

# The Data Governance Act: Breaking down the strategy for data

Written by Florina Pop and Laura Grant

## Introduction

Data has become a huge part of our daily life, and the European Commission realised that data sharing and the re-use of data had limited capacity. With that, the Data Governance Act (COM/2022/68) was born as the first deliverable under the European Strategy for Data. It came into force in June 2022 and will be applicable as of September 2023. This blog aims to provide you with a clear overview of three key aims of the Act, their benefits, and potential concerns.

### Aim 1: Wider re-use of protected public-sector data

Although the Open Data Directive (2019/1024) allows for the use and re-use of public data, certain categories of protected data remain inaccessible, even for research and innovation activities. Therefore, the Commission decided to build upon the Directive, making available under-utilised data across the EU for the benefit of society. This concept will enable the re-use and sharing of protected data held by public sector bodies in a safe manner across sectors (Articles 3-8). It won't create a strict obligation on these bodies to allow data re-use (unlike the ODD) nor release them from confidentiality obligations without prior consent. The Act applies to certain categories of protected data held by public sector bodies that are protected through either:

- (i) commercial confidentiality,
- (ii) statistical confidentiality,
- (iii) intellectual property rights of third parties' protection, or

- (iv) personal data protection.



Where data are made available, they can be shared via a single information point that receives requests for re-use. Public-sector bodies will approve these requests and facilitate re-use, ensuring that the conditions in Article 5 are upheld. These conditions should be non-discriminate, proportionate, and objectively justified, in addition to not restricting competition. Public-sector bodies must ensure data remains protected, for example by anonymising personal data or modifying commercial confidential data – additional competent bodies providing technical support can assist with this. Obligations to access and re-use data within a secure processing environment provided by the public-sector body may be imposed. In terms of third country transfers, Recital 16 notes requirements: the third country re-user must comply with the obligations in the proposal and to do so, should also accept the jurisdiction of the MS public-sector body that permitted re-use.

There is **flexibility** in the re-use mechanism. Where using anonymised or modified data wouldn't match the needs of the re-user, Recital 11 allows on-premises or remote re-use of the data in a securing environment. Also, in instances where public-sector bodies can't grant access to certain data for re-use; they must assist those seeking the data with acquiring the data subject's consent.

***Maybe you're wondering how re-using protected public-sector data will affect you as an individual?***

Think of the impact access and re-use of protected healthcare data could have, for example. Gaining access to more data could lead to improvements in healthcare, from providing better treatments and curing certain diseases. The Commission estimates that up to the economic value of data could increase by up to **€11 billion by 2028** from effectively re-using public sector data.

***EDPB-EDPS concerns***

While increased data re-use may be considered “revolutionary”, concerns have nonetheless been raised. In a 2021 EDPB-EDPS Joint Opinion, the importance of processing personal data in accordance with GDPR principles was expressed. The EDPB-EDPS highlighted that even if public sector bodies can grant or refuse access for re-use of protected data under Article 5, re-use of personal data is only permissible if the **purpose limitation principle** is respected as per Articles 5(1)(b) and 6 GDPR. It's worth noting that the overall aim of the DGA: the more data sharing, the better, might be at odds with fundamental GDPR principles.



*So, let's examine this in more depth:*

Data can only be used for another purpose if it meets the criteria of **“compatible further**

**processing” specified in Article 6(4)(a-e) GDPR.** This means that the new purpose must be compatible with the original purpose. The Opinion noted that the conditions in **Article 5 DGA didn't provide any indication of satisfying the Article 6(4) requirement.** Indeed, it is difficult to ascertain what an additional legal basis may be, with the closest connection made found in Article 5(3) DGA. This allows public sector bodies to impose an obligation to re-use only pre-processed data if they are anonymised/pseudonymised and commercially confidential information is deleted. This could be seen as a nod to the “existence of appropriate safeguards” in Article 6(4)(e) GDPR.

It could be difficult to determine whether the legal basis pursuant to Article 6 GDPR would be met if there is nothing explicitly stated in the Act, and the EDPB-EDPS strongly suggested clarifying this. However, on the Act's adoption on 30 May 2022, there was no reference in Article 5 that the provisions under Article 6 GDPR must be proven regarding data re-use. Article 1(2) does however state that the Regulation is without prejudice to specific provisions in other EU laws regarding re-use of certain categories of data - **could this be interpreted as deferring to the GDPR?**

***Aim 2: (Third Party) Data Intermediation Services***

The second aim of the Act focuses on the private sector and the regulation of data intermediation services (Articles 9-14). They are envisioned as an alternative model to Big Tech platforms who hold a significant degree of market power (Recital 22), and will ideally create a more competitive environment (Recital 33). Article 2(11) provides a catch-all term, defining this as a service:

***“which aims to establish commercial relationships for the purposes of data sharing”***

i.e., connecting individuals/companies with data users. In short, this means providers of these

services will securely organise and exchange data as a **neutral body** to foster better trust in data-sharing, which has been an issue in the past, preventing the scale up of these services. They should be intermediaries only, acting in the best interests of the data holder and not using the exchanged data for other purposes. They must be legally separated from any other services they provide - if they aren't stand-alone services. Providers of data intermediation services are obliged to notify the competent authority of their intention and must meet the requirements stipulated in Article 11(a)-(o). To note, data intermediation services already in operation have until 2025 to comply with the DGA.



There are three types of data sharing services under Article 9(1):

1. Intermediaries facilitating **B2B (business to business) data-sharing**, between data holders and data users
2. Intermediaries facilitating **C2B (consumer to business) data-sharing**, between data subjects and data users
3. Data cooperative services, which **help data subjects or MSMEs realise their rights** with respect to data processing, helping them negotiate terms with data users and enabling them to engage in discourse about processing purposes and conditions.

An example of an intermediary service given by the Commission is DAWEX, a French global data marketplace that connects companies interested in re-using data with data suppliers in a transparent manner on its platform. All transactions must be done through them, ensuring a fairer environment for data sharing. It describes itself as “a mixture of Ebay, Amazon and AirBnB for data”.

### ***How will the Commission ensure that these data intermediary services don't in turn create a monopoly like that of Big Tech platforms?***

Open Future EU points out that there is a contradiction in the concept of intermediary services: even though they have separated data provision, intermediation, and use, these services providing a “novel European way” of data governance (Recital 25) are still based on the idea of a platformed business model. Under the DGA, competition will likely foster between service providers, with Article 11(3) indicating that these services may charge a fee for its services. However, providers who don't charge a fee will likely struggle to sustain their business model without resorting to monetisation. This in turn creates the risk of a growing for-profit model, returning to large platform dominance across these services and reducing the possibility of decentralisation. Despite these concerns, the idea of regulating neutral data intermediaries should hopefully enable the restoration of trust in these services from end-users, fostering a competitive environment whilst providing a boost to the data economy.

### **Aim 3: Data Altruism**

The last primary aim of the Act is to encourage the concept of **data altruism** (Articles 15-22). Article 2(16) defines it as the “voluntary sharing of data”, based on the consent of the data subject or permission of the data holder, without reward. For the subject, this entails consent to process their personal data while for the holder it considers the use of their non-personal data, using a common European consent form for

data altruism, handled by registered data-altruism organisations. This concept aims to make data available for what the Act considers “objectives of general interest” (think healthcare, combatting climate change, providing public services, scientific research, etc.) - as provided for in national law. The arrangements and conditions on this are further explained in Article 16.

The European Parliament explains data altruism simply as a way for people to contribute by using data for the public good, although **it’s presently unclear how the EU will motivate individuals to contribute their data on this voluntary basis**. In an AlgorithmWatch paper, Dr Winfried Veil argues that the additional registration requirements, obligations, forms, and authorities will make the establishment of these organisations burdensome and unappealing. It remains to be seen whether this concept will take off after the implementation of the Act.

### **Conclusion**

Despite the arguable issues with the legal basis for re-use pursuant to Article 6(4) GDPR, the Act has been adopted as it stands and will be fully applicable in September 2023. It will be interesting to see how in practice the conditions for re-use align with the GDPR, how data intermediaries will create a more competitive marketplace, and whether data altruism will function without a clear incentive for the organisations. On a more positive note, the implementation of the DGA will ensure that there will be better access to data, strengthening Europe’s digital sovereignty and increasing the value of data for the benefit of the economy and society.

*Check back here for our second instalment of this blog post series: Breaking Down the Strategy for Data with our next post on the **Data Act**.*

**The views expressed in this blog are those of the authors and not necessarily those of EIPA.**