

(12)

<https://mydata-global.org/datagovernanceact> (download as PDF)

Towards interconnected and human-centric data intermediaries

MyData view on the leaked EU Data Governance Act, Nov 5th 2020

Data holder (Art. 2 (3))	3
Data sharing (Art. 2 (5))	3
Scope of data sharing services (Art 9 (2))	4
Interconnectivity of the data sharing services (new addition)	6
Definition of personal data spaces (Art 1)	8
Competent authorities (Art 11 & Art 23)	8
Evaluation of the regulation (Art 33)	9
Fiduciary duty (Art 10 (l))	10
Structural separation (Art 10 (b))	10
Format transformations (Art 10 (e))	11
Name of data sharing services (Art 1 (b))	11

Within the MyData community, we have spent the last few days studying the [leaked version of the upcoming EU regulation called 'Data Governance Act'](#). The draft regulation was leaked on Oct 28, 2020 and the official publication of the European Commission proposal is expected within a few weeks.

We congratulate the teams in the European Commission who have been working hard on this proposal, it is not an easy task to bring forward a groundbreaking regulation. We acknowledge that the actual drafting of the regulation is progressing and the version we are reading is already outdated. Our comments focus on parts where we see potential for changes and adjustments, but this should not be interpreted as criticism towards the proposal, quite the contrary.

MyData is a human-centric approach to personal data that combines industry needs for data with strong digital human rights. In the European Data Strategy, MyData is recognized as one of the movements that “promise significant benefits to individuals, including to their health and wellness, better personal finances, reduced environmental footprint, hassle-free access to public and private services and greater oversight and transparency over their personal data.” [MyData](#)

2 (12)

[operators](#) (as described in the [Understanding MyData Operators white paper](#)) provide infrastructure and tools for the person in a human-centric system of personal data exchange. Operators enable people securely to access, integrate, manage, and use personal data about themselves as well as to control the flow of personal data within and between data sources and data using services. The Data Governance Act regulates ‘data sharing services’, or data intermediaries, such as the MyData operators.

We welcome the regulation as a needed common ground for clarifying the role of data intermediaries, building trust in these intermediaries and setting the direction for data governance, similar to what GDPR did for data protection. At the same time, we advocate for careful scrutiny of the articles, as the Data Governance Act will be regulating a market that is in its very early stages with many cycles of innovation to come. Thus, the regulation will have a strong influence in the nascent market. It can help the market formation if it builds a framework for trustworthiness as intended, but there is also significant risk of unintended consequences – for example, by setting in law certain structures it may inhibit innovation in the development of alternatives.

We look forward to the final regulation to be strong in setting the direction towards human-centricity and interoperability while at the same time leaving space for innovation around how these objectives will be implemented.

Our top picks for potential improvements are:

- define the key roles in data sharing (Art. 2 Definitions) so that **data rights holders and technical data sources can be separated and acknowledge the type of data sharing where individuals are active participants** in the transactions
- clarify the scope of the data sharing services (Art. 9 (2)) and extended it to **include services that empower the data subject beyond compliance**
- address explicitly in the regulation the **interconnectivity of the data sharing services**

We comment on these and few other topics in more detail below and propose some amendments. We look at it from the perspective of personal data, but most of the issues apply also to non-personal data. We have deliberately restricted our analysis to the field competencies within our community and acknowledge there will be other aspects of the proposed act as leaked that will excite other perspectives.

Data holder (Art. 2 (3))

There seems to be no differentiation between the individual and organisation as data holder and there is no differentiation of technical data holder (data guardian) and the data rights holder.

The draft definition of '**data holder**' reads:

*(3) Data holder means a legal person or data subject who, in accordance with applicable Union or national law, **has the right grant access or share certain personal or non-personal data under its control***

Assuming the text should read 'has the right to grant', this definition has two issues:

- 1. Data rights are not naturally always held by one entity only**, as typically the technical data holder has some rights over the data and individuals have other (personal) data rights over the same data.
- 2. Data rights holders do not always have the actual control over the data**, and the right to grant access to data might be held by more than one entity. In the case of personal data, the data subject holds personal data rights and is the principal actor in the data sharing transactions, but typically the technical data holder has the technical means to control the flow of the data and is therefore also a necessary participant in the data transactions.

Our proposal:

'Data holder' as currently in the draft would probably be clearer as the 'data rights holder', especially considering the statement in Art 2 (6) that *"data access does not necessarily imply the transfer or download of such data"*.

In addition to the 'data rights holder', the role of the data source (technical data holder) should be made explicit with a definition in Article 2.

Data sharing (Art. 2 (5))

The 'data sharing' is defined as a bilateral transaction between data holder and data user. In our view, this is limiting as in many cases three parties are needed in the transaction:

1. An organisation that technically holds the data and may also hold some rights over the data (technical data holder),

4 (12)

2. An individual that holds personal data rights,
3. A data using service that will receive the personal data and gain the rights required to process the data (data access is granted for specific purposes).

Acknowledging the type of data sharing where individuals are active participants would support implementation of truly human-centric personal data infrastructure. If such a model is not recognized by the regulation it may unintentionally exclude some existing data sharing services and discourage further development of solutions where people are active participants in data sharing transactions between data sources and data users.

There is precedence of challenges following the regulation that only recognizes bilateral data sharing:

The Australian Government has introduced a consumer data right (CDR) with the objective to give consumers greater access to and control over their data. It also recognises only data holders and data users with no mechanism for individuals to directly exercise participation. Since the introduction of CDR the Australian regulators have realised that there needs to be a mechanism for citizens to be included and they have now commissioned a new body of work for a policy or regulation around consent.

The draft definition of '**data sharing**' reads:

(5) Data sharing means the act of a data holder providing data access to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements or mandatory rules.

Our proposal:

(5) Data sharing means the act of a data **rights** holder **and data source** providing data access to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements or mandatory rules.

Scope of data sharing services (Art 9 (2))

The second clause of Article 9 sets out the scope of the data sharing services to which the general authorisation framework shall apply. The clause describes 3 classes of data using services and, as written, makes no distinction between personal and non-personal data.

5 (12)

In the definition of the first class of services (a), natural persons are excluded and the use of the possessive 'their data' implies that this class is for organisations with independent rights to grant access to non-personal data. If this is the intention, it should be made explicit in the text to avoid confusion and the need for interpretation.

The exclusion of personal data from the first class of services and/or the need to allow data subjects access to authorised services that deal directly with data users, then requires an additional class for personal data. This class will provide for authorisation of services that allow a data subject to make personal data available to data users as well as the establishment of specific infrastructure for that purpose.

The definition services in the second class (b) is a very narrow characterisation of the purposes for which a data subject can use their personal data spaces. This should be expanded to include services that empower the data subject beyond GDPR compliance, that are beneficial to the data subject, or that are demanded by the data subject. It must be clear that where the individual has the option to select a data sharing service, they have a real choice and that 'technical data holders' recognise them as the legitimate representative of the individual.

The third class of data sharing services (c) are data cooperatives, also commonly referred to as data trusts and data unions. Again, this has a narrow characterisation of the potential for data cooperatives purposes, restricting the application to compliance with the GDPR. We suggest that should be expanded as described above for the class (b) services.

While there may be risks of expanding these definitions, the idea that there could be data sharing services outside the regulation because they do not include those for GDPR compliance is, surely, a great risk. We therefore have a further question about the status of data intermediaries not falling under Art 9(2). Are they henceforth 'prohibited' by the regulation or simply not subject to the general authorisation scheme? Under the second interpretation, intermediaries outside that framework are likely to be considered 'less trustworthy'. Assuming the second interpretation as most likely, this may have the effect of two markets developing in parallel under separate legal frameworks. Does the commission intend for Member States to have local regulatory powers in this case?

Our proposal:

Art 9 (2a) should either be made explicit to non-personal data over which a legal person has exclusive rights, or modified to: "services aimed at supporting data holders which are legal persons to make available **data to which they may lawfully grant access** to potential data

users, which may include...”

An additional class to be added to Art 9 (2): “services aimed at supporting data subjects to make available personal data, stored in one or multiple data sources to potential data users, as well as the establishment of a specific infrastructure for the interconnection of data rights holders, data sources and data users”

Expand Art 9 (2b) to be “services aimed at the creation of personal data spaces for data subjects to exercise the rights provided in Regulation (EU) 2016/679 and coordinate other personal data services which may be paired by making available dedicated data storage services to the data subject”

Expand Art 9 (2c) to be “services aimed at the creation of data cooperatives for data subjects to exercise the rights provided in Regulation (EU) 2016/679 and coordinate other data services which may be paired by making available dedicated data storage services to such data subjects”

In addition, Article 12 specifies the required information to be notified under the general authorisation framework. The class (as defined in Article 9 (2)) for which a service is authorised is important information for transparency and the assessment of trustworthiness - this should be explicit in the notification provided by the service. We suggest that information about the class or classes for which a data using service provider has notified should be mandated.

Our proposal:

Article 12 (5f) be expanded to be “A description of the service it seeks to provide including the class or classes of those services as described in Article 9 (2)”

Interconnectivity of the data sharing services (new addition)

We would like to highlight the absolute necessity of including interoperability as a foundational principle in the Data Governance Act. Interoperability and standards are already mentioned as important objectives for the regulation in the foreground, but in the actual articles, they are incorporated only very lightly.

The draft definition mentions ‘standards’ in the Article 25 Tasks of the European Data Innovation Board:

(c) To advise the Commission on the prioritisation of cross-sector standards to be used and developed for data use and data sharing, while taking into account sector specific standardisation activities

7 (12)

This is a very weak mention as neither the Data Innovation Board nor Commission would have any power to mandate any interoperability requirements.

We suggest that the regulation should set up **clear direction and progressively evolving minimum requirements for the interconnectivity of the data sharing service providers** so that they will form over time a network of intermediaries, instead of isolated silos. Such interconnectivity between the data sharing services will, on one hand, enable substitutability and therefore allow individuals and organisations) to choose the best service providers, fostering market innovation. On the other hand, interoperability will create network effects and speed up the adoption of data intermediaries. This approach will also prevent the market of data sharing services evolving to a winner-takes-all situation.

We see that enabling the interconnectivity between data intermediaries by setting mandatory requirements would be the most important regulatory intervention as it is doubtful if such interconnectivity would emerge otherwise. Clearly, interoperability of data is also necessary, but we see that it will be developed voluntarily by market actors in different sectors and use cases without any regulatory intervention.

We acknowledge the difficulty of codifying in the law such minimum criteria for interoperability in a way that would not be prohibitively restrictive in the early stages of developing data sharing services. This could be implemented by giving the Commission the possibility to determine the interoperability criteria in the form of a 'delegated act' upon being advised by the Data Innovation Board.

Typically delegated acts are not very popular since they increase uncertainty in the legal environment. However, for this purpose it could be a viable option if we have the clear goal of the interoperability in the articles itself and the scope narrowly what will be regulated with the delegated act.

In this regulation there is already one delegated act in Article 22 European data altruism consent form:

(1) In order to facilitate data altruism activities, the Commission may develop European data altruism consent forms, by means of delegated acts.

There is also the example of Art. 12(8) GDPR regarding delegated act power in the case of standardized privacy icons:

“The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.”

Our proposal:

Our recommendation is to add a new article **‘Interconnectivity of data sharing services’** which states the overall direction of interconnected network of data sharing services.

In that article add the delegated act:

(1) In order to facilitate the interconnectivity between the data sharing service, the Commission may develop minimum interoperability criteria, by means of delegated acts.

Definition of personal data spaces (Art 1)

The term ‘personal data spaces’ should be defined clearly as this term is used extensively in the regulation and other communications.

Personal data spaces should be understood as the data spaces that individuals have. Each individual should have their own logical personal data space independent of what data is in it, where the data is held physically, and on what technology or service provider is used to run the personal data space. These personal data spaces are horizontal and cross-cutting in relation to the other data spaces, but we should not speak about a personal data space in singular. The individual should be supported to integrate data from multiple sources into their logical personal data spaces.

Our proposal:

The definition of ‘personal data spaces’ should be made explicit with a definition in Article 2, making it clear that personal data spaces are personal to the individual.

Competent authorities (Art 11 & Art 23)

The authorization and supervision scheme is quite elaborate yet, at the same time, open to diversification and domestic flavors. Our concern is that a network of national authorities may result in fragmented practices that differ between member states. Such variation in practices would (1) undermine the objective of building trust towards the data in intermediaries, (2) negatively influence the fair competition between the data sharing service providers and also, (3)

cause administrative overhead for the service providers that are working internationally.

We also believe that it would be easier to accumulate needed skills, competences and understanding about the emerging new market of data sharing services in one central agency instead of a number of small national entities.

Some known benefits of national authorities would be: (1) close engagement with the market players at the national level, (2) the possibility for national authorities to develop their practices more flexibly, and (3) a wider network of authorities sharing knowledge and co-developing practices.

Presumably, the competent authorities would be supervised by the Commission and the European Data innovation board to prevent a race to the bottom and forum shopping, however in the leaked version of the regulation this was not evident. It is also unclear if the competent authorities are necessarily state agencies or could also be private entities.

Interestingly, the Data Governance Act does not foresee a private cause of action against the competent authority, at least not under its Article 29. Such cause of action might be available under general law, however.

Our proposal:

Consider systematically the pros and cons between the options of designating member state authorities or one EU agency to carry out the tasks related to the general authorisation framework. Whichever option is chosen make sure to set measures to compensate the down sides of the chosen option.

Evaluation of the regulation (Art 33)

The regulated space is new - and will require a review in a few years down the line.

The leaked document suggests the evaluation “no sooner than 4 years after the day of application of this Regulation”. Indeed as the market is being shaped, this regulation will certainly need to be reviewed and this review should not be pushed indefinitely. A more useful way to phrase this would be - to make sure it is not pushed too far, would be:

Our proposal:

“no **later** than 4 years after the day of application of this Regulation”

Fiduciary duty (Art 10 (I))

In our reading of the leaked text, we have paid attention to very important questions of permissible business models, separation of functions and the legal implications of being a 'fiduciary' (esp. Art. 10). While MyData Global is not arguing against fiduciaries duties, we see significant regulatory constraints in the proposals without any commensurate incentives for the data sharing services.

In the MyData Operators white paper, we proposed that it would suffice that the operators carry a duty of care, which is a lower threshold than the requirement for data sharing services to operate as fiduciaries. The legal concept of a fiduciary has different scope and meaning in different legal systems. The Data Governance Act introduces an explicit duty to actively consult data subjects about data sharing practices. Coupled with compliance measures in Art. 13, exposure to private lawsuits and the structural separation requirement (Art. 10(b)), the framework would lay a serious burden on the service providers.

The fiduciary requirement of Art10(I) is at the strong end of the responsibility between operator and person. This has important impacts for any discussions about self-regulatory and optional governance schemes that sit below the level of the legislation - it may limit the potential scope of these considerably.

Continuing to think about the fiduciary requirement of Art10(I), this will also impact the viable business models for organisations working as operators. This requirement raises the cost of delivering the service and it is hard to see what options there will be for operator-only services - they will need to be paid by the services they support or offer their own, separated services.

Our proposal:

Consider systematically the pros and cons between the options of fiduciary and duty of care requirements on data sharing services. Whichever option is chosen make sure to set measures to compensate the down sides of the chosen option.

Structural separation (Art 10 (b))

Art 10(b), in its current wording, seemingly prohibits an original (primary purpose) controller and data holder to serve a data sharing service under the same entity, as could be the case

11 (12)

for some public sector entities deciding upon giving partial data rights on data re-use towards data subjects of original processing. For example, a Member State or a municipality would not be allowed to provide a data sharing service (enabling re-use of original personal data collected under 2016/679 legal basis of public interest) for its citizens, but would have to organise such data sharing via a third party or other separate legal entity.

In contrast, providing a data sharing service should be allowed by the entity but separated into different service provisioning functions (services) with proper isolation. The text's intention is clear and supported (not to misuse the data they intermediate as a fiduciary by maliciously taking the role of a data user) but strict interpretations could cause confusion especially if the data sharing service providing organisation is also a data holder to the same data.

Our proposal:

Clarify Art 10(b) to clear means for providing data sharing service as a large (i.e. region/state, metropolitan area) public sector organisation with intention to open up existing primary-purpose collected personal data for re-use by adopting a data sharing service function.

Format transformations (Art 10 (e))

It is our understanding that the objective of Art 10(e) is to stop data sharing services from deliberately transforming data into proprietary formats (lock-in with proprietary formats). The current wording would prohibit the use of open standard formats and may actually inhibit useful format conversions by leaving room for legal uncertainty about what specific format conversions can be considered to facilitate use by data users.

Our proposal:

We suggest rewording Art 10 (e) so that it specifically states that lock-in using proprietary format shall not be acceptable and conversions to widely used standard formats is acceptable and encouraged.

Name of data sharing services (Art 1 (b))

Sharing data is only one type of activity that the data intermediaries must facilitate and create infrastructure for. The infrastructure providers offer tools and services that support management of data more widely, with decisions around the sharing of data being a subset of 'personal data

12 (12)

management'.

Our proposal:

We suggest changing 'providers of data sharing services' to 'data intermediaries' or, specifically 'personal data intermediaries' - this term is used in the recitals but not in the articles as a noun.