EU Data Act adoption

Ibec response to DETE consultation on proposed Data Act adoption

May 13, 2022

Contents

1. INTRODUCTION 3

2. GENERAL RECOMMENDATIONS AND COMMENTS 4

3. RECOMMENDATIONS AND COMMENTS ON SPECIFIC PROPOSALS 5

CHAPTER I GENERAL PROVISIONS 5

CHAPTER II BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING and CHAPTER III OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE 6

CHAPTER IV UNFAIR TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES 8

CHAPTER V MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES AND UNION INSTITUTIONS, AGENCIES OR BODIES BASED ON EXCEPTIONAL NEED 8

CHAPTER VI SWITCHING BETWEEN DATA PROCESSING SERVICES 9

CHAPTER VII INTERNATIONAL CONTEXTS NON-PERSONAL DATA SAFEGUARDS 10

CHAPTER VIII INTEROPERABILITY 10

CHAPTER IX IMPLEMENTATION AND ENFORCEMENT 11

CHAPTER X SUI GENERIS RIGHT UNDER DIRECTIVE 1996/9/EC 11

CHAPTER XI FINAL PROVISIONS 11

1. INTRODUCTION

Ibec welcomes the opportunity to comment on the efforts to develop a European Data Act. We support the European Commission's ambition to build a European Single Market for Data, recognising that data is at the heart of Europe's competitive future and digital leadership.

As part of Ibec's new campaign, 'Stronger Europe, Stronger Ireland', this paper:

- Complements and builds on preliminary Ibec priorities for the European Commission's Data Strategy and its related legislative proposals[1];
- Offers further recommendations to EU co-legislators in finalising the European Data Act; and
- Responds to the DETE public consultation on the adoption of a European Data Act.

[1] See Ibec views on Data Governance Act and Data Act

2. GENERAL RECOMMENDATIONS AND COMMENTS

1. **Support further excellence in data innovation to complement enhanced trust in data access**. Ibec support responsible data sharing, enhanced portability and switching that benefits our economy and society. The EU must support further investment in capacities and skills in trusted data innovation too. Enabling further access to data, in isolation, may not automatically equate to capacities to gain beneficial insights out of that data.
2. **Ensure robust safeguards** protect intellectual property rights and the confidentiality and security of data. Incentivise further investment and preserve rights.
3. **Ensure the Data Act aligns with existing or draft EU laws.** Support further trust and investment.

3. RECOMMENDATIONS AND COMMENTS ON SPECIFIC PROPOSALS

CHAPTER I GENERAL PROVISIONS[2]

4. **Separate business-to-business (B2B) and business-to-consumer (B2C) data access and sharing provisions into distinct chapters.** Provide for more tailored policy action and greater clarity. B2B and B2C are two different setups of business activity. Industrial Internet of Things (IoT) and consumer IoT require different safeguards as the amount and the nature of data generated are different.
5. **Clarify how data recipients are envisaged to know which users they should reach out to, and how to contact these users**. This is important when users are consumers because their contact details will be rightfully protected by the GDPR.
6. **Refine the definition of data**. The proposed definition appears broad and could cause uncertainty. For example, data handling can include mixes of personal/non-personal or raw/inferred data. In other situations, data plays an internal role in the device; or have been previously encrypted.
    a. Data access/sharing should apply to data where the manufacturer or provider of a related service has some ability to get access or identify the data. Equally, data which is the result of processing (either within the device or after collection) should not be in scope, as recitals 14 and 17 exclude from scope data which is the result of processes which may be subject to IPRs or which is derived from data representing user actions.
    b. Developing data access or data sharing tools should not require a complete re- engineering of an entire product. For example, including data in scope that was previously fully encrypted, only stored locally on a device and where there was no ability to link it to a particular user would appear disproportionate.
    c. Consider the data portability requirement in the Data Act through the lens of technical feasibility and what is the scope of data to be collected. In practice, many businesses do not have specific silos of data for a specific customer. Only when a data portability request is made, do companies start drawing data from different sets and creating dataset pertinent to the requesting customer.
    d. Avoid hampering the data minimisation principle of the GDPR in making data available under the Data Act.
    e. Clarify if *data* and *information* should be considered synonymous or not in relation to trade secrets, see point 13 below.
7. **Clarify the definition of data holder**. In Article 2(6), a data holder for non-personal data is understood as any entity that has the technical ability to make data available, recital 24 equates data holders processing

[2] Concerns the subject matter, scope definitions used throughout the instrument.

personal data to data controllers. There is no explanation of why there is such differentiation between the mechanisms applying to personal and non-personal data sharing. A clearly defined entity should be responsible to act as data holder.

8. **Define "competing product".** Clarify whether a "competing product" means products within the meaning of Article 2 para. 2, i.e., only physical and movable objects, or the understanding of the term via Article 2 para. 3 "related service", i.e., software and data-driven services. If the understanding is limited only to physical products, then the Data Act poses a risk that software providers or service providers could benefit indirectly by developing software-driven products or services based on the extracted data, which then compete directly with the original product or a service. Also, recognise that components of a product should be also protected by the non-compete clauses, and not only the product as a whole.
9. **Clarify responsibilities in the supply chain and who is best placed to provide the access to data in defining 'related service'**. It remains unclear which components (e.g., sensors) of a physical asset fall under the definition of a "product". The proposal is also referring to "consumers" but a definition in Article 2 appears missing. In addition, without a definition for "operator of a data space", Article 28 cannot be enforced, and data spaces should be limited to the well-defined Common European Data Spaces. Recitals 14 to 17 seem to be intended to provide further clarity on what products are in scope and how data should be interpreted, but further clarification and even placing some of the definitions in Article 2 could ease the legal certainty of the proposed regulation.

CHAPTER II BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING[3] and CHAPTER III OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE[4]

11. **Ensure obligations for data holders are possible and technically feasible in Article 3.** Access may not always be feasible in the context of an IoT that lacks a direct user interface. Article 3(2)(a) requires data holders to provide information on the nature and volume of data likely to be generated. While data holders could have expectations of the nature of the data to be generated, the volume of data generation is highly subjective to the use of a product or service, therefore we suggest deleting the "volume" requirement from the paragraph. Furthermore, developing a data accessibility/sharing feature to a product could be less costly than redesigning the entire product.
12. **Ensure the overlapping interests of various parties are balanced in Article 4**. Considerations include enabling users to access data they have contributed to generating and enabling data holders to invest in solutions. Clarify that only data that users have contributed to generating should be accessible (ancillary data should be out of scope).

[3] Concerns rules for consumers and businesses to access data generated by the products or related services they own, rent or lease.
[4] Concerns general rules applicable to obligations to make data available.

13. **Preserve the confidentiality of trade secrets and confidential information**. The Data Act proposal should not lead to an obligation to share trade secrets. The Trade Secrets Directive refers to *information* that has commercial value because it is a secret. The data related to this *information* lacks sufficient protection in the proposal. The Trade Secrets Directive is better placed to clarify the conditions for lawful disclosure of trade secret information and data related to it as well as to provide adequate safeguards. Equally, the legitimate aims of the data holder extend well beyond trade secrets and should also cover commercial confidential information (as do the Open Data Directive and the Data Governance Act),
14. We support the prohibition for the third party to use the data to develop competing product, and the prohibition to share such data to (another) third party for that purpose as provided in Article 6(2)(e). Nevertheless, **co-legislators must ensure conditions for the effective control mechanisms at the disposal of the data holders to make sure these provisions are respected.** For instance, compensation for a data holder from the user or third parties if the data provided has been misused, for example, for the development of a competing product.
15. **Consider a reverse flow of data from service providers to product manufacturers**. Digital services are not just downstream services but are increasingly becoming the focus of the performance and value proposition in industrial applications. Support legally secure and operational specifications for data protection-compliant anonymization of personal data. Maintain high levels of data protection and harness the economic potential of anonymized data.
16. **Support the security of users' data and positive data sharing**. A data holder exercising the obligation to provide access to data upon request by the user shall not be expected to know in what kind of environment the third party will process the data. To strengthen the positive cooperation between data holders and data recipients, and avoid the risk of abuse, data recipients in Article 8(3) should question the conditions under which the data is made available, when they have "reasonable doubt" and not when they "consider" the conditions discriminatory.
17. **Support reasonable compensation and dispute resolution.**
    - **a.** Reasonable compensation should as a minimum cover the actual cost of making the data available, so that the incentives to develop products generating data remain. We generally support Article 9, except paragraph 3, which if not deleted, should detail under what conditions data holders can be obliged to share data with data recipients at a price lower than the actual cost or free of charge.
    - **b.** Refine the dispute settlement mechanism in Article 10. Paragraph 2 does not appear to include any provision on avoiding conflict of interest. Furthermore, paragraphs 5 and 9 should clarity if the parties can go directly to court or if they are obliged to go through a dispute settlement body as first step.

CHAPTER IV UNFAIR TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES[5]

18. **Provide further clarity regarding the conduct that is always unfair and presumed unfair** to ensure legal clarity.

CHAPTER V MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES AND UNION INSTITUTIONS, AGENCIES OR BODIES BASED ON EXCEPTIONAL NEED[6]

19. **Ensure consistency, particularly for requirements on interoperability, with existing EU laws that govern the government-to-business data sharing**, such as the Open Data Directive and the Data Governance Act.
20. **Provide clarity and safeguards on data access requests**. B2G sharing could enable innovative public private partnerships. However further clarity and safeguards would be welcome.
    a. **Focus the scope**: The scope of the proposed obligation to make data available when there is an "exceptional need" could be widely interpreted and public sector data access requests using this legal ground could become the norm rather than the exception.
        i. Requests under Article 14 should be specific, duly substantiated and time limited.
        ii. It is understood that data requested for an exceptional need to respond to a public emergency would be provided free of charge (Article 15 and 20). Requests for exceptional needs in non-emergency situations, which would be understood to be less serious and more frequent, should be subject to close scrutiny and to fair incentives.
        iii. Add an obligation for the public sector bodies, upon the request of the data holder, to demonstrate they have used all possible measures to obtain the data before using the mechanism of Article 15(c)(1). Indeed, aside from public emergencies (Art 15 a and b) it is unclear what other circumstances would merit bypassing legislative action to invoke access to data. Such a possibility could constitute a disincentive for public authorities to seek a legislative route to address future requests for data. As proposed, this provision is broad and further clarity would be welcome.
    b. **Preserve rights**: Article 17 is welcome, but Article 18 should recognise contractual obligations on Data Holders and provide further safeguards regarding privacy, security, intellectual property, and trade secret protections.

[5] Seeks to address potential unfairness of contractual terms in data sharing contracts between businesses.
[6] A harmonised framework for the use by public sector bodies and Union institutions, agencies and bodies of data held by enterprises in situations where there is an exceptional need for the data requested.

c. **Provide clarity** on how data holders can seek remedies in disputes over use of data by a public sector body. This is relevant if the data are further shared under the once-only-principle of e-Government or under Article 21, which must include at least a criterion for considering which actors fall within the definition of research institutions and how these should handle the data with appropriate safeguards and the obligation that those actors shall not use such data to derive insights about the economic situation, assets and production methods that could undermine the commercial position of the data holder or in a manner or for a purpose which is detrimental to the legitimate interests of the data holder. There is a need for clarification to ensure a uniform understanding of the large number of public bodies entitled to claim access throughout the EU.

CHAPTER VI SWITCHING BETWEEN DATA PROCESSING SERVICES[7]

21. **Support an inclusive and competitive cloud market** that empowers business users, and avoids vendor lock-in. We support the Commission ambition to make switching and interoperability easier. Avoid forced data localisation requirements.
22. **Provisions for switching and portability should reflect the type and scope of data involved**. The proposal suggests a mandatory transition period[8] (up to maximum of 6 months) for migrating workloads. This may be feasible for simple workloads from one provider to another. However more time should be considered for projects proven to be more complex. Cloud service providers may need more than 7 days to respond in detail as provided in Article 24(2), and contractual agreements with customers in this regard should be considered. Also, the proposal should exclude data processing services for which no other services of the same type exist, or that operate on a trial basis or just supply a testing and evaluation service for business product offerings. These kinds of data processing services should be out of scope because do not raise potential vendor lock-in problems.
23. **Further clarify** "**functional equivalence**" (Article 26) for the switching of data processing services and which provider carries the responsibility to ensure it. **Enable a reasonable level of co-operation between customers and their (incumbent and new) providers to make switching easier**.
    a. **Reflect customer needs**. Customers may decide to switch providers because they value other (new) functionalities more than the ones they get in their current contract, and therefore may not

[7] Proposes minimum regulatory requirements of contractual, commercial and technical nature, imposed on providers of cloud, edge and other data processing services, to enable switching between such services.
[8] Article 24

require the same functionalities. In such a situation, it would appear disproportionate to oblige a provider to invest in a functionality the market may not want.

b. **Clarify expectations from providers**. How is it envisaged that a provider would ensure the same level of security and performance, quality of service, output, and performance in the environment of one of its competitors? It appears rules should apply to removing obstacles under a provider's control.

CHAPTER VII INTERNATIONAL CONTEXTS NON-PERSONAL DATA SAFEGUARDS[9]

24. **Avoid unnecessary burdens and disruption to further trade, collaboration, and innovation with likeminded partners**. Ensure ongoing efforts to secure international agreements on data are not impacted and our globalised businesses are not disadvantaged in finalising the proposal.
    a. **Clarify the intended objective of this provision**. The proposal should be proportionate to the actual risk of unlawful data access and should not constitute an unfair or arbitrary barrier to the legitimate transfer of non-personal data to third countries for modern business.
    b. **Clarify Article 27**, regarding the precise obligations on business and when they would apply. Stipulate what constitutes 'all reasonable' measures for this purpose, how would they be assessed and provide an indicative example of when such a conflict of law would (and would not) apply. Clarify the impact of an EU-third country data adequacy agreement on Article 27.
    c. **Reflect the nature of cloud provision**. Any guidance on non-personal data should be consistent with those for personal data, given that often these types of data are stored together.
    d. **Support the ongoing OECD work stream aimed at resolving issues around trusted government access to data**. We encourage all parties in the successful conclusion of this workstream for business certainty and the preservation of rights.

CHAPTER VIII INTEROPERABILITY[10]

25. **Support a bottom-up industry-driven transparent approach to standardisation** that will bring greater interoperability. Complement and build on existing international standards too, so our businesses do not face restrictions of market access when doing business outside the EU.

[9] Seeks to address unlawful third-party access to non-personal data held in the Union by data processing services offered on the Union market.
[10] Proposes requirements to be complied with regarding interoperability for operators of data spaces and data processing service providers as well as for essential requirements for smart contracts.

CHAPTER IX IMPLEMENTATION AND ENFORCEMENT[11]

26. **Harmonise enforcement.** Streamline Chapter 9. Enforcement and fines for non-compliance are split among different competent authorities in Member States poses the risk that rules will be diverging from one country or region to another. Furthermore, sector specific legislation that is expected later should not create imbalances in sectors, as this would prevent businesses from competing on equal footing.

CHAPTER X SUI GENERIS RIGHT UNDER DIRECTIVE 1996/9/EC[12]

27. **Provide further clarity and support the principle that the sui generis right should not hamper B2B data sharing[13]**. While the Commission's intention appears to be to unlock the data generated as a by-product of the functioning of connected objects or related services (and not when data is produced to create databases), there is still no certainty if the sui generis right applies in the instances where makers of databases invest substantially in verifying the generated data. Furthermore, Article 7 paragraph 4 of the Database Directive provides a safeguard that the rights in respect of the contents of databases are without prejudice to *the sui generis right*. There is no clarity as to how Article 35 of the Data Act is addressing this matter.

CHAPTER XI FINAL PROVISIONS[14]

28. **Extend the period in Article 42**. Considering the number of the new obligations for data holders proposed in the Data Act, twelve months will be insufficient to implement all necessary changes.

[11] Concerns implementation and enforcement framework with competent authorities in each Member State, including a complaints mechanism.
[12] Proposes that a provision that the *sui generis* right established in Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or related service.
[13] Article 7 of the Database Directive.
[14] Would enable Commission to adopt delegated acts to introduce a monitoring mechanism on switching charges imposed on providers of data processing services, to further specify the essential requirements regarding interoperability, and to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services.

About Ibec

Ibec is Ireland's largest lobby group and business representative. We campaign for real changes to the policies that matter most to business. Policy is shaped by our diverse membership, who are home grown, multinational, big and small and employ 70% of the private sector workforce in Ireland. With 38 trade associations covering a range of industry sectors, 6 offices around Ireland as well as an office in Brussels. With over 240 employees, Ibec communicates the Irish business voice to key stakeholders at home and abroad. Ibec also provides a wide range of professional services and management training to members on all aspects of human resource management, occupational health and safety, employee relations and employment law.

www.ibec.ie/digitalpolicy
@ibec_irl
Connect with us on LinkedIn