Position Paper

Response to European Commission consultation on the Data Act

Our reference:	COB-TECH-21-089	Date:	September 2021
Referring to:	European Commission consultation on the Data Act		
Contact person:	Danilo Gattullo, Policy advisor conduct of business	E-mail:	gattullo@insuranceeurope.eu
Pages:	15	Transparency Register ID no.:	33213703459-54

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

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?

- [x] I don't know / no opinion

Please specify

On requests for access to data: while there are some technical challenges, there are no general obstacles present.

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?

- [x] I don't know / no opinion

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

	Strongly agree	Somewhat agree	Neutral	Somewhat disagree	Strongly disagree	I don't know /no opinion
Legal uncertainty due to different rules across Member States	○	○	○	○	○	**x**

Insurance Europe aisbl • rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

Legal barriers to the use of business data for the public interest (e.g. on what data can be shared, in what form, conditions for re-use), including competition rules						x
Commercial disincentives or lack of incentives/ interest/ willingness						x
Lack of skilled professionals (public and/ or private sector)			x			
Lack of bodies to help bring together supply and demand for data, and to promote, support and oversee B2G data sharing (e.g. provide best practice, legal advice)			x			
Lack of safeguards ensuring that the data will be used only for the public interest purpose for which it was requested		x				
Lack of appropriate infrastructures and cost of providing or processing such data (e. g. interoperability issues)						x
Lack of awareness (benefits, datasets available)			x			

Insufficient quality of public authorities' privacy and data protection tools	○	x	○	○	○	○
Other	○	○	○	○	○	○

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

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

Please specify

Companies are currently subject to extensive reporting obligations. Additional obligations, if not proportionate and legitimate, could lead to the disclosure of core business strategies and discourage investments in innovation.

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

- ■ Depending on the purpose it may be provided at market price, preferential rate or for free

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

B2G data sharing should be based on voluntary arrangements.

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

Please specify

Specific rules on proportionality would play an important role in ensuring that companies are not overburdened by data access requests. The recipient organisations should also have a consistent level of cyber security.

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

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

Which of the following types of non-monetary compensation would incentivize 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 X 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
- Other

Please specify

Companies' strategies and data policies can vary greatly. A one-size-fits-all approach is therefore unlikely to capture all nuances. A combination of the above-mentioned incentives has the highest chance of success.

II. Business-to-business data sharing

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

- Yes

Are you:

- Both data holder and user

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

- Many times

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

The insurance industry shares data intra-industry (eg, for the purpose of reinsurance or industry-wide statistics) and with external stakeholders across all business lines (e.g. surveyors, repair centres, government agencies).

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

- Both voluntary and mandatory

Why does your company share data with other companies?

- Optimisation of the supply chain
- Predictive maintenance
- Training algorithms for AI
- Design of innovative solutions/products
- Other

Please specify

Insurers share data with other companies for multiple purposes, eg, as part of their risk assessment and claims processing. New technologies such as AI and IoT will create new purposes for data sharing in the insurance value chain.

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

Insurers often cooperate with other companies to develop or improve existing offerings. For example, innovative products are available in motor insurance with telematics, which the insurance industry provides in cooperation with third parties. This also applies to IoT data and weather data.

What benefits from data sharing do you expect to be reaped in your sector?

Data sharing offers great opportunities for the insurance sector. With access to and exchange of more types of data, the insurance industry will be able to offer enhanced products and serve customers more effectively by, for example, improving existing risk models.

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

- Yes

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

- Often

What was the nature of such difficulties/issues?

- The data holder refused to give data on the basis of competition law concerns
- The data holder refused to give access to data for reasons other than competition law concerns
- There is no legal basis for the data holder to give access to data
- The data holder gave access to data at an unreasonable price
- Technical reasons like the data was not in usable format or quality or lacks shared vocabularies or metadata or the data holder doesn't support standards for enforce data usage controls (connector)
- Other

Please indicate the type of difficulties / issues

Insurers face multiple challenges when requesting access to other companies' data. The most common hurdles are: legal (GDPR, e-privacy, Solvency II non-insurance activities) and competition law concerns.

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

- I don't know / no opinion

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

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

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

The Data Act should strengthen framework conditions for data partnerships and not, as first step, introduce elements such as a fairness test. While terms of access to data considered essential should be encouraged on reasonable and non-discriminatory terms, they should not be imposed. Model contract terms can protect parties in weaker positions.

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?

- 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
- Other

Please explain

Distinctions should be made depending on the type of data or the purpose of its use. There should be no obligation to share enhanced or similarly processed data, which can be considered commercially sensitive.

III. Tools for data sharing: smart contracts

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

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

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

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

Please specify

Despite significant efforts to modernise privacy rules, the GDPR and the guidelines adopted by the European Data Protection Board (EDPB) are not entirely innovation-friendly or fit for a digital age. For instance, the use of blockchain technology in insurance could be jeopardised due to potential incompatibilities with the GDPR.

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

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

- [x] Yes

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?

- [x] Yes

Please explain your answer

Individuals should be in control of their data. For example, if a customer decides that an insurance undertaking may access their driving data, the vehicle manufacturer should grant access on reasonable terms.

To what extent are the following elements well addressed in contracts relating to the sale or long-term lease of IoT objects for professional use?

	Very well addressed	Somewhat well addressed	Neutral	Not well addressed	Not at all well addressed	I don't know/ no opinion
Right to know which data is being collected by the IoT object'	○	○	○		○	**X**
Right to access data generated by the IoT for own information purposes	○	○	○		○	**X**
Rights to use data generated by the IoT object by selected parties	○	○	○		○	**X**
Rights to transmit data generated by the IoT object to selected parties	○	○	○		○	**X**

Incentives (services, functionalities or other rewards) for permitting the manufacturer of the IoT object, his business partners or third parties to use the data that the object generates	○	○	○	○	○	x
Protection of trade secrets and other commercially sensitive information in the context of the regular data feedbacks of the IoT object	○	○	○	○	○	x

Have you experienced any of the following as a result of insufficient rights in contracts relating to the sale or long-term lease of an IoT object?

- ■ I could not pick and choose a repair or maintenance company of my choice
- ■ I could not use a data analytics service offered by another company because it was technically impossible to allow this service to read the data from the object that I use
- ■ Other

Please explain

Individuals should be in control of their data. For example, if a customer decides that an insurance undertaking may access their driving data, the vehicle manufacturer should grant access on reasonable terms.

How relevant where the difficulties signalled in response to the previous question?

- ■ They appear frequently and/or are having a considerable impact on my business

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

Has your company experienced difficulties in accessing relevant data?

- ■ Yes

What was the nature of such difficulties?

- Prohibitive monetary conditions for data access
- Prohibitive technical conditions for data access
- Restrictive legal conditions for data access and use
- Other

Please specify

Individuals should be ultimately in control of their data. For example, if a customer decides that an insurance undertaking may access their driving data, the vehicle manufacturer should grant access on reasonable terms.

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

Please provide reasons

The after-market for vehicles is a considerable economic factor, with providers from different industries competing to offer products and services.

V. Improving portability for business users of cloud services

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

- 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?

- I don't know /no opinion

In your opinion, could the SWIPO codes of conduct represent a suitable approach to address cloud service portability, if:

- The codes of conduct would be supplemented by Standard Contractual Clauses translating the Codes' requirement into contractual elements
- Other

Please specify

However, it is important that the use of these Standard Contractual Clauses would be voluntary so companies do not have to renegotiate individual clauses.

Do you consider there is a need to establish a right to portability for business users of cloud computing

services in EU legislation?

- Yes

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)

Please explain

Negotiation of contracts with cloud providers is sometimes difficult and very time-consuming. Requirements that are too detailed could be burdensome to negotiate (in this context voluntary standard contractual clauses could help).

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?

- No opinion

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

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

- Yes

Please specify how such standards should be identified / developed

It is important that any approach taken envisages appropriate consultation with stakeholders.

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 but in addition to a legislative right of data portability

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

While not strictly necessary, dedicated SCCs would bring benefits. SCCs would be a practical solution that simplifies portability without setting out detailed requirements that may be burdensome to apply in practice. Establishing high-level principles on cloud service portability would make the use of SCCs more effective.

VI. Complementing the portability right under Article 20 GDPR

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

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 disagree

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 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
- Other

Please specify

The absence of standards ensuring data interoperability, including at the semantic level, is also an important element to be considered.

VII. Intellectual Property Rights – Protection of Databases

Intellectual Property Rights - General questions

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 data from misappropriation and misuse
- To refuse sharing of data

"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?

- I don't know / no opinion

Questions on the Database Directive

Please select what describes you best

- User-maker of databases containing mixed type of data

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 am not sure what the relationship is between such data and the Database Directive

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

- I don't know / no opinion

Questions about trade secrets protection

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

- Yes

With whom do you share?

- Partner
- Supplier

Please specify

- Claims data is shared with partners and suppliers supporting the claims-handling
- In underwriting, data is shared with suppliers providing support when assessing the risk to be insured
- Reinsurance

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

Please indicate why:

- Other

Please specify

There are various circumstances to take into account in the data-sharing context. Key elements are the nature of the data processing, data protection aspects (including legal and security) as well as competition issues.

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 contractual arrangements
- We rely on technical means

Please specify which rights

Data security and integrity are at the centre of the sharing and accessing concepts. As are the state of the art and the specific risks involved.

VIII. Safeguards for non-personal data in international contexts

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 risk for our company

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:

Disproportionate orders/requests that do not serve prevailing substantial public interests and do not provide appropriate safeguards, enforceable rights and effective legal remedies.

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 risk for our company

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

Please explain how it affects your decision

The service provider is required to have implemented mechanisms to prevent and challenge such transfers/access and give notifications without undue delay.

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 anywhere in the world

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

Data should be stored and processed anywhere in the world as long as its safety can be ensured to a reliable extent. In contrast, data localisation is counterproductive to the free flow of data and hampers innovation.

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 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