Granular Data Governance Systems for Open Data

A primer on the impact of the Data Governance Act on open data ecosystems

data.europa.eu
The official portal for European data

This study has been prepared as part of data.europa.eu, an initiative of the European Commission. The Publications Office of the European Union is responsible for the management of data.europa.eu contracts.

For more information about this paper, please contact the following.

European Commission
Directorate-General for Communications Networks, Content and Technology
Unit G.1 Data Policy and Innovation
Email: CNECT-G1@ec.europa.eu

data.europa.eu
Email: info@data.europa.eu

Author:
Hans Graux

Last update: 29 May 2024
https://data.europa.eu/

ISBN: 978-92-78-44250-7 doi: 10.2830/796169 Catalogue number: OA-02-24-798-EN-N

Contents

What is data governance in relation to open data?

1. An introduction to data governance in open data

Data governance generally refers to any human-based system comprising directing, overseeing and accountability, in relation to the availability, usability, integrity and security of certain datasets. These processes help to define the actions people must take, the processes they must follow, and the technology that supports them throughout the data life cycle.

A key aspect of data governance relates to defining data control mechanisms and data usage rights – or in simpler terms, who is allowed to access data for which purposes, and through which systems. Data governance systems can therefore be very straightforward (e.g. "our data can be freely downloaded and used by anyone from an openly accessible server") or very granular (e.g. "accessibility and usage rights depend on the dataset; specific rules, procedures and requirements are defined per dataset, and prior registration is required before access and usage rights are granted"). The establishment of clear data governance rules therefore ensures that data will be made available to parties that have a right to access and use it, while reducing the risk of misuse.

The European data strategy with its open data policy, aims to ensure that information (especially information held by public sector bodies) is made freely available for re-use for any purpose, wherever possible. This has contributed to the emergence of open data ecosystems, to be understood as networks of public administrations, companies and reusers of data that all contribute to increasing the availability and use of datasets. Examples of such open data ecosystems would be the various European open data portals and their surrounding communities of administrations that provide their data to the portals, as well as the organisations that support their growth and use, and the companies that build applications and services around such portals.

These ecosystems tend to implement straightforward data governance systems: when data is openly available, this implies that it should be as freely accessible as possible, including by downloading the data from national or EU level open data portals, or by accessing it via open APIs. Complex data governance systems that impose specific requirements inherently create tensions with the basic objective of open data: the more hoops a user has to jump through under a complex data governance system, the less open it arguably is.

The European Open Data Directive (Directive (EU) 2019/1024) is the most recent iteration of the EU's legal framework governing the availability and reuse of public sector information (PSI). It plays a crucial role in promoting the reuse of PSI across the EU, by defining minimum criteria for public sector bodies to make their PSI available. The general principle is that PSI which falls within the scope of the Directive is made openly available for reuse by both commercial and non-commercial entities.

This sound principle does come at a price, though. PSI generally includes any existing documents held by public sector bodies of the Member States. A document is understood as any representation of

acts, facts or information — and any compilation of such acts, facts or information — whatever its medium (in paper or electronic form or as a sound, visual or audiovisual recording). The scope of PSI (and thus of the Directive) can thus be very extensive.

However, not all information is suitable for fully open reuse. For that reason, the scoping of the Open Data Directive is significantly reduced by Article 1.2, which excludes certain types of PSI from the Directive. By way of examples, the Directive does not apply to any documents for which third parties hold intellectual property rights, which are commercially confidential, or for which access is excluded or restricted by virtue of the access regimes on grounds of protection of personal data. Generally, open availability and reuse is mandatory under the Open Data Directive if there is no clear direct and disproportionate harm to a third party that might suffer negative repercussions by having data that relates to them being openly available.

The Open Data Directive thus creates a fairly balanced regime. It introduces a general principle of openness: if data can be made openly available under the rules of the Directive (meaning that it is not excluded from the scope of the Directive), then public sector bodies should do so. The Directive furthermore explicitly encourages the use of portal sites for the publication of open data, thus supporting the establishment of an open data governance system.

The outcome is beneficial, but is not without flaws. Specifically, the outcome of the Directive's application can be somewhat binary: data is either openly available, or it isn't available at all. More nuanced perspectives on data availability and data governance are possible, which are perfectly permissible already under the Directive, under which more granular decisions can be made: data is made available to some categories of reusers or for some use case, but not for others. Via the Data Governance Act, which entered into application on 24 September 2023, these nuanced perspectives now have a clear legal basis.

2. Problem statement and structure of this research paper

The Data Governance Act (DGA) brought about a number of developments in the EU's legal framework, both in relation to the availability and reuse of PSI, and in relation to data governance in general (including in purely private sector use cases that would be outside of the scope of the Open Data Directive).

Briefly summarised, the DGA introduces several key innovations to enhance trust, facilitate data sharing, and promote responsible data reuse within the European Union. Three of these are examined within this research paper:

- Firstly, the DGA **broadens the legal framework for the reuse of certain categories of data** held by public sector bodies. Certain types of sensitive data that were (and remain) excluded from the scope of the Open Data Directive, such as personal data and commercially confidential data, may now be made available if certain specific safeguards are followed. Notably, it allows the designation of **competent bodies** in the Member States, that would make available a **secure processing environment** (SPE) for sensitive data re-use cases. By relying on a competent body, some of the excluded data can still be made available via the

SPE in a more granular way – i.e. towards specific trusted beneficiaries, or for specific use cases.

- Secondly, the DGA introduces a legal framework for **data intermediation services**, a specialised category of service providers whose platforms would allow data holders to share their data in a controlled manner. The services of data intermediaries are not limited to PSI; they can provide their services to the private sector as well. The outcome however is comparable to the use of competent bodies: they enable more tailored decision making when it comes to sharing data, without reducing it to an all-or-nothing decision.
- Thirdly, the notion of **data altruism** is introduced. Via data altruism services, citizens can make their data available to third parties to achieve objectives of general interest, such as healthcare, combating climate change, improving mobility, scientific research, etc. While the two first innovations above allow data sharing decisions to be made by data holders, data altruism places that possibility with the data subject – the person to whom the data relates.

These innovations allow data holders and individuals to more easily retain **sovereignty and control over their data**, while still enabling the sharing and reuse of data to a certain extent without compromising on privacy or confidentiality.

This research paper examines how these innovations from the DGA will affect open data ecosystems and the sharing of PSI, and how these services can be used by and towards public sector bodies. Can all of them be used in open data environments? What are the trade-offs? And how should public sector bodies approach the new possibilities and risks to be managed?

In the sections below, we will first examine how public sector bodies are affected in situations where *they* decide to share data or not (i.e. the impact of competent bodies and SPEs, Chapter I); and secondly how citizens can be brought into the decision-making process via the mechanism of data altruism (Chapter II). We will conclude with our overall findings on the opportunities and risks of new data governance systems (Chapter III).

Data sovereignty for public sector bodies: the role of intermediaries

1. Introduction on intermediaries in open data

Even prior to the entry into application of the DGA, the reliance on intermediaries was not new in open data ecosystems. In this context, intermediaries can be broadly understood as third parties that play an enabling and facilitating role in ensuring that data can be found, shared and reused easily. The introduction and promotion of data sharing platforms at the national and EU level is a simple example of an intermediary with clear benefits: the platform provides a single point of contact for reusers, and helps them to find and interpret usable data sets.

But platforms in this context are a relatively passive type of intermediary. Not unlike the intermediary service providers defined in European eCommerce legislation (hosting, caching and mere conduit providers), open data platforms have no inherent selection or curating role in relation to the data – they publish what the data holders make available. Additionally, such platforms don't necessarily provide any tools that allow data holders and reusers to interact directly in order to determine the suitability of their match: data is either publicly available to all aspiring reusers, or it is unavailable – there is no decision support system that allows data holder to determine in a more granular fashion whether sharing data is appropriate for a specific use case.

The DGA aimed to change this relatively static image by introducing an EU wide framework for the sharing of sensitive data, and for data intermediation services. These will be briefly described in the following sections.

2. The innovations of the Data Governance Act

Public sector information and secure processing environments

As was already described in the introductory sections, the DGA recognised that in some cases, it should be possible to share sensitive PSI, even in situations where the Open Data Directive didn't apply. For instance, if a certain PSI dataset was subject to certain third party intellectual property rights, it might still be appropriate to share that data if a legal exception would allow the sharing and reuse of that data, e.g. for scientific research or for educational purposes (depending on national copyright law). Similarly, a dataset containing personal data could still be shared if a specific legislation would allow this, even if the Open Data Directive wouldn't apply.

To address these cases, Chapter II of the DGA introduces more nuanced rules for the reuse of certain categories of protected data held by public sector bodies, which apply alongside the rules of the Open Data Directive (which are not modified by the DGA). This Chapter applies only to data held by public sector bodies which are protected on grounds of commercial confidentiality, statistical confidentiality, intellectual property rights of third parties, or data protection. Without requiring these to be made open entirely (i.e. without making them open data as such), it allows public sector bodies to share such data without compromising its protected nature.

Under the DGA, Member States should examine whether it is possible under national law to share these categories of personal data, and to publish the conditions under which this is possible. These conditions can provide for requirements to e.g. first anonymise the data, or to modify it in such a way that the confidentiality and value of the data is safeguarded, without removing its utility to a reuser. They may also impose a limitation that the data can only be accessed and reused remotely within a secure processing environment (SPE) that is provided or controlled by the public sector body, or within the physical premises in which the SPE is located. In other words, in these instances, the public sector body creates the technical and operational conditions (the secure processing environment) that allow the value of the data to be extracted towards an authenticated party. The public sector body becomes an intermediary, rather than a mere data provider.

The new framework of the DGA is, in a sense, a continuation of a pre-existing PSI paradigm shift. While initial PSI directives focused principally on making already available data available under nondiscriminatory terms, later legal revisions focused more on dynamic services where public sector

bodies were encouraged or even required (for high value datasets) to make their data available via APIs – making them service providers, rather than data providers. The new rules in the DGA add a new layer, requiring Member States to ensure that solutions are explored even when complete openness is not legally viable.

The establishment and operation of SPEs is of course not a trivial matter. Member States will need to provide a broad range of tools, including technical solutions for techniques such as anonymization and pseudonymization, the establishment of secure data rooms with accompanying identification and authentication requirements, and policies and contractual terms to enable and manage access and reuse rights.

Since this is a specialized task, Member States will have to designate one or more competent bodies that will support the public sector bodies granting access to the reuse, including by providing the latter with an SPE and by advising them on how to best structure and store data to make it easily accessible. This is complex, but there are ample best practices to build on – notably in the health data sphere, where SPEs have been established for a long time already as a way to facilitate medical research.

It is important to stress however that the DGA introduces no exceptions to the Open Data Directive, nor to intellectual property rights legislation or to data protection law. Where data access and reuse is plainly unlawful, the use of an SPE is not able to provide a solution. Rather, SPEs are aimed at providing a solution where lawful sharing is possible, but complex. In that sense, the intermediary role of SPEs is not to provide a simple solution, but to bundle the expertise (technically, legally and organizationally) that makes data sharing possible.

Data intermediation services

Given the description of SPEs above, it may seem curious that there is a separate and broader framework for data intermediation services in Chapter III of the DGA. After all, if SPEs are available, then hasn't an optimal solution been reached already?

The answer to this question lies in the observation that SPEs and the role of competent bodies are limited to the sharing of data held by public sector bodies. A significant volume of valuable data is held by private sector bodies (such as companies, whether for profit or not for profit), where it may be legally required or simply mutually beneficial to share this data with other private entities, or with the public sector.

Many studies have shown that data sharing currently occurs at a suboptimal level, and that there would be significant value for both the data holder and the data recipients (and for society as a whole) if levels of data sharing could be increased. However, companies often fear that data sharing will have an excessive economic cost, by allowing their competitors to benefit from their investments.

In order to mitigate this problem, Chapter III of the DGA contains a set of rules for providers of data intermediation services (so-called data intermediaries, such as data marketplaces), which should act as trusted third parties in setting up data sharing relationships. Given this objective, the DGA imposes requirements on these intermediaries to ensure their trustworthiness and neutrality.

The DGA distinguishes three broad categories of intermediaries:

- **intermediation services between data holders and potential data users** – i.e. data brokering services, which can operate in a business-to-business model, or in business-to-consumer or business-to-administration. These services generally provide a technical platform that enables bilateral or multilateral exchanges of data, or allow the joint use of data;
- **intermediation services between data subjects (i.e. natural persons) and potential data users** – i.e. personal data management systems that allow individual citizens to decide whether they want to share their data, with whom, and for which purposes, and which enable them to easily exercise their data protection rights under EU data protection law (such as the right to correct data, to delete it, or to obtain a copy of it).
- **services of data cooperatives**, where members of a common organisational structure establish shared rules in relation to their rights with respect to certain data, such as agricultural cooperatives.

These various types of intermediaries are required to meet several legal requirements under the DGA, including notably the following:

- They must submit a prior notification to a nationally designated competent authority, before they are allowed to offer their services. The competent authority will verify that the service provider meets the requirements of the DGA, and only after this step is completed, the service provider may identify itself as a 'data intermediation services provider recognised in the Union', and apply a common logo.
- After the successful completion of the verification, the service provider will be identified in an EU level register.
- Data intermediation services providers are not allowed to use the data for purposes other than to put them at the disposal of data users. Data intermediation services through a separate legal person.
- Charging is allowed, but commercial terms, including pricing, may not be dependent upon whether the data holder or data user uses other services. Commercial bundling of services is thus discouraged.
- Data intermediation services providers must facilitate the exchange of the data in the format in which it receives it, notably by converting the data into specific formats only to enhance interoperability.
- Data intermediation services providers must ensure that the procedure for access to their services is fair, transparent and non-discriminatory.
- Data intermediation services providers must take measures to ensure continuity in the event of its insolvency.
- Data intermediation services providers must put in place adequate technical, legal and organisational measures in order to prevent the unlawful transfer of or access to non-personal data.
- Data intermediation services providers must act in the data subjects' best interest where it facilitates the exercise of their rights, in particular by informing and, where appropriate, advising them about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent.

Collectively, these requirements aim to ensure that the newly minted intermediaries act responsibly, independently, and neutrally. Where the users of the services are natural persons that share their own personal data, the intermediaries have a duty to represent their best interests – i.e. in that particular use case, the neutrality is diminished in favour of the individual citizen, who is likely to be the most vulnerable party.

The DGA regime is recent, having only entered into full application in September 2023. None the less, it has already achieved some result: as of May 2024, the register contains two entities: one in Finland, and one in Hungary.

3. The relevance of the DGA to the open data community

Given the objectives of the DGA and the description above, the relevance of the new legal framework to the open data community is clear. With respect to the sharing of sensitive categories of information and the role of SPEs, the impact is very explicit: public sector bodies are required to carefully consider whether it is legally possible to make such data available for reuse. This is a significant shift from the prior framework, which could have unintentionally incentivized public sector bodies to argue that, since the Open Data Directive didn't apply, sharing was not necessary. This could result in missed opportunities. The DGA instead forces public sector bodies to consider positive options for data sharing, including by calling on SPEs and advances anonymisation and pseudonymisation solutions, rather than opting for an easier negative answer.

With respect to data sharing intermediaries, the impact to the open data community is less direct, but potentially at least equally significant. Public sector bodies are not required to rely on such intermediaries, neither as a data holder, nor as a data requestor. None the less, the anticipated benefits of these intermediaries apply equally to the public sector. Conceptually, it is perfectly viable to offer some categories of data – including the aforementioned sensitive categories of data – via data sharing intermediaries – or indeed for public sector bodies to receive access and usage rights to certain data held by a different public or private sector data holder. In this way, public sector bodies can offset some of the potential costs and complexities of designing their own solutions, and plug into a potentially broader audience, since the intermediaries are likely to already have a pre-existing customer base.

Inversely, the intermediaries can also become an interesting resource for public sector access to critical data. In the context of e.g. handling pandemics, managing climate evolution, or addressing mobility and energy challenges, data sharing intermediaries are a viable partner in getting access to valuable information that data holders might be less willing or interested in sharing directly. The Data Act of course offers more direct means for the public sector to demand access to such data for specific public interest purposes; but via intermediaries, public administrations will have a less forceful option to seek access as well. In that sense, intermediaries offer a new avenue to enable access to data that might otherwise have remained hidden.

Data sovereignty for individuals: the role of personal data management

1. Introduction to personal data management

Most of the preceding sections of this paper – and virtually all PSI legislation, including the Open Data Directive – focused on data exchanges between public administrations and companies. The Open Data Directive inherently focuses on documents held by public sector bodies, and on how reusers (natural persons or legal entities) can get access to such data with the objective of reusing it. Similarly, many of the use cases of data sharing intermediaries focus on interactions between companies or public sector bodies acting as data holders, choosing to make their data available or not to an interested party.

But there is another perspective, namely that of the individual human being. An individual can also be empowered to take control over the data that relates to them. Indeed, this right and ability is one of the main focal points of European data protection law, and notably the General Data Protection Regulation (GDPR). The GDPR allows individual natural persons (data subjects) to exercise certain rights in relation to data that can be linked to them (personal data). This includes the right to share data with third parties based on their freely given, specific, informed and unambiguous consent; to withdraw that consent; and to demand the right to correct or delete their data, or to obtain copies of it (all subject to certain constraints and safeguards).

With that in mind, it is possible to create systems that allow data subjects to decide when and how they wish to share their own personal data. These systems are known as personal data management (PDM) systems, or personal information management systems (PIMS), defined by the European Data Protection Supervisor as "*systems that help give individuals more control over their personal data. PIMS allow individuals to manage their personal data in secure, local or online storage systems and share them when and with whom they choose. Providers of online services and advertisers will need to interact with the PIMS if they plan to process individuals' data. This can enable a human centric approach to personal information and new business models*".

Personal data management systems add a new layer to the open data community: rather than information being shared by public sector bodies or companies, citizens take control themselves. This opens up new options, especially in cases where, under EU data protection law, there is no legal basis that would allow a data holder to share certain personal data. For instance, if a medical research organization wants to obtain access to medical records from a hospital, a personal data management system can facilitate this process by allowing the patients to consent to this directly.

In practice, the process is not that simple. Beyond simply ensuring that the data exists somewhere and is available in a shareable format, a reliable system needs to be created that can be used to obtain the necessary and legally valid consents. It is precisely on this point that the DGA has intervened.

2. The innovations of the Data Governance Act

The DGA supports personal data management via two separate strands of action: firstly via data sharing intermediaries, and secondly via a new framework for data altruism.

The data sharing intermediaries have already been discussed above: intermediary services providers can also offer their services to individual persons, allowing them to share their personal data through a trusted third party. Largely, intermediaries acting in relation to data subjects have to follow the same requirements and obligations as other intermediaries, such as prior registration with a competent authority, transparency, interoperability, continuity, security and so forth. The principal unique element is that intermediary service providers for data subjects are expected to represent the best interests of the data subjects – a so-called fiduciary duty where the neutrality of the intermediary is slanted towards the individual person.

The use of data intermediation services for personal data also creates an interesting new option, since commercial transactions (i.e. paying for data usage rights) are permissible under the DGA. In other words, it is conceptually possible for citizens to 'sell' usage rights to their personal data. This possibility has been criticized by data protection authorities, since so-called "commodification of personal data", where personal data is treated as a tradeable commodity, is seen as being at odds with the fundamental right to data protection – fundamental rights should, in principle, not be waivable as a result of commercial transactions. Nonetheless, under the DGA, the option is not fundamentally unlawful.

Partially in response to this concern, the DGA also introduces a specific set of rules for data altruism, in Chapter IV. The notion is defined in the DGA as "*the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest*". In short, data altruism relates to situations where persons consent to making their data available for free (or merely for a cost compensation), for legally recognised objectives of common good. The focus is on creating societal benefit, rather than on individual gains.

In order to support data altruism, the DGA sets up a framework that is somewhat comparable to that of intermediary services providers. As with the intermediary services, a data altruism organisation will have to undergo a prior registration process with a competent authority designated by the Member States, resulting (after verification) in an EU level registration as a 'data altruism organisations recognised in the Union'. After verification, the organisation will be allowed to use that designation, and the common EU logo.

None the less, there are a few requirements which are unique for data altruism. The organisations must have a not-for-profit character, and offer specific safeguards to protect the rights and interests of citizens and companies who share their data. In addition, they must comply with an EU level rulebook, which will be developed by the Commission, in close cooperation with data altruism organisations and other relevant stakeholders. The rulebook, which is presently not yet available, will lay down

information requirements, technical and security requirements, communication roadmaps and recommendations on interoperability standards. Additionally, the Member States may still apply national policies to data altruism organisations, in order to assist data subjects in making personal data related to them held by public sector bodies available for data altruism, and to set out more detailed transparency requirements.

The system is still fairly recent, and as of May 2024, the altruism register contains one organisation, established in Spain.

3. The relevance of the DGA to the open data community

With respect to personal data management, the potential relevance and impact of the DGA is perhaps more challenging to predict. Public sector bodies are generally not in the habit of interacting with individual citizens to seek their consent when making PSI data sharing decisions – indeed, in instances where individual citizens could be identified and contacted on the basis of the data in the PSI, there would be a strong interest for public sector bodies in not making the data available at all since that might trigger data protection compliance concerns.

On that point, the DGA certainly has the potential of opening new data sharing options: where data sharing would not normally be possible because of data protection problems, the frameworks for data intermediation and for data altruism constitute a possible solution. There are some indications already of early experimentation with personal data vaults and personal data management in European public sector bodies, although these are clearly still in their early stages.

Moreover, intermediaries and even data altruism are conceptually viable avenues for public sector bodies to gain access to data that would not normally be available to them. Where a public sector body might traditionally need to rely on the creation of a specific legal mandate (e.g. a revised legislation) in order to have a legal basis to collect new information, intermediaries and data altruism could become complementary data sources through which data could be collected on a voluntary basis for public sector bodies as well.

Time will tell whether the DGA will be able to spur innovation for the open data community in these cases.

Overall conclusions on new opportunities for open data as a result of the DGA

The overall picture that emerges from this paper is clear: where traditional open data ecosystems are fairly binary in leading to an all-or-nothing approach (data is either available as open data, or it is not available), the DGA creates more granular options. Via secure processing environments, data intermediation services and data altruism, data can be made available in situations where this would not normally be possible, by creating specialised data governance frameworks that can be applied and enforced through specialised technical platforms.

It is worth noting that these new rules in the DGA complement, but don't replace, the existing rules of the Open Data Directive. The open data principles are not undercut – rather, a parallel framework is created that allows new possibilities to be exploited. This is important, because the more granular governance mechanisms of the DGA come with an obvious downside: they all rely on additional procedures and safeguards to ensure the confidentiality of the data. As a result, data which is available via the DGA's mechanisms will generally be "less open" than the data that can be found on data portals – aspiring reusers will have to satisfy a number of requirements before they get access. This is inherent to the design of these services, and not problematic in reality, since the new mechanisms are intended to be applied in instances where the Open Data Directive does not provide a comprehensive solution.

The DGA is still a young legal framework. As the overview above shows, the market is still in its infancy, with only two registered data intermediation services, and one data altruism organisations. There are many open questions still in relation to the challenges that these entities have to overcome, including how they can grow to a significant cross border scale, how the solutions can be applied across multiple sectors and industries that have very different concerns, and how exactly the business case will work, since someone will have to pay to ensure sustainability.

None the less, the potential benefits are obvious: the DGA creates more granular data sharing options for cases that could not be appropriately or fully resolved via the rules of the Open Data Directive. By doing so, the DGA creates new opportunities, and enables data holders and individual citizens to retain a degree of direct sovereignty over their data, while still allowing value to be extracted from that data. In that sense, the lessons of the DGA are well worth learning.

Bibliography – sources and references

- Data Governance and Compliance - Evolving to Our Current High Stakes Environment, Rupa Mahanti, 2021, Springer
- Data Governance in AI, FinTech and LegalTech - Law and Regulation in the Financial Sector, Aline Darbellay, Joseph Lee, 2022, Edward Elgar Publishing
- New Data Governance Act - A Practitioner's Guide, Kristina Schreiber, Patrick Pommerening, Philipp Schoel, 2023, Bloomsbury Academic
- Study to support an Impact Assessment on enhancing the use of data in Europe, see https://ec.europa.eu/newsroom/dae/redirection/document/83513
- Report on architecture and infrastructure options to support EHDS services for secondary use of data; see https://tehdas.eu/app/uploads/2023/03/tehdas-report-on-architecture-and-infrastructure-options-to-support-ehds-services.pdf
- European Commission, Data Governance Act explained - https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained
- Regulating data intermediaire: The impact of the Data Governance Act on the EU's data economy, Gabriele Carovano, Michèle Finck, Computer Law & Security Review, Volume 50, September 2023,
- IBM, What is data governance? See https://www.ibm.com/topics/data-governance

Publications Office
of the European Union