Computer & Communications Industry Association
Tech Advocacy Since 1972

Computer & Communications Industry Association (CCIA Europe) Supplementary Comments to European Commission on Consultation on the Data Act

2 September 2021

1. Section 1 – Business to Government data sharing for the public interest

> *Question 2: Should the EU take additional action so that public sector bodies can access and re-use private sector data, when this data is needed for them to carry out their tasks in the public interest purpose?*

In many cases, **public sector bodies can carry out their tasks in the public interest without relying on data from businesses** (be it mobility, health, urban planning). While access to business data may be *convenient* for public bodies, business data may not be *necessary* for public sector bodies to carry out their tasks. Where the inaccessibility of business data would prevent public bodies from conducting their duties, we would expect existing sectoral legislation to require businesses to provide national and local authorities with data that is strictly to pursue their mandate.

CCIA Europe **strongly cautions against any form of general mandatory B2G data-sharing**. Instead, we encourage the European Commission to **continue enabling sector-specific practices to evolve within regulated sectors.**

First, businesses' data needs can vary very wildly across sectors. Creating a one-size-fits-all approach would not achieve the policy objectives sought by the Data Act if it does not take into account sector-specific practices.

Second, we are **concerned that a one-size-fits-all mandatory public data sharing could give away valuable intellectual property** - not only the workings of the technology but the processes that underpin them. Preserving confidentiality of intellectual property will depend on utilising well-understood and established sector-specific practices (e.g., for type approval, market surveillance) for protecting IP from being shared not only with industry competitors, but also from falling into the hands of adversarial nation-states.

More generally, it is **essential to ensure that any mandatory data sharing practices are balanced against public expectations of privacy**, and data shared with the public sector is narrowly tailored for specific purposes rather than extending to overreaching surveillance, and that the mandates do not force companies to increase data collection for purposes that are not needed by business.

This being said, CCIA Europe believes that the Data Act is an opportunity to **lay down the foundations for voluntary sector-specific initiatives** which can help **accelerate the adoption of B2G data-sharing arrangements** in Europe while **providing legal certainty to businesses**. In practice, in some sectors such as mobility, local governments' data access requests to Mobility-as-a-Service (MaaS) providers can raise significant challenges in terms of business confidentiality and GDPR compliance, especially when the failure to supply such information

may prevent business operations within the jurisdiction of the requesting local authority. CCIA Europe is encouraged to see local authorities across the EU and MaaS providers increasingly working together to negotiate B2G data-sharing governance agreements. But while we welcome an open dialogue between private and public stakeholders, it remains time-consuming for all parties involved, and requires detailed knowledge about the parties' respective rights and obligations.

CCIA Europe therefore invites the European Commission to set out a **high level framework setting out the general conditions and safeguards (personal data protection, IP rights) for voluntary B2G data sharing arrangements**. Governments and/or the European Commission together with relevant industry representatives can then build upon that framework for voluntary sector specific initiatives (e.g., Codes of Conduct). The European Commission may also wish to formulate **guidelines on applicable laws in specific use-cases** for narrowly defined public interest purposes that would assist national and local governments and businesses, and considerably accelerate the roll-out of B2G data-sharing initiatives across the EU.

2. Section 2 - Business to Business data sharing

> *Question 5: 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)?*

The assumption that the application of a fairness test or a list of unfair contractual terms would necessarily increase data sharing between businesses seems speculative. We see **little to no causation between the mere invalidation of one or more clauses in a contract and the increase of data sharing among parties.** In some cases, it may in fact achieve the opposite and incentivise data holders to collect less data resulting in less data for secondary access and use.

A fairness test or a list of unfair contractual terms specifically focused on secondary data access and use could also raise **practical and enforcement challenges**. This may be the case for instance where parties' data access is a mere ancillary feature of a broader contract for the provision of a given service e.g. license to use an IoT service. In those cases, a *fair* enforcement of the fairness test (or list of unfair clauses) would require a case-by-case assessment, with due regard to the object of the contract and the conditions laid down for each party.

More generally, the introduction of a fairness test should be **limited to data that is indispensable** to enter or compete on the market, and where **competition law enforcement cannot address the issue**. Unilateral imposition of contractual terms is common practice and, unlike what the explanatory statement seems to suggest, the mere fact that a data holder has a "stronger bargaining power" should not trigger any form of B2B data-sharing obligation.

Finally, the enforcement of a fairness test would have to take into account statutory limitations, including the upcoming e-Privacy Regulation for co-generated non-personal IoT data in professional use for instance.

> *Question 6: 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)?*

CCIA encourages the European Commission to **set up voluntary standard contractual terms which can provide legal certainty and can be easily implementable for businesses** engaged, or planning to engage, in data-sharing with private parties. We are convinced that model

contracts, alongside guidance on rules that are relevant to B2B data-sharing practices, would greatly facilitate commercial data-sharing agreements in Europe.

To ensure the success of voluntary model contracts, contractual terms should **reflect applicable EU rules** that are relevant for B2B data-sharing purposes, e.g. rules on data protection and privacy in electronic communications, database rights, data localisation prohibition. Parties should also be able to **modulate standard contractual terms according to their needs**.

Model contract terms should be **developed in close cooperation with companies and stakeholders** to ensure that their needs are taken on board, and to learn from and build on their experiences.

> *Question 7: 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)?*

CCIA Europe believes it is important to **preserve as wide a range of B2B data-sharing governance models as possible.** We caution against the temptation to favour one specific model, such as FRAND licensing, over other models. A generalisation of FRAND terms for B2B data sharing may be counterproductive to the extent that other data-sharing governance provides more generous conditions to data users. For instance, open data schemes typically entail free-of-charge access and with little to no restrictions of use. The very notion of FRAND terms denote a licensing commitment that would imply that data holders would, by default, enjoy an intellectual property right over the data they hold. CCIA Europe would caution against inadvertently creating new rules where all data held by the private sector is universally treated as an intellectual property, and where any innovation and research driven by text and data mining would require a licensing agreement.

Furthermore, recent debates over FRAND terms for standard essential patents reveal that **there is little agreement on how to set FRAND rates in practice**, even where technologies are already being licensed for consideration, have clear use cases, and foreseeable valuations. Mandating FRAND licensing in relation to data which has not been previously commercialised, and which has unquantifiable future value, could have significant unintended consequences on private economic incentives in Europe's data economy.

3. Section 5 - Cloud interoperability and data portability for business users

> *Question 1(a): 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?*
>
> *Question 1(b): In your opinion, could the SWIPO codes of conduct represent a suitable approach to address cloud service portability, if:*
> *Option 1: The principles formulated in the self-regulatory SWIPO codes of conduct would be binding for all cloud services offered in Europe*
> *Option 2: The codes of conduct would be supplemented by Standard Contractual Clauses translating the Codes' requirement into contractual elements*
> *Option 3: Both*
>
> *Question 6: Would it be necessary in your opinion to develop Standard Contractual Clauses for cloud service portability to improve negotiating position of the cloud users?*

CCIA Europe has long supported the SWIPO Codes of Conduct for cloud infrastructure and software switching. These Codes of Conduct are the results of an inclusive consensus-building process involving cloud users, including SMEs, and cloud providers. We think the impact of the codes can be improved with better communication and advocacy towards the market by all players involved, including the European Commission. The upcoming EU cloud rulebooks seems particularly apt to achieve that objective.

However, CCIA Europe believes it is **premature to either mandate the SWIPO Codes of Conduct via Standard Contractual Clauses or introduce new legal requirements on cloud service interoperability**. The Codes of Conduct are only a few months old, and companies have only just started to declare their services SWIPO compliant. We therefore invite the European Commission to wait until its review of the Codes November 2022 to assess whether the Codes have had any impact on the market. Furthermore, the Codes of Conduct are meant to be living documents and codifying the Codes into mandatory model clauses would need to be regularly updated to reflect any future changes as technology progresses.

More generally, CCIA Europe **cautions against equating a new data portability right to individuals' portability right under the GDPR**. Transferring live applications and the associated interfaces and data is significantly more challenging than simply transferring personal data.

First, the volume and complexity of data are enormous in comparison to the personal data about a single individual that an organization may hold. Second, specialist technical assistance (which incurs costs on both sides) will always be required given the level of business risk and potential interruption – even in a hypothetical scenario where there was full portability between cloud service providers, these costs and this risk would not be removed.

Finally, customers have freely chosen (and invested in) their cloud environment and will have developed their application suite with this in mind. Switching will likely involve technical modifications such as reformatting data, reconfiguration and potentially new interface requirements.

4. Section 7 - Intellectual Property Rights - Protection of Databases

> *Question 2: "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?*

CCIA Europe **cautions against creating additional exclusive, proprietary rights** to allow data holders to control third party's accessibility and use of their data. The scope of IPR protection and exceptions in the Database Directive (Directive 96/9/EC), the Trade Secrets Directive (2016/943), and the provisions on text and data mining in the Copyright Directive (Directive 2019/790) provide sufficient guarantees for IPR holders without unduly hindering data-driven innovation. Creating a specific access regime to facilitate access to databases or broadening the scope of the *sui generis* right to all data would risk upsetting the balance between legitimate intellectual property rights protection and data-driven innovation.

Instead, contractual and technical limitations should suffice to ensure data holders' control over data access and use outside the purview of EU legislation.

Question 4: In your view, how does the Database Directive apply to machine generated data (in particular data generated by sensor-equipped objects connected to Internet-of-things objects)?

Question 10: 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?

Question 11: In your opinion, how should the new scope of the sui generis right be defined?

The CJEU rightfully ruled that the Database Directive does not apply to newly generated (or created) data, and confined the sui *generis* right to the protection of investments made to produce databases, i.e. the act of *obtaining*, *verifying*, and/or *presenting* the data. By nature, raw data generated by machines is newly created data and is not obtained from existing data sources. There is therefore no need to clarify the scope of the sui generis right.

By way of principle, a thriving data-driven economy values, protects and promotes the insights (output) that generated data (input) may reveal, not the data itself, and it encourages responsible data access and further use among market participants. Extending the *sui generis* right to machine generated data would achieve the opposite of that.

Question 12: 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?

Question 13: In your opinion, how would specific access rules in the Database Directive be best achieved?

Preventing data access and extraction can be done through contractual and technical measures without introducing new rules in the Database Directive.

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

Question 1: How likely do you think it is that a cloud computing service or other data processing service provider that is processing data on your company's/organisation's behalf may be subject to an order or request based on foreign legislation for the mandatory transfers of your company/organisation data?

Question 2: 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?

CCIA Europe is not aware of democratic foreign third country government access orders seeking to obtain EU enterprises' confidential information (including trade secrets) or otherwise non-personal data.

CCIA Europe invites the European Commission to identify and assess any material evidence that would demonstrate the likelihood of foreign government access to companies' data. In doing so, we recommend the European Commission to consider assessing the relevance, in practice, of non-personal data for national security and law enforcement purposes in third countries, and engage with like-minded governments to support its fact-findings.

Question 3: 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?

Question 4: 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: (a) All of my company/organization data in the EU/EEA only, (b) Some of my company/organization data in the EU/EEA only; (c) All of my company/organization data anywhere in the world.

The premise of this question implies that businesses can reasonably identify third country government data access laws and practices, understand how said laws and practices apply to their hosting providers, and assess whether said law and practices meet EU standard of protection (and national security derogations thereof). Where it does not meet such EU standards, businesses and their vendors would need to consider mitigating measures.

It would be **unrealistic and highly disproportionate to expect businesses to conduct assessments that require in-depth knowledge of third country data access laws and practices** and routinely take years to complete in the context of European Commission data protection adequacy decisions for instance. Companies are not, and will never be, in a position to identify and assess which laws in the country(ies) of destination would fail to meet the EU's standard of protection (and national security derogations thereof).

More generally, the rationale for restrictions on sharing personal data relates to the concept that individuals should retain control over how their personal data is used since EU law does not view personal data as the property of the organization that collected it. For non-personal data, this rationale does not hold. Confidential information, intellectual property rights and other non-personal data are assets held and owned by the organization that created or collected them. Imposing restrictions on how those companies can use their data assets in-house or through a third party such as a cloud computing vendor is a 'one size fits all' approach that does not meet the needs of businesses and/or their vendors.

As cloud service providers generally take a hands-off approach to the content of the data stored on their systems, customers would be forced to undertake costly and burdensome data audits themselves to determine which of their data is caught by the restrictions on international transfers – which is likely to be a complex and resource-intensive process which would undermine the substantial benefits to customers of cloud adoption. Additionally, businesses are already free to choose cloud services that operate in a way which suits their needs – certain customers will prioritise low costs over EU-based storage locations, whereas large enterprises may prioritise storing the same data in several jurisdictions. Introducing restrictions on the transfer of non-personal data interferes with the rights of businesses to operate in the way that they see best.

Question 5: 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?
[Option 1] 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
[Option 2] 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*
> *[Option 3] 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*
> *[Option 4] Providing compatible rules at international level for such requests.*

Extraterritorial government and data access laws are a global phenomenon which require multilateral safeguards (Option 4). CCIA Europe encourages the European Commission to pursue dialogues with like-minded countries to draw up international frameworks based on mutual recognition. CCIA Europe also believes that customers have a right to know when their data has been subject to an access order from any jurisdiction whenever the applicable law permits (option 1), no matter how unlikely an access order may relate to a company's non-personal data.

However, **CCIA Europe strongly cautions against a notification and disclosure obligation applicable to companies that may be subject only to foreign extraterritorial government data laws.** While we understand the value of notification and disclosure requirements, we caution against any measures that may inadvertently name and shame non-EU service providers.

Should the European Commission choose to pursue a notification and disclosure regime, we recommend that all service providers operating in Europe should notify which government data access laws their operations may be subject to. This requirement should cover all government data access laws, including EU and national laws as well as foreign laws. As a transparency tool, CCIA Europe sees no reasons why the notification and subsequent disclosure obligation should not include processing subject to European national security and law enforcement laws. As the European Commission seeks to "ensure an open, but assertive approach towards international data flows, based on European values", the same values should be upheld within the Union. In this respect, we recall that the e-Privacy Directive protects the confidentiality of legal persons' communications, and in a landmark ruling from 6 October 2020, the EU Court of Justice clearly stated that EU's safeguards, including the protection and confidentiality of legal persons' electronic communications, extend to all national government data access laws which impose processing obligations on providers of electronic communications services. In any event, the notification and disclosure requirements should not be a name-and-shame exercise against non-EU vendors.

***

Please find below CCIA Europe's responses to the Data Act consultation survey.

For any questions, please contact Alexandre Roure, Senior Manager, Public Policy at aroure@ccianet.org.

Public consultation on the Data Act

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

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.

Question 1: 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

Question 2: Should the EU take additional action so that public sector bodies can access and re-use private sector data, when this data is needed for them to carry out their tasks in the public interest purpose?

☐ EU level action is needed

☐ Action at Member State level only is needed

☒ No action is needed

☐ I don't know / no opinion

Question 3: 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 / interests / 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	☐	☐	☐	☐	☐	☐

Question 4: 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	☐	☐	☐

Question 5: 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

Question 6: 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

200 character(s) maximum

☒ Limitations on onward transfer/sharing
☒ Privacy impact assessments
☒ Independent audits
☒ Liability waivers
☒ Prohibition from coercing businesses in sharing data, especially personal data

Question 7: Which of the following types of financial compensation would incentivise you to engage in a B2G data-sharing collaboration for the public interest (select all that apply):

☐ Marginal costs for dissemination

☐ Marginal costs for dissemination + fair return on investment (ROI)

☒ Market price

Question 8: 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.

Question 1: Does your company share data with other companies? (This includes providing data to other companies and accessing data from other companies)

☒ Yes

☐ No

☐ I don't know / no opinion

Question 1(a): Are you:

☐ Data holder

☐ Data user

☒ Both data holder and user

☐ Other

Question 1(b): In the last five years, how often has your company shared data with other companies?

☒ Many times

☐ Only a few times

☐ Don't know

Question 1(c): Please describe the type of data shared, and the type of businesses with whom it is shared

200 character(s) maximum

Type of data: raw data, structured data, inferred data.

Type of business: customers, commercial partners and affiliates, vendors.

Question 1(d): 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

Question 2: 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

E.g. Online platforms facilitating the sharing and creation of datasets between companies.

Question 3: What benefits from data sharing do you expect to be reaped in your sector?

300 character(s) maximum

Question 4: Has your company experienced difficulties/encountered issues when requesting access to other companies' data?

☐ Yes

☒ No

☐ I don’t know / no opinion

Question 5: 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

Question 6: 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

Question 7: 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

Question 8: 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

Please refer to our response in the enclosed supplementary comments.

Question 9: 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

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 lockin, 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.

Question 1: Was your organisation aware of the SWIPO Codes of Conduct prior to filling in this questionnaire?

☒ Yes

☐ No

☐ I don't know /no opinion

Question 1(a): 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

Please refer to our response in the enclosed supplementary comments.

Question 2: 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

200 character(s) maximum

Please refer to our response in the enclosed supplementary comments.

Question 3: 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

Question 4: 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

Question 5: 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

Question 6: 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

Question 7: 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

None of the policy options mentioned above would appear necessary until the European Commission can demonstrate that the SWIPO Codes of Conduct has had little to no effect on cloud providers' portability provision.

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.

Question 1: To what extent do you agree with the following statement: "Individual owners of a smart connected object (e.g. wearable or household appliance) should be able to permit whomever they choose to easily use the data generated by their use of that object."

☐ Strongly agree

☒ Somewhat agree

☐ Neutral

☐ Somewhat disagree

☐ Strongly disagree

☐ I don't know / no opinion

Question 2: To what extent do you agree with the following statement: "The device manufacturer of a smart connected object (e.g. wearable or household appliance) should be able to permit whomever they choose to easily use the data generated by the use of that object, without the agreement of the user."

☐ Strongly agree

☐ Somewhat agree

☐ Neutral

☒ Somewhat disagree

☐ Strongly disagree

☐ I don't know / no opinion

Question 3: 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

Please specify

200 character(s) maximum

Existing EDPB guidelines on data portability - see p. 5-8 of https://www.ccianet.org/wp-content/uploads/2020/06/FINAL-Supplementary-comments-CCIA-submission-on-EC-Data-Strategy-Consultation.pdf

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

Question 1: 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

Question 2: "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

Please refer to our response in the enclosed supplementary comments.

Questions on the Database Directive

Question 3: 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

CCIA is a trade association.

Question 4: 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

Consistent with the CJEU case-law, the sui generis right does not, and should not, apply to machine generated data. Please refer to our response in the enclosed supplementary comments.

Question 5: 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

Question 6: 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

Question 7: 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

Question 8: 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

Question 9: 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

Please refer to our response in the enclosed supplementary comments.

Question 10: 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

Please refer to our response in the enclosed supplementary comments.

Question 11: 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

Please refer to our response in the enclosed supplementary comments.

Question 12: 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

Question 13: 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

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

Preventing data access and extraction can be done through contractual and technical measures without introducing new rules in the Database Directive.

Question 14: 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

Question 15: 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

Please refer to our response in the enclosed supplementary comments.

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.

Question 1: Do you rely on the legal protection of trade secrets when sharing data with other businesses?

☒ Yes

☐ No

☐ I don't know / no opinion

Question 2: With whom do you share?

☒ Partner

☒ Supplier

☒ Customer

☐ Unrelated business

☐ Other

Question 3: 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

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.

Question 1: How likely do you think it is that a cloud computing service or other data processing service provider that is processing data on your company's/organisation's behalf may be subject to an order or request based on foreign legislation for the mandatory transfers of your company/organisation data ?

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

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

Please refer to our response in the enclosed supplementary comments.

Question 2: 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

Question 3: 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

Please refer to our response in the enclosed supplementary comments.

Question 4: 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

Please refer to our response in the enclosed supplementary comments.

Question 5: 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

Please refer to our response in the enclosed supplementary comments

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

Final comments

2021.09.02 - CCIA supplementary comments on EC Data Act consultation