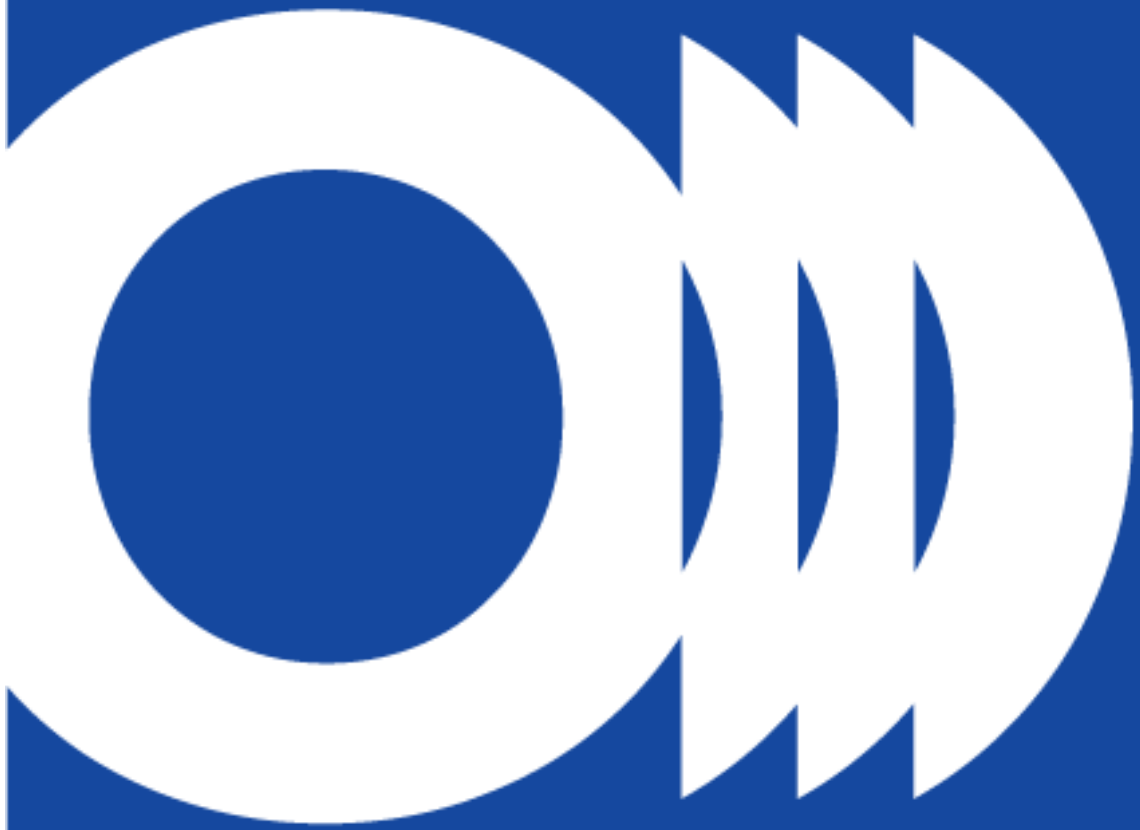
EBU
OPERATING EUROVISION AND EURORADIO

POSITION PAPER

EBU response to the European Commission's Public consultation on the Data Act

07 SEPTEMBER 2021



Contribution ID: f372c78c-f0f2-4c95-9d33-c32756d55d88
Date: 03/09/2021 18:53:23

Public consultation on the Data Act

Fields marked with * are mandatory.

Introduction

The COVID-19 crisis has shown the essential role of data use for crisis management and prevention, and for informed decision-making by governments. Data also has a key place in the recovery of the EU, given its potential for innovation and job creation, as well as its contribution to the efficiency of industries across all sectors. Data will also contribute to achieving the goals of the European Green Deal.

With its European strategy for data, published on 19 February 2020, the Commission formulated a vision for the data economy. This includes the adoption of a horizontal legislative initiative (the 'Data Act') that would complement the proposal for a Regulation on data governance, which was adopted by the Commission in November 2020.

The objective of the Data Act is to propose measures to create a fair data economy by ensuring access to and use of data, including in business-to-business and business-to-government situations. The initiative would not alter data protection legislation and would seek to preserve incentives in data generation.

Under this initiative, a review of Directive 96/9/EC on the legal protection of databases is also planned in order to ensure continued relevance for the data economy.

This questionnaire aims at consulting all types of stakeholders, including citizens and businesses, about the different measures being explored in preparing the Data Act. It is divided into the following sections:

I. Business-to-government data sharing for the public interest
II. Business-to-business data sharing
III. Tools for data sharing: smart contracts
IV. Clarifying rights on non-personal Internet-of-Things data stemming from professional use
V. Improving portability for business users of cloud services
VI. Complementing the portability right under Article 20 GDPR
VII. Intellectual Property Rights – Protection of Databases
VIII. Safeguards for non-personal data in international contexts

After the mandatory 'about you' section, please answer the sections that are of interest to you.
Please note that, although they all appear in the PDF questionnaire, some questions and the entire section on 'safeguards for non-personal data in international contexts' will only appear in the online questionnaire for respondents that indicated they are responding as a company/business organisation or as a business association.

The questionnaire will be available in all EU official languages on 11 June 2021.

Finally, please note that you can upload a document (e.g. position paper) at the end of the questionnaire.

About you

* Language of my contribution

- ○ Bulgarian
- ○ Croatian
- ○ Czech
- ○ Danish
- ○ Dutch
- ◉ English
- ○ Estonian
- ○ Finnish
- ○ French
- ○ German
- ○ Greek
- ○ Hungarian
- ○ Irish
- ○ Italian
- ○ Latvian
- ○ Lithuanian
- ○ Maltese
- ○ Polish
- ○ Portuguese
- ○ Romanian
- ○ Slovak
- ○ Slovenian
- ○ Spanish
- ○ Swedish

* I am giving my contribution as

- ○ Academic/research institution
- ◉ Business association
- ○ Company/business organisation

- ○ Consumer organisation
- ○ EU citizen
- ○ Environmental organisation
- ○ Non-EU citizen
- ○ Non-governmental organisation (NGO)
- ○ Public authority
- ○ Trade union
- ○ Other

* First name

Francois

* Surname

Lavoir

* Email (this won't be published)

lavoir@ebu.ch

* Organisation name

255 character(s) maximum

European Broadcasting Union

* Organisation size

- ○ Micro (1 to 9 employees)
- ◉ Small (10 to 49 employees)
- ○ Medium (50 to 249 employees)
- ○ Large (250 or more)

Business sector

- ○ Agriculture, forestry and fishing
- ○ Food processing, food supply chain
- ○ Automotive, including suppliers, manufacturing, retail, service and maintenance and related after-market services
- ○ Household appliances, "smart living", including suppliers, manufacturing, retail, service and maintenance and related after-market services

- ○ Machinery
- ○ Other manufacturing, including suppliers, manufacturing, retail, service and maintenance and related after-market services
- ○ Raw materials and energy-intensive industries
- ○ Construction
- ○ Passenger transportation (taxi, bus, train, plane, waterways)
- ○ Logistics
- ○ Postal services, including express services
- ○ Telecommunications, including suppliers
- ○ Retail and wholesale
- ◉ Media, publishing, broadcasting and related services including advertising
- ○ Creative and culture industries
- ○ Health
- ○ Proximity, social services and social economy
- ○ Finance, insurance and re-insurance (other than motor insurance)
- ○ Legal advice; market research
- ○ Production and/or transmission/supply of electricity, gas, water, steam and air, including related data services
- ○ IT
- ○ Space and defense
- ○ Textile
- ○ Tourism
- ○ Other

Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

93288301615-56

* Country of origin

Please add your country of origin, or that of your organisation.

- ○ Afghanistan
- ○ Åland Islands
- ○ Djibouti
- ○ Dominica
- ○ Libya
- ○ Liechtenstein
- ○ Saint Martin
- ○ Saint Pierre and Miquelon

- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar/Burma
- Namibia
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden

- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States

- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **Fo r the purpose of transparency, the type of respondent (for example, 'business association, 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* Contribution publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

Anonymous

Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

Public

Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

☑ I agree with the personal data protection provisions

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

Access to private sector data can provide public authorities in the EU with valuable insights, for example to improve public transport, make cities greener, tackle epidemics and develop more evidence-based policies. To facilitate such data sharing, the European strategy for data announced that one of the objectives of the Data Act would be to create a framework to bring certainty to business-to-government (B2G) data sharing for the public interest and help overcome the related barriers.

In this context, 'public interest' is understood as general benefits to society as a whole – like effective responses to disasters or crises and improvements to public services – as recognised in law, at EU or Member State level. Some key examples are provided in the question "*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?*"

This framework could set the objectives, general obligations and safeguards that should be put in place for B2G data sharing.

An Expert Group on B2G data sharing, whose report was published in February 2020, issued a number of recommendations in order to ensure scalable, responsible and sustainable B2G data sharing for the public interest. In addition to the recommendation to the Commission to explore a legal framework in this area, it presented several ways to encourage private companies to share their data. These include both monetary and non-monetary incentives, for example tax incentives, investment of public funds to support the development of trusted technical tools and recognition schemes for data sharing.

In this section, we would like to hear your views on how the Commission should foster B2G data sharing for public interest purposes.

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

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

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						
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						
Commercial disincentives or lack of incentives/ interest/ willingness						
Lack of skilled professionals (public and/ or private sector)						

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)	○	○	○	○	○	○
Lack of safeguards ensuring that the data will be used only for the public interest purpose for which it was requested	○	○	○	○	○	○
Lack of appropriate infrastructures and cost of providing or processing such data (e. g. interoperability issues)	○	○	○	○	○	○
Lack of awareness (benefits, datasets available)	○	○	○	○	○	○
Insufficient quality of public authorities' privacy and data protection tools	○	○	○	○	○	○
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	○	○	○
Data (e.g. price data from supermarkets) for official statistics	○	○	○
Data (e.g. emissions data from manufacturing plants) for protecting the environment	○	○	○
Data (e.g. fuel consumption data from transport operators) for a healthier society	○	○	○
Data for better public education services	○	○	○

Data (e.g. employment data from companies) for a socially inclusive society			
Data for evidence-based public service delivery and policy-making			
Other			

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

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

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

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

II. Business-to-business data sharing

In this section, we would like to hear your views on fair contractual terms and conditions as an important tool that can stimulate companies to exchange their data while safeguarding the freedom of contracts and in full compliance with applicable legislation (such as the GDPR or competition law). The Data Strategy intends to promote business-to-business (B2B) data sharing which will benefit in particular start-ups and SMEs, putting emphasis on facilitating B2B voluntary data sharing based on contracts. We are seeking options for promoting fairness in contracts governing access to and use of data.

Model contract terms would provide businesses willing to share data, but lacking the experience, in particular SMEs and start-ups, with practical guidance on how to set up the contract based on fair terms. The use of such model contract terms would be voluntary for the parties.

A legislative fairness test for all B2B data sharing contracts would create general boundaries with the purpose to prevent the application of abusive contract clauses imposed by the party with the stronger bargaining power on the weaker party. The fairness test would only address excessive clauses while all other terms would be left to the parties’ contractual freedom. A contracting party would not be bound by an unfair contract term. Precedents for a B2B fairness test in EU law can be found in Directives 2011/7/EU (Late Payments) and Directive (EU) 2019/633 (Unfair trading practices in the food supply chain).

If sectoral rules were to establish a data access right, horizontal access modalities would regulate in a harmonized way how data access rights should be exercised while the possible creation of sectoral data access rights would be left to future sectoral legislation, where justified. The contract which the parties would agree for such data access could be based on variations of fair, reasonable, proportionate, transparent and non-discriminatory terms taking into account possible specificities of the relevant sectoral legislation. Whenever personal data are concerned, processing of such data shall comply with the GDPR. The data concerned would not include commercially sensitive data that could facilitate collusive outcomes on the market, nor data that is very strategic for competition, including trade secrets, nor legally protected data, for instance those covered by intellectual property rights.

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

Are you:

- ( ) Data holder

- ○ Data user
- ◉ Both data holder and user
- ○ Other

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

200 character(s) maximum

PSM receive data from their service providers (e.g. audience measurement), their subscribers (e.g. subscription to newsletters) and provide data (processors, advertising partners, etc.)

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

- ○ Voluntary
- ○ Mandatory
- ◉ Both voluntary and mandatory
- ○ I don’t know / No opinion

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

Please specify

200 character(s) maximum

The data is used by some public service medias (PSM) to know their audiences, to offer them personalized services (content and / or advertising).

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

The knowledge of audiences and the personalisation of online services may be based on declarative (socio-demographic) and / or navigation data.

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

300 character(s) maximum

These two purposes (knowledge of the public, personalisation of services) are essential to certain PSM for the fulfillment of their public service remit: to enhance and improve the offer of services in an environment which increasingly relies on personalisation.

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

- (●) Yes
- ( ) No
- ( ) I don’t know / no opinion

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

- ( ) Very often
- (●) Often
- ( ) Sometimes
- ( ) Rarely
- ( ) I don’t know / no opinion

What was the nature of such difficulties/issues?

- [ ] The data holder refused to give data on the basis of competition law concerns
- [x] The data holder refused to give access to data for reasons other than competition law concerns
- [ ] The data holder is prevented by law to give access to data
- [x] There is no legal basis for the data holder to give access to data
- [ ] The data holder gave access to data at unreasonable conditions, e.g. unilateral change of contractual terms, disproportionate restriction of use of data, limitations in the termination of contract
- [x] The data holder gave access to data at an unreasonable price
- [x]

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

Please indicate the type of difficulties / issues

200 character(s) maximum

Some media service distributors (IPTV, OTT, e.g.) refuse to provide even anonymous audience data, thus distorting media audience results.

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

- (•) Yes
- ( ) No
- ( ) I don't know / no opinion

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

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

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

300 character(s) maximum

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

III. Tools for data sharing: smart contracts

This section seeks to get your views on smart contracts. Smart contracts are computer programs, which automatically execute data and/or value transfers according to certain predetermined parameters. Smart contracts have important potential in manufacturing 4.0, smart mobility, and smart energy. Smart contracts can play an important role here by automating data transfers and data pooling, by triggering payments for data transfers and for guaranteeing the implementation of conditions linked to a data transfer. The following questions aim to (1) solicit your experiences with smart contracts and relevant uses cases, and (2) get your views on the need of harmonized standards for smart contracts in order to ensure interoperability and what the essential elements of such standards should be.

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

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

Please explain your answer

200 character(s) maximum

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

Please explain your answer

200 character(s) maximum

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										
Lack of interoperability										
Difficulties with governance										
Data protection issues										
Competition law compliance concerns										
Others										

If interoperability is an issue for scaling smart contracts, which requirements should inform standardisation to scale smart contracts across blockchains and/or across

ecosystems? Should such standards determine in particular minimum safeguards for cyber security? If so, which best practices would you consider relevant?

300 character(s) maximum

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

In this section, we would like to hear your views on non-personal data that is generated by smart objects connected to the Internet-of-Things ('IoT objects') in professional use. Examples of such objects include industrial robots, machine tools with sensors, construction engines or smart farming equipment.

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

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

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

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

V. Improving portability for business users of cloud services

In this section we would like to hear your views on cloud service portability. In order to prevent vendor lock-in, it is necessary that business users can easily switch cloud providers, by porting their digital assets in the broadest sense, including data and applications, from one cloud provider to another provider or back to their own infrastructure and software on-premise IT systems, including those digital assets stored at the edge of the network.

Cloud service providers and cloud users have jointly developed self-regulatory (‘SWIPO’) codes of conduct to address this issue in IaaS- and SaaS-specific contexts (IaaS i.e. Infrastructure as a Service; SaaS, i.e. Software as a Service), as mandated by Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union.

As part of the Commission’s evaluation of the development and implementation of the codes of conduct, the Commission will evaluate whether self-regulation in the field of business-to-business (B2B) data portability achieved the desired outcomes or whether other policy options should be considered.

The outcome of the recent public consultation on European Strategy for Data showed that 22.6% of the total respondents are of the opinion that the self-regulation is not the appropriate best practice in area of data portability. On the contrary, 30.8% agreed it is appropriate practice. The remaining (46.6%) of respondents did not express their opinion on the topic. However, 48% of the respondents answered that they have experienced problems in the functioning of the cloud market, the most common problem experienced being vendor lock-in.

Considering the above, the following questions aim to receive additional input on the topic of B2B data portability.

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

- (•) Yes
- ( ) No
- ( ) I don’t know /no opinion

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

Self-regulatory codes of conduct (SWIPO) have not achieved their objectives, according to several user organizations (CIGREF, BELTUG, VOICE, etc.) due to the structural imbalance of resources between users and digital service providers. Self-regulation has not been effective in mitigating providers’ unfair practices that reduce data and user mobility. A European framework with clear prohibitions would be essential to foster competitiveness and innovation in Europe.

Three main limitations to SWIPO codes lead to support a stricter regulation : (1) the low number of providers who have adhered to the codes, making them inoperative and unenforceable for users ; (2) the lack of integration of fundamental recommendations for users ; (3) the excessive complexity of governance, making it difficult to evolve in the future.

Moreover, SWIPO codes of conduct are merely "high level" provisions that are discussed pre-contractually and which do not become part of the contract. This means that there are no consequences in case of non-compliance. In addition, SWIPO codes of conduct only cover IaaS and SaaS; PaaS (i.e. Platform as a Service) is missing.

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.

200 character(s) maximum

Please see the annex.

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

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

We invite you to See the position paper published by the Belgium (Beltug), French (CIGREF), German (VOICE) and Dutch (CIO Platform) business users associations on the SWIPO SaaS code of conduct (CoC).

Common rules are necessary and should bind all cloud services offered in Europe, however the self-regulatory approach and the SWIPO codes of conduct have demonstrated their limits.

The current version of the SaaS CoC handles the technical aspects of porting rather adequately. However, the adherence of a supplier to the SaaS CoC does not guarantee that the customer will be able to perform the porting process if and when needed for its business. Thus, the SaaS CoC does not ensure data export for interoperability, nor porting at all times ; it does not ensure data export in case of organisational change ; it does not mitigate certain operational risks relevant to all customers ; it does not push adherents to moderate charges for data export, nor does it condemn the creation of vendor lock-in as a non-acceptable business practice ; it does not protect the customers against adverse unilateral changes in contract terms ; it does not facilitate customers' comparison of Transparency Statements issued by different providers.

Much stronger vendor lock-in occurs with PaaS and FaaS.

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?

200 character(s) maximum

See annex

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

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

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

It is important that any standardisation process includes all interested parties.
Cigref drafted a “Trusted Cloud reference document”, elaborated with its user members, which could be a first contribution for a European standardisation. This is also the work initiated within the project Gaia-X.

VI. Complementing the portability right under Article 20 GDPR

In this section we would like to hear your views on the portability of personal data. Under Article 20 of the GDPR, individuals can decide to port certain personal data to an organisation or service of their choice. Non-discriminatory access to smart metering data is mandated by Article 23 Directive (EU) 2019/944 on common rules for the internal market for electricity. Additional rules are proposed for facilitating the portability of personal data generated in the context of an online service offered by a “gatekeeper platform” under Article 6(1)(h) of the proposal for a Digital Markets Act (COM(2020) 842 final).
Smart connected objects connected to the Internet-of-Things (IoT objects) and services available on them, e.g. smart home appliances or wearables, generate a growing amount of data. Normally, the data generated by such objects and by the services available on them in their interaction with their human users are personal data. Such data is covered by the General Data Protection Regulation (GDPR). Any data

stored in terminal equipment, such as connected objects, can only be accessed in accordance with Article 5 (3) of Directive 2002/58/EC (ePrivacy Directive). However, the obligations under Article 20 GDPR does not require the controller to put in place the technical infrastructure to enable continuous or real-time portability.

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

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

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

VII. Intellectual Property Rights – Protection of Databases

The Directive 96/9/EC on the legal protection of databases (Database Directive) provides for two types of protection for databases. Firstly, databases can be protected, when original, under copyright law. Copyright protection applies to databases (collections of data) that are creative/original in the selection and/or arrangement of the contents and constitute their authors’ own intellectual creation.

Secondly, databases for which a substantial investment has been made into the obtaining, presentation and verification of the data can benefit from the protection under the so-called “sui generis” right. Such protection is automatically granted to the maker of any database which fulfils these conditions. The maker of databases protected under the sui generis right can prevent the extraction or re-use of their database content. The Directive lays down two main mechanisms to manage rights of users: the exception regimes (including the provision of specific exceptions in the fields of teaching, scientific research, public security or for private purposes) and the rights of lawful users.

To sum up, the copyright protection of databases only arises where the structure of the database, including the selection and arrangement of the database’s contents, constitute the author's own intellectual creation. The sui generis right protects, as an intangible asset, the results of the financial and/or professional investment carried out towards the methodical and systematic classification of independent data.

The Commission published a report evaluating the Database Directive in 2018. The evaluation highlighted that important questions arose as regards the interaction of the Directive with the current data economy, notably in view of the potential legal uncertainties as to the possible application of the sui generis right to machine generated data. The evaluation concluded that the Directive could be revisited to facilitate data access and use in the broad context of the data economy and in coordination with the implementation of a broader data strategy.

The following consultation is focusing on the aspect of the application of the Database Directive within the Data Economy, while also asking questions of a more general nature on this instrument.

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 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

“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

Questions on the Database Directive

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

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

Please explain and substantiate your answers with concrete examples and any useful information and experience you may have.

200 character(s) maximum

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

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

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

What was the source of such difficulties?

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

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

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

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

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

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

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

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

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

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

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

Questions about trade secrets protection

As indicated in the intellectual property action plan (COM(2020) 760 final), fostering data sharing requires a secure environment where businesses can keep investing in data generation and collection, while sharing

them in a secure way, in particular as regards their confidential business information and their trade secrets.

At EU level, the legal protection of trade secrets is harmonised by the Trade Secret Directive (Directive 2016/943), which has been transposed in all Member States and is not up for evaluation before 2026. It includes the definition of a trade secret, which means information meeting all of the following requirements:

- it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- it has commercial value because it is secret;
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

The Directive defines cases of lawful and unlawful acquisition, use and disclosure of trade secrets. The Directive also specifies the measures, procedures and remedies in case of unlawful acquisition, use or disclosure of a trade secret. Exceptions to trade secret protection as well as the freedom to reverse engineer are also included in the directive.

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 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

VIII. Safeguards for non-personal data in international contexts

Non-personal data generated by EU companies may be subject to access requests pursuant to provisions of laws of third (non-EU/EEA) countries. This would be specifically relevant when processing of such data occurs in a cloud computing service, the provider of which is subject to the laws of third countries. The recent proposal for a Data Governance Act does not cover such services. The access requests can be of a

legitimate nature, in particular for certain cross-border criminal law investigations or in the context of administrative procedures. In particular, these requests may be made in the framework of multilateral or bilateral agreements that determine certain conditions and safeguards. Whereas the GDPR provides for rules and safeguards in this respect, for non-personal data there are currently no statutory law rules that would oblige the cloud computing service providers to give precedence to EU law on the protection of IP and trade secrets. There can be differences in approach between the EU and third countries, e.g. to the fundamental rights safeguards or on the scope of legislation that can mandate access requests to data for law enforcement and other legitimate purposes. Where conflicts of law occur, this may expose the cloud providers to conflicting legal obligations and as a result of this conflict put commercially sensitive data of EU companies at risk.

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

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

Access to data containing confidential journalistic information, confidential internal company data, personal data.

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

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

These risks can restrict the possibilities of using cloud services and require additional organisational or technical measures to limit them.

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

Some EBU Members support that part of their data (personal and non personal data) should be stored in the EU/EEA only. Please see the annex for more information.

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?

- [x] 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
- [x]

- [ ] 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
- [x] 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

Closing section (possibility to upload a document, and to share final comments)

Please upload your file

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

a034b3e1-da38-41eb-915b-255493aa1a0e/Public_consultation_Data_Act_-_Annex_EBU_answer.pdf

Final comments

1. As a general remark, public service media organisations would like to emphasize that they abide by high ethical and regulatory standards in terms of data protection. In that regard, the future Data Act should carefully assess the cost and benefits of introducing additional rules to an already dense legislative framework (e.g. GDPR). In that view, we would kindly suggest to first focus on a better enforcement of existing rules before introducing additional obligations which could prove burdensome for European companies.

2. More specifically, as regards B2B data sharing in Section 2, public service media organisations have explained on several occasions the difficulties they encounter in accessing data (e.g. large platforms' to share the vast amounts of data they have accumulated) and would be keen for any data sharing rules included in the Data Act to go beyond the Digital Markets Act (DMA). Indeed, the DMA targets a specific set of companies that offer 'core platform services'. Nevertheless, many other entities (e.g. ISPs), which do not

offer ‘core platform services’, control data that PSM would need to access in order to fulfil their remit. As a result, though PSM welcome the ‘data sharing’ obligations that will be imposed on gatekeeper platforms by the DMA, that instrument will need to be complemented with rules that facilitate the fair and free flow of data between businesses.

In order to combine the above point with the objective of Section 2 which establishes‘ fairness’ in B2B data sharing, we propose to adopt a few general principles (based on the lessons learnt from competition enforcement and regulation) imposing access on FRAND terms. Three issues are particularly important here:

- The scope of data (e.g. raw v processed): along the lines of the DMA proposal, the data needs to be effective and high-quality in order to enable those companies that need access to it to improve user experience.
- The pricing mechanism on the basis of which data would be shared: the Commission would need to establish certain principles that ensure that the provider granting access to data does not charge excessive prices. It is reminded that, in cases where the Commission left it to the dominant or merging firms to set up the pricing mechanism they deemed fit to share a valuable input with competitors (e.g. IP, know-how), the prices charged were unsustainable on many occasions. It is also reminded that, in its Communication on data sharing in the private sector, the Commission referred to the principle of ‘shared value creation’. This means essentially that the company controlling the data benefits from the fact that other businesses use its services because it can thereby accumulate more data. This principle needs to be reflected in the mechanism that will determine the price to be paid.
- Effective enforcement: As the DMA proposal acknowledges, data often needs to be ‘real-time’. In other words, it is highly perishable. For this reason, there needs to be an effective enforcement mechanism that can lead to a speedy resolution of any disputes that may arise in the future.

Contact

Contact Form

EBU

OPERATING EUROVISION AND EURORADIO

EBU answer to the public consultation on a Data Act - Annex

Some of the space provided in the online survey was not sufficient to provide a full answer. Please find below additional comments on the related questions.

Section V: Improving portability for business users of cloud services

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

Yes

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

To avoid vendors' lock-in, business users need to be able to easily switch cloud providers with their data and applications, without extra costs or time limitations. This right should ensure sovereignty over one's own data. Customers incur prohibitive financial, organisational and technical costs in transferring to alternative cloud suppliers. A lack of assistance and differing technical requirement hinder portability.

Both legislative approaches proposed are required and are complementary: generic provisions guaranteeing the principle of interoperability complemented by specific measures to make this principle effective i.e. contractual provisions (such as the prohibition of charging for indirect access) and technical provisions (API, open standards).

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

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

Please refer to the Cigref Trusted Cloud reference document – section 7: "reversibility requirements" & section 8: "interoperability requirements".

However, it is unclear how something like this could look. For IaaS, standard formats already exist; for SaaS, it is not very realistic to get more than rudimentary interoperable formats.

EUROPEAN BROADCASTING UNION
L'Ancienne-Route 17A
1218 Le Grand-Saconnex
Geneva, Switzerland
Tel. +41(0)22 717 25 05
www.ebu.ch
EBUID-834011548-5525

Section VIII: Safeguards for non-personal data in international contexts

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

Some EBU Members support that part of their data (personal and non personal data) should be stored in the EU/EEA only. Relevant factors are:

- Type of non-personal data being processed, e.g. commercially sensitive data; highly confidential data; business critical internal data.
- How data is processed, e.g. by a third-party cloud service provider.
- The territory where the data is processed and the applicable laws in that territory, e.g. laws that require the cloud service provider to allow a law enforcement agency to access the data.