appliance) should be able to permit whomever they choose to easily use the data generated by the use of that object, without the agreement of the user."

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly disagree
- **I don't know / no opinion**

6.3a. Among the elements listed below, which are the three most important elements that prevent the right under Article 20 GDPR to be fully effective? (select maximum of 3 only)

- **The absence of an obligation to provide a well-documented Application Programming Interface**
- The absence of an obligation to provide the data on a continuous basis
- The absence of universally used methods of identification or authentication of the individual that makes the portability request in a secure manner
- The absence of clearer rules on data types in scope
- The absence of clear rules on liability in case of misuse of the data ported
- The absence of standards ensuring data interoperability, including at the semantic level
- **Other**
- I don't know / no opinion

6.3b. Please specify. 200 characters max

Short form answer:

These measures highlighted above could provide users and organisations with greater control and sharing of data, as well as create opportunities to improve products and services for end-users.

In our response to the European Data Strategy[4], AFME members emphasised the importance of portability to ensure that data can be shared in a simple, ongoing, real-time, standardised, and secure way. We are supportive of the elements highlighted in Q6.3a as areas where the GDPR Article 20 Right to Data Portability could be made more effective. These measures could provide users and organisations with greater control and sharing of data, allowing for increased data use

[4] afme.eu/Portals/0/DispatchFeaturedImages/2020%2005%2029%20AFME%20EC%20European%20Strategy%20for%20Data%20response%20(FINAL)_CLEAN.pdf

and re-use in the financial sector, and creating opportunities to improve products and services for end-users (e.g., improving the accuracy of systems on fraud, security, AML).

Section 7. Intellectual Property Rights – Protection of Databases

Intellectual Property Rights - General questions

7.1a. In your view, how are intellectual property (IP) rights (including the sui generis database right) and trade secrets relevant for business-to-business sharing of data?

- **To protect valuable data through IP, where possible**
- **To share data in a manner that ensures control on who will use it and for what purposes**
- **To protect data from misappropriation and misuse**
- To refuse sharing of data
- IP has nothing to do with data sharing
- I don't know / no opinion
- Other

7.2b. Please specify or explain. 200 characters max

Short form answer:

IP is important for the protection of data and permissions in managing third-party relationships and enforcing a firm's rights to databases where there is creativity and/or substantial investment.

In a business-to-business context, IP is important for the protection of data and permissions for use in managing third-party relationships and enforcing of a firm's rights to databases where there is creativity and/or substantial investment, recognising the organisation and arrangement of the database. Like other IP rights, the sui generis right aims to ensure a balance between the rights granted to database makers and those of users.

7.3a. "Control over the accessibility and use of data should not be realised through the establishment of additional layers of exclusive, proprietary rights". To what extent do you agree with this statement?

- Strongly agree
- Somewhat agree
- **Neutral**
- Somewhat disagree
- Strongly disagree
- I don't know / no opinion

7.3b. Please explain. 200 characters max

Short form answer:

We require further information regarding what would constitute a "layer" as described. There may be instances where this could provide further protections or reduce the reluctance to share data.

There may be instances where additional layers of exclusive, proprietary rights, could provide further protections in addition to contractual measures, or reduce the reluctance to share data (depending on the type of data in question). However, to answer this question we require further information regarding what would constitute a "layer" as described.

More generally in the context of increasing digitisation, there has been an increase in the volume of technology-related IP, which may require further consideration of IP rights to ensure the existing framework continues to protect and foster innovation. This includes:

- All technology-related IP including registered IP (e.g. patents), unregistered IP (e.g. copyright, source code), confidential information, know-how and trade secrets protecting technology-related intellectual assets and

capital (e.g. software, information systems, algorithms, R&D efforts, innovative concepts, client data, employee expertise), and
- Non-tech IP (e.g. business models, processes, banking know-how) where the intellectual property and expertise sits.

Questions on the Database Directive

7.4. Please select what describes you best:

- Maker of databases containing machine generated data
- Maker of databases containing other type of data than machine generated data
- Maker of databases containing mixed type of data
- User of databases containing machine generated data
- User of databases containing other type of data than machine generated data
- User of databases containing mixed type of data
- User-maker of databases containing machine generated data
- User-maker of databases containing other type of data than machine generated data
- **User-maker of databases containing mixed type of data**
- Other

7.5a. In your view, how does the Database Directive apply to machine generated data (in particular data generated by sensor-equipped objects connected to the Internet-of-things objects)?

- I consider that the sui generis right under the Database Directive may apply to databases containing those data and offers opportunity to regulate the relationship with clients, including licences
- I consider that the sui generis right under the Database Directive may apply to databases containing those data and offers protection against third-party infringements (i.e. unauthorised use of machine generated data)
- I am not sure what the relationship is between such data and the Database Directive
- **Other**

7.5b. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. 200 characters max

Short form answer:

Clarity regarding database rights for machine generated and/or processed data could be useful as machine learning capabilities may significantly reduce the cost of creating/maintaining the database.

Clarity regarding database rights for machine generated and/or processed data could be useful in the context of ongoing technological development. For instance, we note that there is an increasing focus on considering how machine learning may affect the definition of a database. Machine learning capabilities may significantly reduce the cost of creating and maintaining the database.

We note that while the relationship between clients and vendors may be established through contractual terms and conditions, the sui generis right under the Database Directive could be an option to offer protection against third-party infringements as it offers protection against copies of data and thus applies further to the contractual terms established by the database producer.

We support the planned review of the Database Directive as an opportunity to explore these areas in more detail.

7.6a. According to your experience, which of these statements are relevant to your activity / protection of your data? (select all that apply)

- **The protection awarded by the sui generis right of the EU Database Directive is used to regulate contractual relationships with clients**
- The protection awarded by the sui generis right of the EU Database Directive is used against third-party infringements
- **The protection awarded by the Trade Secret Rights Directive [Directive (EU) 2016/943] is used against third-party infringements**
- **Other contractual means of protection are used**
- **Technical means to prevent illicit extraction of content are used**
- There is certain content that is deliberately not protected
- I don't know / no opinion
- Other

7.6b. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. 200 characters max

AFME has not responded to this question.

7.7. Have the sui generis database right provided by the Database Directive (Directive 96/9/EC) or possible uncertainties with its application created difficulties and prevented you from seeking to access or use data?

- Yes
- No
- **I don't know / no opinion**

7.8a. The difficulties you are aware of or have experienced because of the sui generis database right relate to the access or use of:

- Data generated in the context of Internet-of-things/machine generated data
- Data other than generated in the context of Internet-of-things/machine generated data
- Data, irrespective of their type (machine generated or data other than machine generated)
- No difficulties experienced
- **I don't know / no opinion**
- Other

7.9a. What was the source of such difficulties?

- No difficulties experienced
- Difficulty to find the right holder of the sui generis database right (database maker
- Lack of reaction from the part of the right holder of the sui generis database right / Refusal of cooperation from the part of the right holder of the sui generis database right
- Prohibitive licence fees
- Technical measures / technical difficulties
- Denied access despite the proposed use falling under one of the exceptions defined in the Database Directive
- Denied access despite the proposed use falling under the rights of the lawful user
- Lack of clarity regarding application of the sui generis right to the database (incl. possible legal consequences and risk of litigation)
- Other
- **I don't know / no opinion**

7.10a. To what extent do you agree that there is a need to review the sui generis protection for databases provided by the Database Directive, in particular as regards the access and sharing of data.

- Strongly agree
- **Somewhat agree**
- Neutral
- Somewhat disagree
- Strongly disagree
- I don't know / no opinion

7.10b. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. 200 characters max

Short form answer:

Clarity regarding database rights for machine generated and/or processed data could be useful as machine learning capabilities may significantly reduce the cost of creating/maintaining the database.

Clarity regarding database rights for machine generated and/or processed data could be useful in the context of ongoing technological development. For instance, we note that there is an increasing focus on considering how machine learning may affect the definition of a database. Machine learning capabilities may significantly reduce the cost of creating and maintaining the database. We would welcome clarity on how this may affect the scope of this Directive.

7.11a. Do you think that it is necessary to clarify the scope of sui generis right provided by the Database Directive in particular in relation to the status of machine generated data?

- **Yes**
- No
- I don't know / no opinion

7.11b. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. 200 characters max

Short form answer:

Further clarity regarding what constitutes substantial investment in the creation of the data as well as defining the creator of a database would be helpful.

Yes, further clarity regarding database rights for machine generated and/or processed data could be useful with respect to what constitutes substantial investment in the creation of the data as well as defining the creator of a database. For instance, we note that there is an increasing focus on considering how machine learning may affect the definition of a database. Machine learning capabilities may significantly reduce the cost of creating and maintaining the database. We would welcome clarity on how this may affect the scope of this Directive.

7.12a. In your opinion, how should the new scope of the sui generis right be defined?

- By narrowing the definition of the scope to exclude machine generated data
- By explicitly including machine generated data in the scope
- I don't know / no opinion
- No need for a change of the scope
- **Other**

7.12b. Please explain and substantiate your answer with concrete examples and any useful information and experience you may have. If possible, indicate also the impact on cost and potential benefits of your selected option. 200 characters max

Short form answer:

Clarity regarding database rights for machine generated and/or processed data could be useful as machine learning capabilities may significantly reduce the cost of creating/maintaining the database.

Clarity regarding database rights for machine generated and/or processed data could be useful in the context of ongoing technological development. For instance, we note that there is an increasing focus on considering how machine learning may affect the definition of a database. Machine learning capabilities may significantly reduce the cost of creating and maintaining the database. We would welcome clarity on how this may affect the scope of this Directive.

7.13. Do you think that the Database Directive should provide specific access rules to ensure access to data and prohibit companies from preventing access and extraction through contractual and technical measures?

- Strongly agree
- Somewhat agree
- Neutral
- **Somewhat disagree**
- Strongly disagree
- I don't know / no opinion

7.14a. In your opinion, how would specific access rules in the Database Directive be best achieved?

- Creating a new exception
- Creating compulsory licences to access data
- Creating general access right
- **No need for a specific access rules**
- Other
- I don't know / no opinion

7.14b. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. If possible, indicate also the impact on cost and potential benefits of your selected option. 200 characters max

Short form answer:

The sui generis right is one mechanism, although there are other drivers that may help encourage investments in database production (e.g. copyright, technical measures, contracts, competition law).

The sui generis right is one possible mechanism to protect investments in databases, although there are other drivers which may help encourage such investments in the production of databases (e.g. copyright, technical measures, contracts, competition law).

7.15. Do you agree that databases held by public authorities should be treated differently than other type of databases under the Database Directive?

- Strongly agree
- **Somewhat agree**
- Neutral
- Somewhat disagree
- Strongly disagree
- I don't know / no opinion

7.16a. In your opinion, how should databases held by public authorities be treated differently?

- **Creating an exception to the sui generis right**
- Excluding public sector databases from the scope of the sui generis right of the Database Directive
- Creating compulsory licences to access public sector databases

- No need for different treatment
- Other
- I don't know / no opinion

7.16b. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. 200 characters max

Short form answer:

Exceptions could relate to emergency/disaster relief or other high-value public sector datasets. This approach will ensure legal certainty to public-private initiatives which should remain in scope.

Databases held by public authorities could be subject to exceptions, for example, relating to emergency or disaster relief. Access to the databases could then be granted once the results of the data are made publicly available.

We note that some public databases are already freely accessible, however it is our view that further conditions to data access may be required when requesting the data in a structured or processed template.

7.17a. In 2018, the Commission published an Evaluation of Directive 96/9/EC on the legal protection of databases, which was preceded by a public consultation. The Evaluation Report pointed out several legal uncertainties related to the Database Directive that may prevent the Directive from operating efficiently. Please indicate which of the following elements of the Database Directive could be reviewed (select all that apply):

- Definition of a database
- **Notion of substantial investment in a database**
- **Notion of substantial part of a database**
- **Exclusive rights of database makers**
- **Exceptions to the sui generis right**
- **Notion of the lawful user and his rights and obligations**
- **Term of protection**
- No elements need to be reviewed
- I don't know/ no opinion
- **Other**

7.17b. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. If possible, indicate also the impact on cost and potential benefits of your selected option. 200 characters max

Short form answer:

Providing further detail and thresholds on these definitions would help harmonise national law and interpretation, providing legal certainty at EU level. The term 'ownership' should also be reviewed.

Providing specific thresholds and clarity with respect to these definitions would help harmonise national law and interpretation and therefore encourage investment; as well as provide more legal certainty in database production at the EU level. In addition, it would be beneficial to provide further clarity on the term 'ownership' of the database.

7.18. Please provide any other information that you find useful regarding the application of the Database Directive in relation to the data economy. 200 characters max

Short form answer:

We welcome clarity on how database rights in third countries will be impacted by the Database Directive review, and on cases where 'promoting economic welfare' would be an exception to infringement.

We welcome clarity in how database rights created in third countries will be impacted by any changes to the Database Directive.

Regarding the proposal to promote economic welfare as a policy priority, we welcome further clarity on the circumstances where this would be considered as an exception to infringement.

Questions about trade secrets protection

7.19. Do you rely on the legal protection of trade secrets when sharing data with other businesses?

- **Yes**
- No
- I don't know / no opinion

7.20a. With whom do you share? (select all that apply)

- **Partner**
- **Supplier**
- **Customer**
- Unrelated business
- Other

7.21a. How do you ensure that the shared information remains secret?

- **By contractual arrangements, e.g. a non-disclosure agreement**
- By using a trustee (a law firm or another trusted intermediary)
- **By means of a special cyber security solution that also ensures confidentiality, such as encryption**
- Other
- No specific measures are taken

7.22a. Please indicate why: (select all that apply)

- We are not certain whether the legal protection for trade secrets applies
- We do not share commercially sensitive data with other businesses
- We do not share any data with other businesses
- I don't know / no opinion
- **Other**

7.22b. Please specify. 200 characters max

Short form answer:

Reasonable steps, such as those listed in 7.21a must be taken to ensure information is protected as a trade secret.

Reasonable steps, such as those listed in 7.21a must be taken to ensure information is protected as a trade secret.

7.23a. If you share confidential business information, how do you ensure control over the use of your data by other businesses, i.e. that it is not misused, misappropriated or disclosed unlawfully?

- **We rely on the legal protection of trade secrets**
- **We rely on intellectual property rights**
- **We rely on contractual arrangements**

- **We rely on technical means**
- We do not take any specific measures to control the use of our data
- I don't know / no opinion
- Other

7.23b. Please specify which rights. 200 characters max

AFME has not responded to this question.

Section 8. Safeguards for non-personal data in international contexts

8.1. How likely do you think it is that a cloud computing service or other data processing service provider that is processing data on your company's/organisation's behalf may be subject to an order or request based on foreign legislation for the mandatory transfers of your company/organisation data?

- This is a big risk for our company
- This is a risk for our company
- This is a minor risk for our company
- This not a risk at all for our company
- We do not use cloud computing/data processing service provider to store or process our company
- **I don't know / no opinion**

8.2. Please explain what order or request for the mandatory transfers of you company/ organization data would you consider as illegitimate or abusive and as such presenting the risk for your company. 200 characters max

Short form answer:

It is challenging to answer this question on a general rather than case-by-case basis. We also welcome further detail on the definition and scope of 'other data processing service provider'.

It is challenging to answer this question on a general rather than case by case basis. We also welcome further detail on the definition and scope of 'other data processing service provider'.

8.3. Do you consider that such an order or request may lead to the disclosure and/ or misappropriation of a trade secret or other confidential business information?

- This is a big risk for our company
- This is a risk for our company
- This is a minor risk for our company
- This not a risk at all for our company
- **I don't know / no opinion**

8.4a. Does the risk assessment related to such possible transfers of your company /organisation data to foreign authorities affect your decision on selection of the data processing service providers (e.g. cloud computing service providers) that store or process your company/organisation data?

- **Yes**
- No
- I do not use data processing services to store or process my data
- I don't know / no opinion

8.4b. Please explain how it affects your decision. 200 characters max

Short form answer:

Banks' risk assessments account for factors such as the data request rationale, type of data, transfer destination and the jurisdiction-specific protections required where the data will reside.

The likelihood of a data processing service being subject to a request for the transfer of data on behalf of an organisation will be dependent on each case. Banks' risk assessments today account for factors such as the rationale for the data request, the type of data, where the data is intended to be transferred, and the protections required for the transfer of data within existing law for the jurisdictions where the data will reside.

8.5. In light of risk assessment of your data processing operations as well as in the context of applicable EU and national legal frameworks (e.g. national requirements to keep certain data in the EU/EEA), do you consider that your company /organisation data should be stored and otherwise processed:

- All of my company/organization data in the EU/EEA only
- Some of my company/organization data in the EU/EEA only
- All of my company/organization data anywhere in the world
- I don't know / no opinion

AFME has not responded to this question.

8.6. Please explain what categories of data that should be stored in the EU/EEA only are concerned and why. 200 characters max

Short form answer:

Firms should be able to assess the risks associated with data storage and decide where to store their data, as the sensitivity and associated risks of different types of data are context dependent.

We believe that firms should have the flexibility to assess the risks associated with data storage and decide where to store their data. As noted in other responses to this survey, the sensitivity and associated risks of different types of data are highly context dependent. These risks should be evaluated by companies on a case-by-case basis, accounting for various relevant risk factors.

8.7a. In your opinion, what would be the best solution at an EU regulatory level to mitigate the risk for European companies stemming from the request for access by foreign jurisdiction authorities to their data?

- **Introducing an obligation for data processing service providers (e.g. cloud service providers) to notify the business user every time they receive a request for access to their data from foreign jurisdiction authorities, to the extent possible under the foreign law in question**
- Introducing an obligation for data processing service providers to notify to the Commission, for publication on a dedicated EU Transparency Portal, all extraterritorial foreign laws to which they are subject and which enable access to the data they store or process on behalf of their business users
- Introducing an obligation for data processing service providers to put in place specified legal, technical and organisational measures to prevent the transfer to or access of foreign authorities to the data they store or process on behalf of their business users, where such transfer or access would be in conflict with EU or national laws or applicable international agreements on exchange of data
- Providing for compatible rules at international level for such requests
- **Other solution**
  There is no action needed to address this
- I do not know / no opinion

8.7b. Please specify. 200 characters max

Short form answer:

Leverage existing EU frameworks, e.g. the 2019 EBA Guidelines on Outsourcing, which include measures to account for potential data transfer risks. Avoid creating inadvertent data localisation rules.

We note that the EU regulatory framework has been developed to mitigate potential data transfer risks to public bodies outside of the EU. For example, the 2019 EBA Guidelines on Outsourcing require that an organisation's risk assessment for outsourcing considers the political and security environment of the jurisdictions in question. This includes laws in force that relate to data protection. Further, many data processing service providers (such as cloud service providers)

have legal counsel available to review requests against applicable law, mechanisms to notify customers of data requests, and transparency registers.

We encourage further consideration and industry engagement regarding any measures which could potentially lead to future data localisation requirements. The free flow of information across borders is important for financial institutions in ensuring regulatory compliance, cybersecurity, effective risk management, developing new products and improving client services.

AFME contacts

Andrew Harvey, aharvey@eu.gfma.org	+44 (0)20 3828 2694
Ian Waterworth, ian.waterworth@afme.eu	+44 (0)20 3828 2685
Madeline Taylor, madeline.taylor@afme.eu	+44 (0)20 3828 2688

About AFME

The Association for Financial Markets in Europe (AFME) represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. AFME advocates for stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.