Data Governance Act explained

The economic and societal potential of data is enormous: it can enable new products and services based on novel technologies, make production more efficient, and provide tools for combatting societal challenges. In the area of health, for example, data can contribute to providing better healthcare, improving personalised treatments and helping cure rare or chronic diseases. It is also a powerful engine for innovation and new jobs, and a critical resource for start-ups and SMEs.

However, this potential is not being realised. Data sharing in the EU remains limited due to a number of obstacles (including low trust in data sharing, issues related to the reuse of public sector data and data collection for the common good, as well as technical obstacles).

In order to truly capitalise on this enormous potential, **it should be easier to share data in a trusted and secure manner**.

The Data Governance Act (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act) (DGA) is a cross-sectoral instrument that aims to regulate the reuse of publicly/held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes. Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the General Data Protection Regulation (GDPR) applies. In addition to the GDPR, inbuilt safeguards will increase trust in data sharing and reuse, a prerequisite to making more data available on the market.

Reuse of certain categories of data held by public sector bodies

What are the key goals?

The Open Data Directive (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX%3A32019L1024) regulates the reuse of publicly/available information held by the public sector. However, the public sector also holds vast amounts of **protected data** (e.g. personal data and commercially confidential data) that cannot be reused as open data but that could be reused under specific EU or national legislation. A wealth of knowledge can be extracted from such data without compromising its protected nature, and the DGA provides for rules and **safeguards** to facilitate such reuse whenever it is possible under other legislation.

How does it work in practice?

- **Technical requirements for the public sector**: Member States will need to be technically equipped to ensure that the privacy and confidentiality of data is fully respected in reuse situations. This can include a range of tools, from technical solutions, such as anonymisation, pseudonymisation or accessing data in secure processing environments (e.g. data rooms) supervised by the public sector, to contractual means such as confidentiality agreements concluded between the public sector body and the reuser.
- **Assistance from the public sector body**: If a public sector body cannot grant access to certain data for reuse, it should assist the potential reuser in seeking the individual’s consent to reuse their personal data or the data holder’s permission whose rights or interests may be affected by the reuse. Furthermore, **confidential information** (e.g. trade secrets) can be disclosed for reuse only with such consent or permission.
- To have even more publicly held data available for reuse, the DGA limits reliance on **exclusive data reuse agreements** (whereby a public sector body grants such an exclusive right to one company) to specific cases of public interest.
- **Reasonable fees**: public sector bodies may charge fees for allowing the reuse as long as those fees do not exceed the necessary costs incurred. In addition, public sector bodies should incentivise the reuse for scientific research and other non-commercial purposes as well as by SMEs and start-ups, by reducing or even excluding charging.
- A public sector body will have up to **2 months** to take a decision on a reuse request.
- Member States can choose which **competent bodies** will support the public sector bodies granting access to the reuse for example by providing the latter with a secure processing environment and by advising them on how to best structure and store data to make it easily accessible.
- To help potential reusers **find relevant information** on what data is held by which public authorities, Member States will be required to set up a **single information point**. The Commission created the European register for protected data held by the public sector (ERPD (https://data.europa.eu/data/datasets?superCatalogue=erpd&locale=en)), a searchable register of the information compiled by national single information points in order to further facilitate data re-use in the internal market and

beyond.

Data intermediation services

What are the key goals?

Many companies currently fear that sharing their data would imply a loss of competitive advantage and represent a risk of misuse. The DGA defines a **set of rules** for providers of data intermediation services (so-called data intermediaries, such as data marketplaces) to ensure that they will function as trustworthy organisers of data sharing or pooling within the Common European Data Spaces. In order to increase trust in data sharing, this new approach proposes a model based on the neutrality and transparency of data intermediaries whilst putting individuals and companies in control of their data.

How does it work in practice?

The framework offers an alternative model to the data-handling practices of the Big Tech platforms, which have a high degree of market power because they control large amounts of data.

In practice, data intermediaries will function as neutral third parties that connect individuals and companies with data users. While they may charge for facilitating the data sharing between the parties, they cannot directly use the data that they intermediate for financial profit (e.g. by selling it to another company or using it to develop their own product based on this data). Data intermediaries will have to comply with strict requirements to ensure this neutrality and avoid conflicts of interest. In practice, this means that there must be a structural separation between the data intermediation service and any other services provided (i.e. they must be legally separated). Also, the commercial terms (including pricing) for the provision of intermediation services should not be dependent on whether a potential data holder or data user is using other services. Any data and metadata acquired can be used only to improve the data intermediation service.

Both stand-alone organisations providing data intermediation services only and companies that offer data intermediation services in addition to other services could function as trusted intermediaries. In the latter case, the data intermediation activity must be strictly separated, both legally and economically, from other data services.

Under the DGA, data intermediaries will be required to notify the competent authority of their intention to provide such services. The competent authority will ensure that the notification procedure is non-discriminatory and does not distort competition and will confirm that the data intermediation services provider has submitted the notification containing all required information.

Upon receipt of such a confirmation, the data intermediary can legally start to operate and use the label ‘data intermediation services provider recognised in the Union’ in its written and spoken communication, as well as the common logo (https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union). Those authorities will also monitor compliance with the data intermediation requirements and the Commission keeps a central register of recognised data intermediaries (https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services).

Data altruism

What are the key goals?

Data altruism is about individuals and companies giving their consent or permission to make available data that they generate – voluntarily and without reward – to be used for objectives of general interest. Such data has enormous potential to advance research and develop better products and services, including in the fields of health, environment and mobility.

Research indicates that while in principle there is a willingness to engage in data altruism, in practice this is hampered by a lack of data-sharing tools. As such, the goal of the Data Governance Act is to create trusted tools that will allow data to be shared in an easy way for the benefit of society. It will create the right conditions to assure individuals and companies that when they share their data, it will be handled by trusted organisations based on EU values and principles. This will allow the creation of pools of data of a sufficient size to allow data analytics and machine learning, including across borders.

How does it work in practice?

Entities that make available relevant data based on data altruism will be able to register as ‘data altruism organisations recognised in the Union’. These entities must have a not-for-profit character and meet transparency requirements as well as offer specific safeguards to protect the rights and interests of citizens and companies who share their data. In addition, they must comply with the rulebook (at the latest 18 months after it comes into force), which will lay down information requirements, technical and security requirements, communication roadmaps and recommendations on interoperability standards. The rulebook will be developed by the Commission, in close cooperation with data altruism organisations and other relevant stakeholders.

The entities will be able to use the common logo (https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union) designed for this purpose and can choose to be included in the public register of data-altruism organisations. An EU-level register of recognised data altruism organisations (https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations) has been set up by the Commission, for information purposes.

A common European consent form for data altruism will allow the collection of data across Member States in a uniform format, ensuring that those that share their data can easily give and withdraw their consent. It will also give legal certainty to researchers and companies wishing to use data based on altruism. This will be a modular form, which can be tailored to the needs of specific sectors and purposes.

European Data Innovation Board

What are the key goals?

As provided in the DGA, the Commission established the European Data Innovation Board (EDIB) (https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3903) to facilitate the sharing of best practices, in particular on data intermediation, data altruism and the use of public data that cannot be made available as open data, as well as on the prioritisation of cross-sectoral interoperability standards.

How does it work in practice?

The EDIB includes representatives from the following entities:

- Member State competent authorities for data intermediation
- Member State competent authorities for data altruism
- the European Data Protection Board
- the European Data Protection Supervisor
- the European Union Agency for Cybersecurity (ENISA)
- the European Commission
- the EU SME Envoy/representative appointed by the network of SME envoys
- other representatives of relevant bodies selected by the Commission through a call for experts.

The list of EDIB members is available here: Register of Commission expert groups and other similar entities (europa.eu) (https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3903).

EDIB will have the power to propose guidelines for Common European Data Spaces, for example on the adequate protection for data transfers outside of the Union.

International data flows

What are the key goals?

The European strategy for data of February 2020 acknowledged the importance of having an open, yet assertive approach towards international data flows.

International data transfers can unlock the significant socioeconomic potential of the vast amount of data generated within the EU, thereby increasing the international competitiveness of the Union in the global arena, while contributing to economic growth, which is crucial especially in the post-COVID recovery era.

While the DGA plays a key role in strengthening the open strategic autonomy of the European Union, it also contributes to creating trust and confidence in international data flows.

How does it work in practice?

Whereas the GDPR has put in place all the necessary safeguards in the context of personal data, it is thanks to the DGA that similar safeguards exist for access requests from third country governments in the context of non-personal data.

These safeguards concern all scenarios and provisions laid down by the DGA, namely for public sector data, data intermediation services and data altruism constellations. The reuser in the third country will need to ensure the same level of protection with respect to the data in question as the level of protection ensured in EU law, as well as accept the respective EU jurisdiction.

If judged necessary, the Commission may adopt additional adequacy decisions for the transfer of public protected data for re-use when it comes to an access request with respect to non-personal data from a third country. These adequacy decisions will be similar to the adequacy decisions related to the transfer of personal data under the GDPR.

Additionally, the DGA empowers the Commission to make model contract clauses available for public sector bodies and re-users for scenarios where public sector data is involved in data transfers with third countries.

Source URL: *https://digital-strategy.ec.europa.eu/policies/data-governance-act-explained*