Consultation response

European Commission Public Consultation – A European Strategy for Data

29 May 2020

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the Public Consultation (referred to hereafter as the "CP") on a EUROPEAN STRATEGY FOR DATA. 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 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.

We have developed Annex I to support and provide further detail to our response to the consultation survey below. Each section title in the Annex identifies the questions in the survey that are addressed.

Section 1: General questions on the data strategy

Q1 Do you agree that the European Union needs an overarching data strategy to enable the digital transformation of the society?

- Yes
- No

Q2 ***"More data should be available for the common good, for example for improving mobility, delivering personalised medicine, reducing energy consumption and making our society greener."*** **To what extent do you agree with this statement?**

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q3 Do you think that it should be made easier for individuals to give access to existing data held about them, e.g. by online platform providers, car manufacturers, producers of wearables, voice assistants or smart home appliances, to new services providers of their choosing, in line with the GDPR?

- Yes
- No

Q4 What mechanisms(s) do you think would help to achieve this?

- A compelling offer to use the data that brings benefits to the individuals
- Practical solutions that allow individuals to exercise control, such as mobile and online dashboards or apps
- Additional rights in law
- Other

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)69 153 258 967
www.afme.eu

- Don't know/no opinion

Additional rights in law (200 characters):
A legal framework should create the right conditions for the secure transmission of cross-sectoral data.

Other (200 characters):
Enhancing portability for key datasets of particular value to individuals, including data from digital platforms and other key sectors. Sharing should be possible only through APIs, where available.

Q5 Have you faced difficulties in recruiting data professionals (workers who collect, store, manage, analyse, interpret and visualise data as their primary or as a relevant part of their activity) during the last 2 years?

- Yes
- No

Q6 'General data literacy across the EU population is currently insufficient for everyone to benefit from data-driven innovation and to become more active agents in the data economy.' To what extent do you agree with this statement?

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q7 Have you had difficulties in using data from other companies?

- Yes
- No

Q8 What was the nature of such difficulties?

- Impossibility to find companies to supply data of relevant quality
- Denied data access
- Prohibitive process or other conditions considered unfair or prohibitive
- Technical aspects relating to both data interoperability and transfer mechanisms
- Other (if yes, please specify)
- Don't know/no opinion

Q9 *'It is currently challenging to define solutions on the allocation of the rights to use data coming from smart machines or devices that are fair for all parties concerned'*. To what extent do you agree with this statement?

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q10 ***'The EU should make major investments in technologies and infrastructures that enhance data access and use, while giving individuals as well as public and private organisations full control over the data they generate.'*** **To what extent do you agree with this statement?**

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q11 ***'The development of common European data spaces should be supported by the EU in strategic industry sectors and domains of public interest (industry /manufacturing, Green Deal, mobility, health, finance, energy, agriculture, public administration, skills).'*** **To what extent do you agree with this statement?**

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q11.1 Are there general comments you would like to make about the data strategy?

[300 characters limit on general comments]:

Common data spaces could be an opportunity to solve coordination problems and specific use cases in different sectors to address common challenges. This should include the key sectors identified within the Data Strategy, as well as digital platforms. Please see Annex I for more detail.

Section 2.1 - Specific questions on future actions: Data governance

Q12 'Data governance mechanisms are needed to capture the enormous potential of data in particular for cross-sector data use.' To what extent do you agree with this statement?

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q13 ***'The re-use of data in the economy and society would benefit greatly from standardisation to improve interoperability.'*** **To what extent do you agree with this statement?**

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree

- Don't know/no opinion

Q14 ***'Future standardisation activities need to better address the use of data across sectors of the economy or domains of society.'*** **To what extent do you agree with this statement?**

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q15 Which of the following elements do you consider to be the most useful in terms of standardisation?

- Metadata schema
- Metadata variables (semantic interoperability at the metadata level), including ontologies, controlled vocabularies and agreed thesauri
- Data formats
- Common data models
- Data exchange protocols
- Application Programming Interfaces (APIs)
- Licences or licence terms
- Other
- Don't know/no opinion

[Text box for if other, please specify]: User experience – see Annex I for more detail.

Q16 What role should EU or national government bodies take in standardisation?

- Provide necessary funding in order to ensure open standards
- Take an active role in the prioritisation and coordination of standardisation needs, creation and updates
- Be directly involved in defining standards
- Provide funding to test draft standards in practise and develop tools to implement them early on
- Other
- Governments should not have a role in standardisation
- Don't know/no opinion

[Text box for if other, please specify]:
International or European standardisation organisations should be clearly endorsed by EU government bodies to avoid market fragmentation but should be managed by professional organisations.

Q17 'Public authorities should do more to make available a broader range of sensitive data for R&I purposes for the public interest, in full respect of data protection rights.' To what extent do you agree with this statement?

- Strongly agree
- Somewhat agree
- Neutral

- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

[Text box for if other, please specify]

Q18 Which of the following should public authorities do to facilitate data re-use:

- Help the re-user to identify the exact authority that is holder of a specific set of data (one-stop-shop)
- Ensure that the request for data access is processed faster, within agreed deadlines
- Assess whether the re-use of the data could potentially harm the interests of others (of the persons/companies whose data is being used) for concrete use-cases
- Be able to provide anonymisation of specific data for concrete use-cases
- Offer the possibility to process data within a secure environment it makes available, so that the user does not need to obtain a copy of the data
- Clarify from the outset the legal rules on the purposes for which the data can be used
- Provide for recourse mechanisms to challenge decisions on one or several of the above.
- Other
- I don't know / no opinion

[Text box for if other, please specify]

Q19 Do you think that law and technology should enable citizens to make available their data for the public interest, without any direct reward?

- Yes
- No
- Don't know/no opinion

Q20 For which of the following purposes would you be willing to make data available:

- For health-related research
- For aspects relating to the city/municipality/region I live in, including for example improving mobility, to improve environmental challenges that can be addressed through action at local or regional level
- For other public interest purposes
- None of the above
- I don't know / no opinion

Q21 Do you think there are sufficient tools and mechanisms to "donate" your data?

- Yes
- No
- Don't know/no opinion

Q22 In which of the following domains do you see potential for the use of 'contributed' data:

- For health-related research
- For aspects relating to the city/municipality/region I live in, including for example improving mobility, to improve environmental challenges that can be addressed through action at local or regional level

- For other public interest purposes
- None of the above
- I don't know / no opinion

Q23 What would support the usefulness of 'data altruism' mechanisms as a means to build up data pools for research and innovation:

- A standard form for obtaining consent (and, where necessary, requesting data portability) from the individual in line with the GDPR
- A European approach to obtaining consent that is compliant with the GDPR
- Public registers of persons that are willing to make available some of their data for research or innovation purposes
- The existence of intermediary infrastructures such as personal data spaces
- The existence of intermediary infrastructures such as personal data spaces /wallets/stores controlled by each individual from which the data could be retrieved
- Additional EU legislation on data altruism relating to deceased persons
- Information campaigns sensitising individuals on the subject matter, e.g. via clinical practitioners
- Measures to mitigate inherent bias in the data collected through this means
- Other

Q24 ***'Such intermediaries are useful enablers of the data economy.'*** **To what extent do you agree with this statement?**

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Section 2.2 - Specific questions on future actions: identification of high-value datasets

Q25 ***'The establishment of a list of high-value datasets, to be made available free of charge, without restrictions and via APIs, is a good way to ensure that public sector data has a positive impact on the EU's economy and society.'*** **To what extent do you agree with this statement?**

- Strongly agree
- Somewhat agree
- Neutral
- Somewhat disagree
- Strongly Disagree
- Don't know/no opinion

Q26 Apart from the potential to generate socio-economic benefits, please indicate the relevance of the following additional factors to be taken into account when selecting datasets for the future list of high value datasets (very relevant, relevant, neutral, not relevant, not relevant at all, don't know/no opinion):

- The re-use of the dataset would increase if it was provided free of charge. (relevant)
- The dataset belongs to a thematic area in which there are few EU-level requirements for opening up data (relevant)

- The reuse of the dataset would increase if its availability under uniform conditions was ensured across the entire EU (relevant)
- The re-use of the dataset would increase if it was available via an application programming interface (API) (very relevant)

[If other factors, please specify]

Q27 Under the Open Data Directive, specific high-value datasets will have to be available free of charge, in a machine-readable format, provided via APIs and, where relevant, provided as a bulk download. Please indicate the relevance of each of the other arrangements indicated below to improve the re-usability of specific high-value datasets (very relevant, relevant, neutral, not relevant, not relevant at all, don't know/no opinion):

- Licensing and other terms of applicable to re-use (very relevant)
- Standardised formats of data and metadata (very relevant)
- Possibility of user feedback (relevant)
- Specific technical arrangements for dissemination (very relevant)

[If other arrangements, please specify] *[Please specify which specific technical arrangements for dissemination]:* Please see Annex I for more detail.

Q28 EU programmes may provide funding to enhance the availability and re-use of high-value datasets across Europe. For each of the following activities, please indicate how relevant it is to support them.

- Improving the quality (e.g. machine readability) and interoperability of the data/metadata. (very relevant)
- Ensuring sustainable data provision via application programming interfaces (APIs) (very relevant)
- Engaging with re-users (promoting the data, co-defining use cases) (relevant)

[If other activities, please specify]

Q29 According to your experience and the expected potential of concrete datasets, indicate up to three specific datasets that should be listed in each of the thematic categories of high-value datasets, as referred to in Article 13(1) of the Open Data Directive:

	Specific datasets
Geospatial	- Business locations - Detailed cadastre for business and household premises
Earth observation and environment	- Natural disaster risk maps, crop yields data, annual rainfall, and other datasets that measure exposure to climate change risk - Energy data: official certification of building efficiency, and other datasets from a product perspective
Meteorological	

Statistics	- Economic indicators (such as income) at high levels of granularity and availability on at least a monthly basis, with disaggregation by geography or local administrative region and by demographic characteristics
Companies and company ownership	- Company registration information and public accounts - Court information regarding companies, e.g. public case brought by state against a firm
Mobility	- Anonymised disaggregated passenger travel information on all public transport (i.e. travel journey for each transport customer, without other personally identifying factors)

Section 2.3 - Specific questions on future actions: the (self-/co-) regulatory context of cloud computing

Q30 Does your organisation use and/or provide cloud or edge services?

- Yes, my organisation uses cloud or edge services
- Yes, my organisation provides cloud or edge services
- None of the two

Q31 Does your organisation use:

- Cloud
- Edge
- Both cloud and edge

[If no, please explain why you do not use cloud, edge or neither of the two, 200 characters max]: Edge technologies are not yet widely used by the industry, but uptake within the next five years is possible as the technology continues to develop.

Q32 Do you believe the cloud market currently offers the technological solutions that you need to grow and innovate your business?

- Yes
- No

Q33 Do you feel that your organisation's sensitive data is adequately protected and secured by the cloud services you use?

- Yes
- No

[*Please specify the problems, 200 characters max]*

Q34 Have you experienced problems in the context of the current functioning and constitution of the market for cloud services in Europe?

- Yes
- No

Q35 Do these problems relate to:

- Cost of cloud services
- A limited possibility to switch providers, please specify
- Asymmetry of power negotiation between customer and provider, please specify
- Contractual practise on the market, including unilateral change of terms and conditions, please specify
- Security risks, including leakage of data or intellectual property
- Other

[Please specify, 200 characters max]: Other: Termination periods and switching, data localisation requirements, please see Annex I for more detail.

Q36 Do you perceive risks emerging from the current functioning and constitution of the market for cloud services in Europe?

- Yes
- No

Q37 Do these risks relate to:

- Cost of cloud services
- A limited possibility to switch providers, please specify
- Asymmetry of power negotiation between customer and provider, please specify
- Contractual practise on the market, including unilateral change of terms and conditions, please specify
- Security risks, including leakage of data or intellectual property
- Other

[Please specify, 200 characters max]: Concentration risk – please see Annex I for more detail.

Q38 Does your organisation have flexibility to procure/adopt new and innovative cloud solutions if they emerge on the market?

- Yes
- No

Q39 If no, is this related to:

- Technical barriers
- Legal/contractual barriers
- Economic/cost barriers
- Security barriers
- Other barriers

[If legal/contractual please specify, 200 characters max]:
[If other please specify, 200 characters max]:

Q40 Is your organisation aware of self-regulatory schemes for cloud/edge services (for example, codes of conduct or certification schemes)?

- Yes
- No

Q41 Please indicate in which of the following areas you are aware of self-regulatory approaches:

- Data protection
- Data portability
- Security
- Energy efficiency
- Other

[If other, please specify, 200c]:
[Please name the specific schemes you are familiar with]:

- EC Data Portability, cloud switching/ porting data (SWIPO) Workgroup – Codes of Conduct
- Scope data protection Codes of Conduct
- CSPCert for cloud services provider security certification - *Recommendations for the implementation of the CSP Certification scheme*
- *Cloud Industry Forum – Code of Practice (https://www.cloudindustryforum.org/content/cif-code-practice)*
- *ISO 14001 compliance for energy efficiency*

[How do you believe market awareness of these schemes could be raised?]:
Authorities should support the development of these schemes (as they are already doing) and promote their adoption to help reduce compliance burdens associated with adopting certified cloud services.

Q 42 Do you believe a self-regulatory approach is appropriate to identify best practices to apply EU legislation or self-regulation?

- Yes
- No

Q43 If yes, do you believe a self-regulatory approach is appropriate to identify best practises to apply EU legislation or self-regulation relating to (Yes/No/Don't know/no opinion]:

- Data protection - No
- Data portability - Yes
- Security – Yes
- Energy-efficiency – Yes
- Other

[If other, please specify, 200 characters max]
[Please explain why, 200 characters max]: We believe the examples listed in Q41 provide examples of appropriate self-regulatory approaches.

Q44 Would it be beneficial for your organisation if applicable rules for cloud and edge would be bundled and corresponding information made available by the European Commission?

- Yes
- No
- Don't know/no opinion

Supporting Paper (Annex I)

General Comments

This paper (Annex I) has been developed to support the AFME response to the European Commission (Commission) public consultation, '*A European Strategy for data*'.

AFME welcomes the Commission's efforts to enable a European data economy that is built on a robust legal framework, competitive European infrastructures, and promotes policy measures that address issues related to connectivity, processing and storage, computing power and cybersecurity.

A European Strategy for Data will be important for ensuring the EU economy can remain competitive and for promoting the individual's rights to data sharing. AFME agrees with the Commission that more data should be available to support the Commission's sustainability objectives and for the common good.

Both regulatory and non-regulatory data initiatives could support European financial institutions (FIs) to remain competitive, take advantage of new technologies and services and further transform their business models. This importance of data, technology and innovation for Europe has been further highlighted during the COVID-19 response.

However, we believe that any requirements for increased data sharing which are only implemented for certain sectors could put FIs' digital competitiveness at risk.

We have therefore put forward the following high-level considerations in support of the European Data Strategy:

- **Apply a cross-sector approach to data sharing**. Data sharing must be driven across multiple sectors, particularly as new entrants emerge, and any mandatory requirements should be applied equally to market participants to maintain a level playing field. Increased standardisation of data types, and formats, across sectors will be important to facilitate this effective data sharing. European supervisory authorities and standards setting bodies, as well as global organisations, will have an important coordinating role to play in achieving these objectives.
- **Facilitate access to both personal and non-personal data**. EU policymakers should promote a data sharing policy that improves services to both consumers and businesses. Mechanisms should be put in place to facilitate greater access to non-financial data on an ongoing, real time, standardised and secure basis.
- **Promote data sharing within, and between, Common European Data Spaces.** Common European Data Spaces (CEDS) can facilitate the sharing of raw and observed data for the benefit of multiple parties, both private and public. We believe that CEDS should recognise that data generated in one sector may be relevant in another, and therefore should facilitate the flow of data both within, and between, sectors. We also request the Commission to continue to address data localisation restrictions across Member States, which act as a barrier to greater data sharing.
- **Put individuals and businesses in control of their data.** Users should be in control of their data, which includes controlling how it is shared and with whom (data access must be granted with permission by the individual or business). We support enhancing data portability to empower individuals to understand and effectively utilise their rights. This portability should ensure that data can be shared in a way that is simple, ongoing, real-time, standardised (via Application Programming Interfaces (APIs)) and secure.
- **Ensure the secure transmission of data.** In line with the Commission's Data Strategy, we believe a future framework should be considered that outlines the conditions for the secure transmission of data. APIs are the preferred industry method for the transmission of data as they are secure, efficient and can provide access on a real-time and/or regular basis. Further, access can also be more easily revoked, where appropriate. Interoperability between APIs will be essential to make data sharing a reality (both within and across sectors).

- **Clarify the different types of data that could be shared.** Action is needed from the Commission to delineate clearly between raw/observed data and elaborated/inferred data insights. Users have rights relating to their raw and observed data (e.g. their consumption data or transactions history, search history, contact list); however, organisations can then build around this data to enhance its quality and value. Organisations must be able to retain this value. In line with the Article 29 Working Party[1], we believe that elaborated or inferred data insights should not be subject to mandatory sharing requirements between businesses, except as specific competition policy interventions.

AFME would welcome the opportunity to discuss our response to this Consultation Paper (CP) in further detail and identify where we can continue to support the Commission in this important initiative.

Content

This paper is comprised of five sections which support our response to the Commission's 'A European Strategy for Data' public consultation, launched on 19 February 2020. The sections are:

1. Data access;
2. Data sharing and user control;
3. Access to public data;
4. Common European Data Spaces; and
5. Cloud computing

Questions in the CP that are addressed further in this paper are provided in the title headings below.

1. Data access

AFME believes that when proposing a strategy for greater data sharing in the EU, the Commission should consider principles for safety, efficiency and appropriateness with regard to data access.

Access to a wider range of data can create new opportunities, as currently, the amount of data held by FIs is limited compared to other organisations, such as technology platform providers. In some cases, FIs can only access this data in a rudimentary manner, relying on bilateral agreements and being subject to those organisations' terms and conditions.

We note also that Artificial Intelligence (AI) techniques are a crucial element to understanding and effectively utilising data[2], therefore we request that the Commission's AI Strategy compliments, and is coordinated, with the Commission's work on a European Data Strategy.

1.1. Governance mechanisms for data access (Q7, Q8, 12)

AFME believes the Commission has a role to play to facilitate the improvement of mechanisms for data access. This could include improving governance and coordination mechanisms and improving technical infrastructure for exchanging data. However, we agree that Commission should "[abstain] from overly detailed, heavy-handed ex ante regulation" and focus on "an agile approach to governance that favours experimentation."[3]

We believe that a current lack of effective mechanisms to allow individuals, FIs, or other organisations to safely share and reuse data is a barrier for the financial services sector. In particular, some FIs have faced difficulties in using data from other non-financial organisations, either because data is unavailable or access is denied, or because there is a lack of

[1] https://edpb.europa.eu/our-work-tools/article-29-working-party_en
[2] For more information on the use cases and applications of AI in capital markets see https://www.afme.eu/reports/publications/details/Artificial-Intelligence-Adoption-in-Capital-Markets
[3] See European Strategy for Data, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf p 12.

technical interoperability, transfer mechanisms and/ or appropriate security measures. We provide some additional detail below:

- **Denied data access, prohibitive processes or other conditions considered unfair or prohibitive**

It can be difficult for some organisations to access certain types of data, in particular where other organisations have greater bargaining power, even though other valued data could be offered in return, in full compliance with the General Data Protection Regulation (GDPR) and with consent from the individual. 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.

- **Technical aspects relating to both data interoperability and transfer mechanisms**

The lack of harmonised transfer mechanisms with corresponding API standards is one of the main barriers to data sharing and data availability. Further, the reading and capturing of relevant data from public registers (e.g. powers of attorney, incorporation of companies) has proven difficult, because organisations must first train algorithms to read the text in order to structure the data. More broadly, the utilisation of unstructured data remains difficult for these and other technical reasons and could be a promising field of innovation in Europe.

1.2. Data standardisation (Q13, 14, 15, 16)

One main issue with standardisation across sectors is 'the absence of a consistent description of the data, including information on how it has been gathered'.[4] There is a need to consolidate the different data types, standards and ontologies that are in use in different sectors in the market today. In this respect, we note that standardisation of data definitions will be an essential pre-cursor to other initiatives required to facilitate data sharing, for example where the value of an API as a sharing tool is reduced if the inputs are not consistent. It will be important for European supervisory authorities and standards setting bodies, as well as global organisations, to coordinate in achieving this goal.

An important aspect of standardisation is ensuring a user is able to identify the exact authority that is the holder of a specific dataset and ensuring that the request for data access is processed quickly and efficiently, within agreed deadlines. We believe the following mechanisms would be most effective for facilitating standardisation:

- **Metadata schema and metadata variables**:

Metadata is critical for enabling rapid service switching between different providers, preventing vendor lock-in and increasing the mobility of data between systems.

- **APIs**

Allowing FIs to more easily integrate standardised APIs would be beneficial to all industry participants (including supervisory authorities and third-party providers) and would promote a level playing field. APIs should be uniform where possible, and technical details of the required API functionality and standards landscape should be clearly defined. We note, for example, that standards continue to be developed as part of the ongoing MiFID review on market transparency, to promote greater efficiencies[5].

- **User experience**

Sharing is only successful if users complete the necessary process, including any authentication processes (e.g. identity verification) and the selection of relevant datasets. This requires the data sharing process to be efficient, user-friendly and to maintain users' confidence. Certain standard approaches can help ensure this is adhered to by all organisations. This could include, for example, maximum API response times, minimum API uptimes and the removal of artificial barriers during the user journey.

[4] See European Strategy for Data public consultation paper, https://ec.europa.eu/eusurvey/runner/DataStrategy, p 9.
[5] E.g. https://www.esma.europa.eu/sites/default/files/library/mifid_ii_mifir_review_report_no_1_on_prices_for_market_data_and_the_equity_ct.pdf

Further, European and national government bodies can play an important coordination role by supporting the prioritisation of standardisation needs, their development, and updates and maintenance. Regulators can also encourage standardisation across sectors, which should be an important element for greater data sharing. Standards should be set by professional global or European standard setting organisations, however these standards should also be clearly endorsed by EU government bodies in order to avoid market fragmentation. Further, this is not the only role that regulators could take, and some level of funding may also be required.

1.3. The role of data professionals (Q5)

The difficulties in recruiting data professional are not consistent across sectors, including financial services. They may include a range of factors, such as: salary, skills or location.

Financial services firms are often at a disadvantage in their ability to attract talent in technology and innovation due to the need to fulfil regulatory requirements that other firms (such as technology companies) are not subject to. For example, financial services firms in the EU must operate under compensation and incentive requirements for employees within the EBA 'material risk takers' framework[6].

We would welcome further clarity from the Commission on which difficulties in recruiting data professionals are implied in the survey.

2. Data sharing and user control

2.1. Data portability (Q3)

AFME agrees that it should be easier for end users to give access to their existing data. Further, we support enhancing data portability to empower individuals to understand and effectively utilise their rights. This portability should ensure that data can be shared in a way that is simple, ongoing, real-time, standardised (via APIs) and secure.

We note that greater control and sharing of data could allow for increased data use and reuse in the financial sector, creating opportunities to improve products and services for end users and to improve the accuracy of underlying systems (e.g. systems pertaining to fraud, security, AML). Relevant data of this nature is also held by organisations in sectors outside of financial services that includes but is not limited to e-commerce, telecommunications, public utilities services, social media platforms and the public sector.

Individuals in the EU now have a right to data portability under GDPR. However, data-holders in some instances respond to such queries in various formats and timelines that are not compatible with an end users' preference for greater immediacy, as GDPR allows an organisation up to 30 days to respond. These implementation issues, among others, may require further assessment by the Commission to ensure data is shared with appropriate immediacy while protecting the rights of the individual.

Action should also be taken to ensure that organisations can also exercise control over their data and share it if they so choose. Under the framework created by the Second Payment Services Directive (PSD2), FIs now provide third parties access to both organisations' and individuals' information in a structured, safe and consistent manner. The initiatives in the Data Act to clarify organisations' rights over data (particularly where it is co-generated) should be a precursor to any wider initiative to also provide organisations with effective portability of their data, as should improving the security of data shared by FIs to non-FI third parties.

A first step towards this could be taken as part of the development of ex ante rules for markets with digital platforms, planned for the Digital Services Act. An increasing number of organisations depend on and transact through digital platforms, making the data stored in these platforms critical to business users. If this data was shareable it would increase

[6] https://eba.europa.eu/revised-regulatory-technical-standards-identified-staff-remuneration-purposes

competition and allow data to be reused across sectors to create innovative new products and services. Therefore, any new ex ante rules should ensure that digital platforms offer their business users portability tools that allow them to share their raw/observed data in the same way as individuals – in a way that is easy, secure, in real time, and on a repeated basis, through standardised interfaces such as APIs.

Europe has the opportunity to lead in this area by introducing a cross-sectoral data mobility regime with the end-user at the centre. This would stimulate innovation and competition for the benefit of both end-users and industry. If the Commission instead continues with a sectoral approach, this should at the very least include not only the key sectors identified within the Data Strategy, but also digital platforms, in order to ensure a level playing field. Whichever course is chosen, following a robust assessment of the market failures, it will be essential to have well communicated objectives, outcomes and timelines for every sector and to leverage lessons learnt from previous data sharing initiatives.

On a separate note, fragmented approaches to data localisation can be a hindrance to greater data sharing, so we request the Commission to continue to address the various approaches to data localisation across Member States.

2.2. The role of intermediaries (Q24)

Intermediaries (e.g. data brokers) may play a useful role in enabling individuals or FIs to take greater control over their data and facilitate data sharing with other organisations. However, regulation should not prescribe a particular business model for intermediaries and individuals. Organisations should be able to share their data with or without intermediaries.

Intermediaries, especially if they become significant, have the capacity hold a large amount of European citizens' data. Therefore, intermediaries must comply with all relevant regulations and should be certified to operate in this field. Regulatory requirements should be proportionate and risk based, for instance considering an intermediary's ability to potentially manage large amounts of EU citizens' data. However, it is important to note that intermediaries can, where regulated appropriately, play a beneficial role by helping citizens manage their consent and data sharing preferences. For instance, cloud-based intermediaries can sometimes increase administrative efficiency.

2.3. Horizontal data sharing initiatives

2.3.1. Areas where horizontal data sharing would be beneficial (Q14)

The benefits of data sharing should also be viewed from an end-to-end use case perspective, rather than within a sector.

Combatting fraud and scams – some of the fastest growing crimes across Europe – is a clear example of where greater data sharing between sectors could result in societal benefits (protecting customers from losing their money, and stemming the flow of funds to organised crime). These types of crimes are increasingly undertaken through the exploitation of vulnerabilities across multiple organisations (e.g. social media sites, online sales platforms, dating websites, telecoms networks, and financial services firms). Therefore, greater sharing of data between these organisations could enable potential fraud and scams to be identified earlier, stopping them at their source.

A cross-sectoral approach will also be key to fulfilling sustainability objectives, as outlined in the European Green Deal, as data on emissions, energy usage, and climate risk mapping will be key in identifying more sustainable products and services and ways of doing business. We therefore invite the Commission to facilitate the development of data ecosystems for the sharing of relevant Environmental Social Governance (ESG) data.

There are some cases where useful data insights are intuitively material. However, in other occasions, the usefulness of data cannot be realised until it is analysed (e.g. through AI techniques). Therefore, it is important that data access also provides opportunities for analysis and testing of large and anonymised data sets. For example, the Commission has recently launched the European COVID-19 Data Portal to facilitate the sharing and analysis of relevant data amongst researchers[7].

[7] https://www.ebi.ac.uk/covid-19

2.3.2. The role of the public sector (Q10)

AFME believes that public and private organisations should be able to retain full control over the data they generate, however action is needed from policymakers to delineate clearly between raw/observed data and elaborated/inferred data insights. Users have rights relating to their raw and observed data, in which organisations can then use their expertise to build around this data (for instance through data validation, combination and analysis). This data is the product of the intellectual property of an organisation, so to continue to encourage research, development and innovation, organisations must be able to retain this value. Further, this data is unique to an individual organisations' processes and would not necessarily be easily standardised or understood by other industry participants. It is for these reasons that we believe elaborated or inferred data insights should not be shared between organisations on a mandatory basis, except where required as part of specific competition policy interventions where a market failure is clearly detected.

Any major government investments that enhance data access and use should also ensure high standards for cybersecurity. However, the Commission should avoid making significant investments in infrastructure with no clear use case or benefits.

Further, we somewhat agree that public authorities could do more to make available a broader range of data for Research and Innovation (R&I) purposes for the public interest, in full respect of data protection rights. However, this should come with clear terms & conditions regarding the limitations of use of such data, minimum expected protection needs, and what to do in case of a breach involving this data. There are important considerations, such as cost, data protection and commercial sensitivities, when this data is generated or held by private organisations.

Finally, individuals and organisations should be able to access and share more easily their information held by public sector organisations. The public sector should be at the forefront of ensuring that this is possible for the most valuable datasets.

3. Access to public data

3.1. High value datasets (Q26, 27, 28, 29)

High value datasets may provide useful insights for FIs that can be used to drive improved services and offerings for clients. While the re-use of data would likely increase if provided with limited or no cost, this does not need to be the approach to all data sets. 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. The ability to monetise data services will also encourage innovation and competition and improve FIs' capacity to offer enhanced products and services. This is particularly the case for inferred data sets, which can be offered to individuals for enhanced products and services at a cost. We request the Commission to consider these factors further.

We believe the below factors are relevant to improving the re-usability of specific high-value datasets:

- Licensing and other terms of applicable to re-use;
- Standardised formats of data and metadata;
- Possibility of user feedback; and
- Specific technical arrangements for dissemination.

Standardised or common data exchange protocols and APIs across data providers, particularly within a Member State, would support the reuse of datasets and maximise value. However, standardisation should not come at the cost of creating additional barriers or complexity, which could limit an organisation's capacity to test new variables in search of meaningful correlations.

Regarding thematic categories for high-value datasets (as referred to in Article 13(1) of the Open Data Directive[8]), we believe that ESG data would be useful for FIs, as it is a driving force for the reshaping of financial services and it would assist with the assessment and analysis of climate risk. ESG data is also useful for understanding the physical risks that contribute to the measurement of an organisation's climate risk exposure and for the development of improved services and offerings for clients who seek to hedge against their own climate risk. We note that ESG data can be utilised like any alternative data source for financial analysis purposes, such as for investment and credit forecasting. Specific types of environmental datasets could include information that pertains to the physical risk associated with climate risk, such as natural disaster risk mapping (e.g. flood plain data) and weather forecasting information. Building energy efficiency certifications could also be leveraged as part of investment analyses. However, ESG data quality is an important issue that will need to be addressed, and ESG source diversity is key. We request the Commission to consider further how the European Data Strategy will cover ESG data.

We request more detail from the Commission on what "statistics" as a dataset would be included in the Data Strategy (beyond the demographic and economic indicator examples provided in paragraph 66 of the Open Data Directive). We believe relevant statistics could include economic indicators (such as income) at high levels of granularity and availability on at least a monthly basis, with disaggregation by geography or local administrative region and by demographic characteristics. Ideally, these statistics would be published on a regular basis by central and regional governments and be available wherever feasible through standardised technical interfaces, such as APIs. The accuracy of data is crucial in supporting decision-making processes, therefore it is important that this data is pre-validated where possible.

The following information might be useful regarding company ownership, if not already available through APIs:

- Company registration information and public accounts; and
- Court information regarding companies, e.g. public case brought by state against a firm.

In respect of "companies and company ownership", the provision of beneficial ownership information can be utilised for AML purposes within financial institutions, which would yield benefits for society.

Regarding mobility, information on the transport sector is relevant for developing new products. This could take the form of anonymised disaggregated passenger travel information on all public transport (i.e. travel journey for each transport customer, without other personally identifying factors). Furthermore, greater access to public data related to the spread of COVID-19 could be leveraged by FIs as part of their resiliency planning and for the maintenance of appropriate health and safety procedures in real time.

3.2. Government to business (G2B) data sharing

Mechanisms should be put in place to ensure individuals and organisations are able to share their data that is stored by the government. This will yield greater efficiencies (including potentially within the public sector itself) and allow for more effective reuse of data across private sector services.

Decisions around the sharing of government or regulator held information must be transparent to preserve trust between parties. Regulators should disclose the way information will be shared, how it will be changed or amended prior to publication and exactly what information will be available. Further, we encourage the Commission to ensure a level playing field when requiring business to government (B2G) data sharing from different sectors.

We also note that depending on the nature of the underlying data, to the extent that data is shared with regulators and includes data points with reference to third parties, there is the potential for an inadvertent disclosure of another organisation's sensitive information. Any governance framework needs to appropriately cater for these scenarios.

A number of key data sets are likely to involve minimal references to third parties and the public sector could move rapidly to enable easier sharing by organisations and individuals.

[8] https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information

4. Common European Data Spaces

AFME believes that CEDS, if created appropriately, could support a stronger European data economy. However, we acknowledge that at this stage of their consideration, further clarity on their role, purpose, operation, technology (infrastructure) and governance will be required.

To support the Commission, we set out below what we believe should be the key objectives for CEDS and considerations for their governance.

4.1. Objectives (Q11)

We believe a CEDS should aim to provide additional benefits to market participants, drive greater efficiencies within organisations and meet other public policy objectives such as achieving sustainability goals, or in the financial sector, supporting improvements to financial stability or operational resilience.

We believe that when designing CEDS, the legislation should recognise that data generated in one sector may be relevant in another and therefore facilitate the flow of data both within and between sectors, where there is a specific use case.

For example, access to additional and varied data, if facilitated appropriately, could improve service offerings to end-users, for instance through improved risk management by the FI (e.g. better fraud and cyber incident detection). A "European Green Deal data space" may support access to and sharing of data that is useful across a number of different sectors, including the financial sector. The financial sector could use relevant data to contribute to its role in helping market participants and wider economy meet sustainability objectives, including through better climate change related risk assessments or the provision of green-loans. Data would be best organised as an ecosystem in these cases.

We believe that further consideration is needed regarding what data types should be shared in a CEDS and the cost implications this will have on FIs. If data sharing is mandated and not on a voluntary basis, a CEDS must ensure that all market participants are subject to the same requirements, and we believe that elaborated or inferred data insights should not be shared between organisations on a mandatory basis, except where required as part of specific competition policy interventions, if a market failure is clearly detected. A situation where organisations bear the costs for the business models of their competitors (for instance where PSD2 has allowed other organisations to develop banking services without maintaining banking technology infrastructure) will not only limit the organisation's ability to invest in innovation but may also have negative implications on their ability to maintain and continuously improve their technical infrastructure and on their business model. This could potentially affect the sector's resilience.

Other factors such as privacy, data concentration risk and appetite from institutional clients for greater data sharing should also be considered. We caution the Commission to consider these issues in detail when exploring initiatives that may build on existing horizontal data sharing initiatives such as PSD2.

4.2. Governance

Standardised APIs will be an important mechanism for ensuring the secure and efficient transfer of data. We believe authorities could play a strong coordinating role here, particularly in coordinating the development of standards. There is a need in particular for greater coordination between the relevant EU-wide authorities (e.g. European Supervisory Authorities, European Data Protection Board, DG Competition) and their national counterparts, although global coordination should also be an objective.

Intermediaries can also play an important role in sharing information and providing useful services that other organisations are unable to offer, ensuring the protection of users' data.

5. Cloud computing

While Section Five is dedicated to cloud computing as part of our response to the CP, we note that cloud is only one method for data computation. Other examples include big data platforms (e.g. Hadoop and Spark), GPU, edge computing, and next-generation computing, such as quantum computing, noting that they do not all possess the same capabilities. These examples should also be assessed by the Commission in the context of the Data Strategy.

5.1. Cloud in Financial Services (Q30, 31, 33)

AFME believes that the cloud market currently offers solutions that support innovation in financial services. In our 2019 paper on '*Public cloud adoption in capital markets',*[9] AFME members cited benefits of cloud that included:

- Greater business agility and innovation;
- Improved overall cost management;
- Increased operational efficiency;
- Enhanced client experience and service offerings; and,
- Effective risk mitigation.

We believe that cloud services can bring security benefits to the financial services industry, supporting the Commission view that correct usage of cloud can increase overall security resilience.[10] We also believe that the adoption of cloud can provide an enhanced ability to identify and remediate system vulnerabilities through a series of controls. In particular, the ability to flexibly deploy encryption and key management can mitigate the risk of unauthorised access data stored on the cloud.

It is important to encourage the efficient functioning of the European cloud market but also to ensure this contributes to the efficiency of the global market for cloud services. In the context of FIs that execute a global operating model, the ability to utilise cloud technologies in different jurisdictions supports the ability to leverage different technologies and therefore contributes to enhanced resiliency and scalability. As such, any initiatives that are put in place to remedy problems experienced in the European context should appropriately consider the implications, intended and unintended, for FIs' ability to operate such global models.

5.2. The European Cloud Market

We consider that increased competition in the European Cloud Market will result in greater innovation and advances in the technology to the benefit of users. We therefore support efforts to increase the supply of cloud services provided by EU-based organisations. Further, we welcome the Commission's efforts to ensure that cloud services, regardless of their geographical origin, be used in such a way that is fully compliant with EU law and data privacy regulation.

In addition, we see market demand rapidly driving Cloud Service Providers (CSPs) towards greater interoperability. Several providers, including newer and established providers, have launched multi-cloud offerings designed to increase the portability of cloud deployments. We recommend that the Commission consider what it can do to further encourage the market in this direction.

5.3. Problems (present) (Q34, 35)

Problems experienced in the current functioning and constitution of the market for cloud services in Europe relate to:

- **Asymmetry of power negotiation between customer and provider**

Negotiation issues may arise if CSPs are unable or unwilling to satisfy an organisation's necessary terms to fulfil financial sector specific regulation. This asymmetry of negotiating power is aggravated when dealing with larger CSPs. Example areas of contractual challenges include access and audit rights or notice and post termination periods for exit (e.g.

[9] https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20Cloud%20Paper%20November%202019%20Final.pdf

regarding changes in sub-providers). We recognise that the Commission is currently developing Standard Contractual Clauses (SCCs) which could help in some areas, such as access and audit rights.

- **Contractual practise on the market, including unilateral change of terms and conditions**

FIs often face problems with CSPs whose business models provide a 'one to many' service globally. The possibility of unilateral changes in terms and conditions creates uncertainty for cloud adoption. FIs require sufficient time to assess changes made (and withdrawal orderly from a contract or service if deemed necessary). Changes to terms and conditions should be clearly communicated ensuring minimum notification periods to inform customers. Pre-contractual information, such as service fees, could also be set in agreements (rather than contained within a separate webpage) and sufficient notice given of any change.

- **Other - Termination periods and Switching**

Although some amount of vendor lock-in will always be present (specially in Software as a Service offerings – SaaS – which may have no suitable market alternative), providers do not always guarantee an appropriate period of time for an effective migration of data to another provider or in-house development.

- **Other – Data localisation requirements**

Regulatory fragmentation can create additional barriers for market participants. Different jurisdictional requirements for the localisation of data can prevent certain activities or limit the storage of data when using the cloud.

EU regulations, such as GDPR, the Free Flow of Non-Personal Data Regulation (FFND), and the 2019 EBA Guidelines on Outsourcing, have made significant progress in clarifying, or removing, regulatory inconsistency such as data localisation requirements. However, variations remain at the Member State level, especially in data location requirements, which continue to add complexity for the adoption of cloud at scale for cross-border banks and limit the security and resilience posture of the industry.

We request the Commission to support greater harmonisation in respect of cloud requirements (promoting a consistent framework for authorisation, adoption, management and reporting) and to continue to identify and remove forced data localisation requirements.

5.4. Risks (future) (Q36, 37)

Some possible risks that we perceive include:

- **Asymmetry of power negotiation between customer and provider**

This can present issues in the context of 'sub-outsourcing', where a vendor is not itself a CSP but subcontracts to a CSP (i.e. the vendor is an intermediary between the bank and the CSP). These vendors may face issues contracting with a CSP to reflect the outsourcing requirements of supervisory/regulatory authorities, particularly where they are software providers and not regulated FIs.

- **Contractual practise on the market, including unilateral change of terms and conditions**

Ensuring a sufficient level of unlimited access and audit rights for financial institutions and supervisors, as required by the EBA 2019 Guidelines on Outsourcing, remains challenging in negotiations with CSPs.

- **Other: Concentration risk**

Concentration of cloud services within a limited number of CSPs could introduce risks at an industry level. For risks of this nature, authorities (e.g. supervisory bodies) are well positioned to have oversight at an industry level, as compared to FIs individually, and to take any necessary actions. In addition, we believe that introducing new mandatory solutions on FIs (such as exposure limits, or mandatory rotation mechanisms) would potentially impact FIs' ability to continuously enhance resilience capabilities, adapt to emerging business models and technologies, and make commercial decisions.

FIs should continue to have the flexibility to define their own cloud strategy, following a risk-based approach, as noted in our response to the European Commission Public Consultation on 'Digital Operational Resilience: Making the EU financial sector more secure'.[11] We therefore recommend, as stated in our response, that the Commission continues to collaborate with the industry (FIs, CSPs, Authorities) in this regard to support continued cloud adoption within the EU.

5.5. Flexibility to procure/adopt new and innovative cloud solutions (Q38, 39):

Whilst we believe FIs have sufficient flexibility to procure/adopt new and innovative cloud solutions, a number of barriers provided by the Commission are often faced.

There is a lack of clarity and support from authorities on the applicability of the 2019 EBA Outsourcing Guidelines to SaaS providers. This often presents a challenge in negotiating agreements that can satisfy regulatory requirements with these providers.

There is also a lack of harmonisation regarding the notification and/or approval of migration of services to the cloud as outlined in the 2019 EBA Guidelines on Outsourcing. For example, the Luxembourg CSSF Cloud Circular imposes notification and approval requirements for the use of cloud platforms constituting "material activities".[12] FIs need common criteria to facilitate greater scalability in cloud solutions when operating in several EU countries. The need to have a prior authorisation (or at least no opposition) from authorities (as it happens in some Member States), as opposed to a notification, can limit time to market for moving to the cloud and creates a fragmented EU approach.

Related to this issue is also the approach to private cloud adoption (where some jurisdictions have included authorisation requirements for the migration to internal cloud infrastructure that is provisioned for exclusive use by a single organisation).

We therefore recommend that the Commission continues to support harmonising cloud regulations across EU Member States, such as the 2019 EBA Guidelines on Outsourcing, which will support both FIs and CSPs in promoting adoption and limiting regulatory fragmentation. We also support plans for the creation of an 'EUCloud rulebook' which could usefully include some more explicit requirements such as those in the 2019 EBA Guidelines on Outsourcing.

5.6. Regulatory approaches (Q42, 43)

AFME believes that a self-regulatory approach is currently appropriate for identifying best practises to apply to EU cloud legislation. Self-regulatory approaches allow for a flexible adaptation to innovative practices and products; this is especially important for technologies and services, such as cloud, that are continuing to mature and develop at pace. Authorities should continue to support the development of these proposals, such as CSP security certification schemes, as a mechanism to reduce the due diligence obligations when adopting cloud services.

We note that the Commission is progressing an initiative from the 2018 Fintech Action plan on the development of SCCs for cloud use in the financial sector. We support this initiative and note that SCCs could provide value where applied consistently throughout Europe and reduce regulatory fragmentation across Member States.

However, whilst SCCs should provide a useful tool to achieve compliance with the 2019 EBA Guidelines on Outsourcing for critical/important cloud outsourcings, they should not be become an additional compliance obligation for FIs, and should be seen as one path to compliance for FIs. FIs must already comply with the requirements as set out in the 2019 EBA Guidelines on Outsourcing, and an additional compliance layer would likely contribute to additional cost and complexity.

We would welcome further discussion with the Commission on how the SCCs are intended to be implemented and governed, and how they can facilitate the greatest value to the industry in their intended form.

[11] https://www.afme.eu/Portals/0/DispatchFeaturedImages/20200319%20AFME%20EC%20CP%20Digital%20Operational%20Resilience.pdf
[12] https://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf19_714eng.pdf

AFME contacts

Andrew Harvey, aharvey@gfma.org	+44 (0)203 828 2694
David Ostojitsch, david.ostojitsch@afme.eu	+44 (0)20 3828 2761
Hélène Benoist, helene.benoist@afme.eu	+32 (2) 788 3976
Madeline Taylor, madeline.taylor@afme.eu	+44 (0)20 3828 2688

About AFME

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 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 listed on the EU Register of Interest Representatives, registration number 65110063986-76.