MASTT2040

THHINKBV 2024

Data Governance Act

The Data Governance Act (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act) aims to provide a framework to enhance trust in voluntary data sharing for the benefit of businesses and citizens. This will make it easier to share data in a trusted and secure way. The goal is to enable data sharing to create new products and services, make production more efficient, and provide tools to address societal challenges such as healthcare.

Already the Open Data Directive (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024) regulates the re-use 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 re-used as open data but could be re-used under specific EU or national legislation. A wealth of knowledge can be extracted from this data and the aim of the Data Governance Act is thus to provide rules and safeguards to facilitate such re-use whenever it is possible under other legislation.

There are, however, a number of obstacles to data sharing, a key one being a lack of trust. The act regulates the re-use 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. The act covers both personal and non-personal data. Within this personal data is covered under the General Data Protection Regulation (GDPR). The Data Governance Act provides similar safeguards for access requests from third countries in the context of non-personal data. These safeguards apply to public sector data, data intermediation services and data altruism constellations. A re-user from a third country will need to ensure the same level of protection as the EU level of protection as well as accept the respective EU jurisdiction. Model contract clauses will be available for public sector bodies and re-users for scenarios where public sector data is transferred to third countries. The Commission may also adopt additional adequacy decisions for the transfer of public protected data for re-use if an access request for non-personal data comes from a third country.

Under the act Member States will need to be technically equipped to ensure that the privacy and confidentiality of data is fully respected in re-use situations. This can be provided by a range of tools, such as anonymisation, pseudonymisation or accessing data in secure processing environments (e.g. data rooms) supervised by the public sector, and contractual means such as confidentiality agreements between the public sector body and the re-user.

The DGA limits the use of exclusive data re-use agreements to single companies to maximise the reuse of data for public interest. It also limits the charging of fees to data to “reasonable fees” which are aimed to cover the costs incurred in sharing. Public sector bodies will be encouraged to

incentivise the re-use of data (with reduced fees or free access) for scientific research and other non-commercial purposes as well as to provide the data to SMEs and start-ups. To make the process quicker a public sector body will need to make a decision on sharing the data within 2 months. If a public sector body is unable to grant access to certain data for re-use, it should assist the potential re-user in seeking the individual's or data holder's consent to re-use their data. Confidential information (e.g. trade secrets) can be disclosed for re-use only with permission.

Competent bodies will be chosen by Member States to support public sector bodies to grant access to data by providing a secure processing environment and by advising on how to best structure and store data for easy access. Potential re-users also need to know what data is available and so Member States will also set up a single information point. The Commission has created a European Register for Protected Data (ERPD) to provide a searchable register of the information compiled by national single information:

(https://data.europa.eu/data/datasets?superCatalogue=erpd&locale=en)

Data Intermediation Services

The fear of many companies is that they will lose competitive advantage by sharing data, and even worse there is a risk of misuse if the data. The DGA defines a set of rules for providers of data intermediation services (data intermediaries and data marketplaces) to ensure that they will function as trustworthy organisers of data sharing or pooling within the common European data spaces. A model based on the neutrality and transparency of data intermediaries is used to engender trust. Key to the act is that individuals and companies maintain control of their data. In practice, data intermediaries will act as neutral third parties that connect individuals and companies with data users.

Intermediaries can charge for facilitating data sharing between the parties, however, they will not be allowed to directly use the data for financial profit either by developing their own product or by selling the data to another company. They will need to comply with strict requirements to ensure neutrality and avoid conflicts of interest via strict separation legally of the data intermediation service and other services they provide.

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. This will result in the label 'data intermediation services provider recognised in the Union' being given to the company and its registration in a central register of recognised data intermediaries.

An example of this is Deutsche Telekom which provides a Data Intelligence Hub marketplace which allows companies to securely manage, provide and monetize things like production data, in order to optimise processes or value chains. Telekom takes the role of a neutral trustee and guarantees data sovereignty through decentralised data management. Currently more than 1,000 users from over 100 different companies are active on the platform.

Data Altruism

Individuals and companies are being encouraged to adopt data altruism by making their data voluntarily available with consent or permission to be used in the public interest. The aim is to use this free data to advance research and develop better products and services, in a variety of areas such as health, environment and mobility. Data altruism requires trusted data sharing tools and the Data Governance Act aims to enable these based on EU values and principles. The intention is to create pools of data which can be used for data analytics and machine learning. A common logo will be used to badge companies that are recognised as data altruism organisations and these will be listed in an EU-level public register. These will need to be not-for-profit and meet transparency and safety requirements to protect the rights and interests of citizens and companies who share their data. In addition, they must comply with a rulebook which is being developed by the Commission in cooperation with data altruism organisations and other stakeholders. These rules will lay down information requirements, technical and security requirements, communication roadmaps and recommendations on interoperability standards. A common consent form will be used to allow collection of data in a uniform format covering different sectors.

European Data Innovation Board

To promote the aims of the DGA, the Commission has also established the European Data Innovation (https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3903) to facilitate the sharing of best practices with respect to data intermediation, data altruism and the use of public data, as well as on the prioritisation of cross-sectoral interoperability standards. 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 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.