

FESE response to the Commission consultation on the Data Act

1st September 2021, Brussels

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

Q1. 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

Q2. 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

Q3. 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

use), including competition rules						
Commercial disincentives or lack of incentives/interest/willingness	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of skilled professionals (public and/or private sector)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of safeguards ensuring that the data will be used only for the public interest purpose for which it was requested	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of appropriate infrastructures and cost of providing or processing such data (e.g. interoperability issues)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of awareness (benefits, datasets available)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insufficient quality of public authorities' privacy and data protection tools	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q4. 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

management, prevention and resilience			
Data (e.g. price data from supermarkets) for official statistics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data (e.g. emissions data from manufacturing plants) for protecting the environment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data (e.g. fuel consumption data from transport operators) for a healthier society	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data for better public education services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data (e.g. employment data from companies) for a socially inclusive society	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data for evidence-based public service delivery and policy-making	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q5. 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

Please provide an example(s) of when public sector bodies should be able to obtain data for the public interest at a preferential rate.

As a general rule, FESE believes that when sharing data with public bodies businesses should provide it at market price. It is important that data sources are fairly remunerated, so they have an incentive to produce high-quality data. However, limited exceptions to this general principle can be made where the data is solely used for a relevant supervisory purpose and in consultation with the business in question and based on a legislative mandate.

Q6. What safeguards for B2G data sharing would be appropriate?

- 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

Q7. 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

Q8. 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

2. Business-to-business data sharing

Q9. 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

(if yes) Are you:

Data holder

Data user

Both data holder and user

Other

(if yes) In the last five years, how often has your company shared data with other companies?

Many times

Only a few times

Don't know

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

Production, dissemination, marketing of data from financial products listed with FESE Members. Also, price data, reference data, index data, or statistics about products. No personal data is involved.

(If yes) On what basis does your company share data with other companies?

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

(If yes) Why does your company share data with other companies?

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

(If other) Please specify: (200 character(s) maximum)

B2B data sharing works best where the data holder has an incentive to share data. The offering/commercialisation of data products is part of Exchanges' business.

Q10. 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 character(s) maximum)

Data is produced from listing and trading of financial products. This data is produced internally.

Q11. What benefits from data sharing do you expect to be reaped in your sector? (300 character(s) maximum)

The offering/commercialisation of data products is part of Exchanges' business. As such, the benefit is economical.

Other data is mandatory from a regulatory perspective and contributes to the overall supervision and resilience of financial markets.

Q12. Has your company experienced difficulties/encountered issues when requesting access to other companies' data?

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

Q13. 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 nonpersonal IoT data in professional use)?

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

Q14. 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

Q15. 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

Q16. 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? (*at most 3 choice(s)*)

- 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

(If other) Please explain:

Companies need to invest to develop data products/services and the party sharing data must obtain a reasonable return. Investment incentives are key where a satisfactory downstream yield is necessary.
--

3. Tools for data sharing: smart contracts

Q17. 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

Q18. 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

Q19. 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

Q20. 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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of interoperability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Difficulties with governance	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data protection issues	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Competition law compliance concerns	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q21. 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?

Cross-blockchain bridges (e.g. oracles, sidechains, asset lock-in models) enable the transfer of information or assets across the blockchain and pose considerable security risks. An added layer of security to the underlying blockchains should be provided to ensure effective transfer of information.

4. Clarifying rights on non-personal Internet-of-Things data stemming from professional use

Q22. Do you currently or are you planning to use in the near future a smart object connecting to the Internet-of-Things?

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

Q23. Do you agree that IoT objects and data coming from such objects may represent new challenges for market fairness when access to relevant information concerning the functioning and performance is held by the manufacturer of such object?

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

Q24. Is your company in the business of after-sales services that use data from IoT objects in professional use in order to offer that service (e.g. repair and maintenance, data analytics services)?

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

Q25. What was the nature of such difficulties?

- Outright denial of data access
- Prohibitive monetary conditions for data access
- Prohibitive technical conditions for data access
- Restrictive legal conditions for data access and use
- Competition law compliance concerns
- Other
- I don't know / no opinion

Q26. How relevant were the difficulties signaled in response to the previous question?

- They appear frequently and/or are having a considerable impact on my business
- They appear infrequently and/or are having only a minor impact on my business
- They only appear rarely and/or have an insignificant impact on my business
- I don't know / no opinion

5. Improving portability for business users of cloud services

Q27. Was your organisation aware of the SWIPO Codes of Conduct prior to filling in this questionnaire?

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

(If yes) 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

Please explain:

SWIPO is not binding and does largely rather cover principles than concrete rules. Rules need to be more concrete and binding.

Q28. 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

Please explain your answer, detailing as much as possible what this right should entail.

Such right would be needed to avoid vendor lock in effects and increase resiliency being able to run workloads on different providers when required. Highest need is seen in the area of SaaS services.

Q29. 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?

- 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)
- More specific set of conditions of contractual, technical, commercial and economic nature, including specification of the necessary elements to enable data portability
- Other solution
- I don't know / no opinion

Q30. 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

Please explain:

SWIPO codes can serve as a good basis, but regulation needs to be more specific, e.g. providing concrete timeframes for migration.

Q31. 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

Can you be more specific about which standards should be developed in this regard?

Consider reuse of GAIA-X formats or include development of new formats into this initiative. Standards should be minimal requirements, not hindering innovation of CSP or compromising IT security.

(If yes) 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

Please specify how such standards should be identified / developed

We consider it best suitable to develop standards embedded, for example, in the GAIA-X initiative.

Q32. 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 stand alone 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

Q33. Do you have any other comments you would like to address with respect to cloud service portability, which were not addressed above? (300 character(s) maximum)

Cloud services are important for exchanges. We recognise the limited offer of EU providers but to favour innovation, it is crucial that the EU market remains open to non-EU Cloud providers. We would also like to stress the current asymmetries of power in negotiation between customers and CSPs.

6. Complementing the portability right under Article 20 GDPR

Q34. 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

Q35. 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

Q36. Among the elements listed below, which are the three most important elements that prevent the right under Article 20 GDPR to be fully effective?

- 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

7. Intellectual Property Rights - Protection of Databases

7.1. Intellectual Property Rights - General questions

Q37. 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

Please specify or explain: (200 character(s) maximum)

In the case of data ownership, data owners should have the right to be protect valuable data through intellectual property.

Q38. “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

Please explain: (200 character(s) maximum)

7.2. Questions on the Database Directive

Q39. 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

Please specify:

Q40. 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

Q41. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. (200 character(s) maximum)

Q42. According to your experience, which of these statements are relevant to your activity / protection of your data?

- 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

Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. (200 character(s) maximum)

Q43. 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

Q44. 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

Please specify: (200 character(s) maximum)

Q45. 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 use
- 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

Q46. Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. Please indicate how often you have encountered these difficulties in the past 5 years. (200 character(s) maximum)

Q47. 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

Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. (200 character(s) maximum)

Q48. 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

Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. (200 character(s) maximum)

Q49. 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

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 character(s) maximum)

Q50. 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

Q51. In your opinion, how would specific access rules in the Database Directive be best achieved?

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

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 character(s) maximum)

Q52. 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

Q53. 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

Please explain and substantiate your answers with concrete examples and any useful information and experience you may have. (200 character(s) maximum)

Q54. 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:

- 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

Q55. 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 character(s) maximum)

Q56. Please provide any other information that you find useful regarding the application of the Database Directive in relation to the data economy. (200 character(s) maximum)

7.3. Questions about trade secrets protection

Q57. Do you rely on the legal protection of trade secrets when sharing data with other businesses?

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

(If yes) With whom do you share?

- Partner
- Supplier
- Customer
- Unrelated business
- Other

Please specify: (200 character(s) maximum)

(If yes) 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

Please specify: (200 character(s) maximum)

(If no) Please indicate why

- 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

Please specify: (200 character(s) maximum)

Q58. 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

8. Safeguards for non-personal data in international contexts

Q59. 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

Q60. 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 character(s) maximum)*

Q61. 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

Q62. 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

Please explain how it affects your decision: *(200 character(s) maximum)*

Q63. 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

Please explain what categories of data that should be stored in the EU/EEA only are concerned and why *(200 character(s) maximum)*

Q64. 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

Please specify: (200 character(s) maximum)

9. Closing section

Final comments:

FESE supports the plan of the European Commission in proposing an overarching data strategy that has the potential to achieve the benefits of the single market. To this end, we believe a harmonised European approach is preferable to speed up the use/investment in technologies while effectiveness, fairness, proportionality, the international competitiveness of the EU market, and the safety of its people should be a guiding principle.

We consider that regulators possess the appropriate tools to act effectively to prepare a harmonised approach. To avoid overregulation and/or ambiguity, special attention should be given as well to potential overlapping provisions. The Commission has produced an increasing number of initiatives in the data space. This non-exhaustive list includes:

- European strategy for data
 - Data Governance Act (DGA)
 - Implementing act on high-value datasets
 - Data Act
 - Supervisory data collection strategy
 - Further open-finance initiatives
- European Single Access Point
- Consolidated Tape under MiFID II/R

FESE is concerned that the scope of the various initiatives might overlap to a significant degree. For example, it is still unclear whether and to what extent the products and

services provided by trading venues are covered by the DGA proposal, and what would be covered, instead, in the potential scope of the "Data Act". Besides this, it is not clear how these proposals would relate in terms of sector-specific rules and regulations for the financial sector.

Furthermore, we took note that the "Supervisory data collection strategy" aims at considering several horizontal measures that contribute to the overall objective of improving supervisory data collection (i.e. B2G relations). The "Data Act", in a similar fashion, aims to ensure access and use of data for, inter alia, B2B and B2G situations. Hence, from our perspective, there is a clear overlap in scope.

The same can be traced under the ESAP proposal and the Commission implementing act on high-value datasets. Both have the objective of defining/establishing a dataset for financial and non-financial data and company information, albeit in different formats. These separate initiatives are under the remit of different DGs in the Commission (DG FISMA and DG CNECT).

The Commission should clarify and better define the scope of these initiatives. Legislative proposals should be designed to be proportionate to the existing business environment. From our perspective, these should not introduce new mandatory disclosure, access to data, or reporting requirements as there is a concrete risk of unnecessary duties duplication for both issuers and regulated markets. Furthermore, the possibility of gold-plating from Member States would exacerbate these risks.

Against this background, we call for a holistic approach that supports the EU's objective of enhancing the CMU for issuers and investors. An ill-designed data strategy will increase compliance cost for the financial sector, including trading venues and issuers, further fragmenting the virtual space where information/data is reported. This could create more barriers to investments.

FESE wishes to underline the need to recognise the importance of supervisors' understanding of supervised stakeholders and the markets where they operate. The right balance must be struck, within the European supervisory system, between a centralised European approach and the role of NCAs. For the same information, issuers and trading venues should report to one authority only, making it a simple and straightforward approach.

FESE urges the Commission to perform a general assessment of both the current proposals being discussed as well as those to come in the future. All data-related initiatives should be analysed in a harmonised and holistic fashion, characterised by strong cooperation and communication between the different DGs. We stand ready to provide the Commission with further clarity on the information reported by regulated markets.