Implementing the Data Governance Act – guidance document

Contents

The purpose of this document is to provide practical guidance to stakeholders in implementing the provisions under the Data Governance Act. It not a legally binding document nor does it represent the formal position of the Commission. Please note that this is a 'living' document which may be updated over time.

The Data Governance Act (Regulation (EU) 2022/868) is a cross-sectoral instrument that provides a framework to enhance trust in voluntary data sharing for the benefit of businesses and citizens. It includes measures to:

- regulate the reuse of certain publicly held data that is subject to the rights of others ('protected data', such as personal data or commercially confidential data),
- boost data sharing through the regulation of providers of data intermediation services,
- encourage the sharing of data for altruistic purposes, and
- establish the European Data Innovation Board to facilitate the sharing of best practices.

CHAPTER I – General provisions

Chapter I explains what the Data Governance Act (DGA) regulates and contains the definitions. Both personal and non-personal data are in scope of the DGA, and where personal data is concerned, the General Data Protection Regulation (GDPR) and ePrivacy rules apply additionally. While the formulation that the DGA is without prejudice to these two regimes already implies that the rules of the GDPR and of the ePrivacy Directive are not modified, the legislator chose to reinforce this provision by stating that in the event of any legal conflict between a DGA rule and a GDPR or ePrivacy rule, the latter rules shall prevail. Furthermore, the DGA clarifies that the role of the supervisory authorities under the GDPR are not touched upon. This means that in any situation where rules, rights and obligations under the GDPR or ePrivacy Directive are to be interpreted, data protection authorities or the authority competent for ePrivacy are competent. This can lead to a need to collaborate between the competent authority set up on the basis of Article 13 and 23 DGA and the competent data protection authority.

Below is a selection of terms, with a simplified explanation, that will help the reader navigate the provisions.

Article 2 – a selection of definitions

- ***consent*** means the consent given by an individual regarding the processing of their personal data; for this concept, the DGA refers to the definition in the GDPR;
- ***permission***, on the other hand, refers to the permission given by an individual or an entity regarding the use of non-personal data pertaining to them;
- ***data subject*** means an individual to whom data relates and who can be identified, directly or indirectly, in particular by reference to an identifier; for this concept, the DGA refers to the definition in the GDPR;
- ***data holder*** means an entity or an individual that is not the data subject and that has the right to grant access to or to share certain (personal or non-personal) data. For example, a company that holds data about its manufacturing yield is the data holder of that data;

- ***data intermediation service*** means a service that connects an undetermined number of data subjects and data holders with data users to establish a commercial data-sharing relationship. Services for closed user groups in particular are outside the scope of the DGA;
- ***data altruism*** means the voluntary sharing of data for objectives of general interest without the intention of generating profit;
- ***public sector body*** is defined as covering authorities and bodies governed by public law. Research-performing organisations that are set up as public sector bodies or governed by public law are included in this definition. Public undertakings are outside the scope.

CHAPTER II – Re-use of certain categories of protected data held by public sector bodies

The Open Data Directive regulates the re-use of publicly available information held by the public sector that can be shared without any specific restriction or limitation. For databases containing personal data or commercially confidential information, this means that they can only be shared as open data once anonymised or aggregated in a manner that no potential re-user can re-identify persons or confidential information. In practice, however, this means that many databases that are held by the public sector are not re-usable. A wealth of knowledge can be extracted from such data, without compromising its protected nature, through the use of certain techniques. The DGA provides for rules and safeguards to facilitate such re-use.

It is important to note that the DGA does not create a right for re-use or a new legal basis in the sense of the GDPR for the re-use of personal data (***Article 1***). This means that Member State or Union law determines whether a specific database or register containing protected data is open for re-use in general. However, where the re-use of protected, publicly held data is allowed under Union or Member State law, it must be done in accordance with the conditions laid down in this Chapter of the DGA.

Key provisions

- Article 3: categories of protected data
- Article 4: prohibition of exclusive arrangements
- Article 5: conditions for re-use, including in international situations
- Article 6: fees
- Article 7: competent bodies to assist public sector bodies
- Article 8: national single information points and the European single access point

Categories of protected data

These conditions apply when a re-use request concerns the following categories of data (***Article 3***):

(a) commercially confidential data such as trade secrets or know-how,
(b) statistically confidential data,
(c) IPR protected data of third parties, or
(d) personal data, insofar as such data falls outside the scope of the Open Data Directive.

Article 3 further specifies the categories of data that are not concerned by this Chapter. For example, data held by public undertakings, museums, schools and universities are out of scope. There are also two situations in particular where this Chapter does not apply to publicly held, protected data: (1) data that are protected for reasons of public security, defence or national security, and (2) data that public sector bodies hold for purposes other than the performance of their defined public tasks. Finally, the exchange of data between researchers for non-commercial scientific research purposes is also out of scope of this Chapter.

Prohibition of exclusive arrangements

Article 4 – In order to ensure that publicly held data is available to anyone who would like to re-use it, the DGA limits the reliance on exclusive data re-use agreements. Consequently, a public sector body may grant such an exclusive right to one company only in specific cases of public interest. Such an agreement may not last longer than 1 year and, for the sake of transparency, the public sector body must inform the public about its decision to grant such an exclusive right and the reasoning behind it. Exclusive re-use agreements that were concluded before 23 June 2022 must be terminated by 24 December 2024.

Conditions and procedure for requesting re-use

Article 5 lays down the requirements regarding the conditions for re-use and imposes obligations both on public sector bodies and on re-users, whilst ***Article 9*** specifies the request procedure.

The conditions must be non-discriminatory (i.e. re-users that share the same characteristics should be treated equally), transparent, proportionate and objective, and they shall not be used to restrict competition. They should also be designed in a way that promotes access to data by SMEs and start-ups, and that promotes scientific research.

What public sector bodies must do:

- make the conditions and the request procedure **publicly available** via the single information point (see ***Article 8***);
- to prevent illegitimate re-use of data, make sure that the **protected nature of data is preserved**. The DGA does not prescribe the exact measures that must be taken to this end;
- **confidentiality**: the public sector body must require that the re-user adheres to a confidentiality obligation that prohibits the re-user from disclosing any information obtained through the re-use that might jeopardise the rights and interests of third parties;
- **decision**: the public sector body must take a decision on the re-use request within 2 months after receiving the request. If the request is exceptionally extensive or complex, the public sector body may extend this period by a maximum of 30 days and inform the applicant of the extension and of the underlying reasons.

In addition, the DGA provides for the following:

- on the **scope of the data** eligible for re-use: this would be defined in national law;

- on **assistance to potential re-users**: if the public sector body cannot allow the re-use, for example because the protected nature of personal data or of a trade secret cannot be guaranteed, the re-user can try and seek GDPR-compliant consent or permission directly from the data subjects or entities concerned through the public sector body;
- on the **means to provide access**: the DGA strongly recommends making use of available technologies to strike the balance between the value of re-using the data and the need to preserve privacy:
  - one such technique is **anonymisation**. This is well known for personal data, but *mutatis mutandis* could also apply to commercially confidential information;
  - another is to allow access to the data only via a **secure processing environment**, i.e. an IT environment controlled by the public sector body. This would allow the public sector body to determine what re-users can see and which elements of the data or what type of calculations they can make on the data so that they cannot reconstruct the original data. Also, measures would need to be taken by the operator of the secure processing environment to control the outgoing analytical results. Such secure environments have been in use for years, notably by statistical offices (e.g. https://ec.europa.eu/eurostat/web/microdata). Depending on the technical capabilities, access could be restricted to re-users coming on-premises. Access through a VPN connection could also be possible.

What re-users must do:

- **privacy**: re-users are prohibited from re-identifying data subjects. This is an active obligation as re-users must not only refrain from the re-identification but also take technical and operational measures to prevent it;
- **notification obligation**:
  - **personal data**: in case of the re-identification of a natural person, the re-user must inform the public sector body that granted the re-use permission. In accordance with Article 33 of the GDPR, additional data breach reporting obligations are likely to apply (for the re-user, for the public sector body, depending on the roles of each in the case in question);
  - **non-personal data**: in case of the non-authorised use of non-personal data, the re-user must inform the legal persons concerned. For example, if the protected nature of a trade secret is compromised, the re-user must inform the company that owns that trade secret. Where necessary, the re-user can get assistance from the public sector body that initially granted the re-use permission.

International transfers of data

Whilst re-users may transfer **personal data** to third countries only in compliance with Chapter V of the GDPR, the DGA sets rules for international transfers of **non-personal data (*Article 5*)**. By default, the transfer of non-personal data for re-use is allowed, provided that the re-user complies with certain requirements. The process has two stages:

1. **inform the public sector body in advance**: when requesting re-use, the potential re-user must inform the public sector body about its intention to transfer and of its purpose;

2. **contractual commitment** whereby the re-user commits to ensure that the protection of the data is not breached even after the transfer and accepts the jurisdiction of the Member State of the public sector body in case any dispute arises related to this commitment.

To facilitate safe international transfers, the Commission is empowered do the following:

1. propose **model contractual clauses** that public sector bodies may use in their transfer contracts with re-users;
2. when a large number of re-use requests coming from particular countries justify it, adopt '**equivalency decisions**' designating these third countries as providing a level of protection of trade secrets or IP that can be considered equivalent to that provided in the EU. Such decisions will reassure public sector bodies and will also help re-users, as they would not have to rely on the contractual commitments taken on a case-by-case basis when they want to transfer protected, publicly held non-personal data for re-use to a third country with such a decision. It is important to note, however, that such decisions are not a pre-requisite for international transfers, which can happen in the absence of equivalency decisions, provided that the re-user takes up the contractual commitments mentioned above;
3. adopt **conditions** that should be applied to **transfers of highly sensitive non-personal data**: certain categories of non-personal data may be considered as highly sensitive in EU legislative acts (c.f. designation of certain non-personal health data as 'highly sensitive' by the European Health Data Space Regulation – final number of the article pending). For example, certain public health data (e.g. anonymised and aggregated healthcare-related administrative data, including dispensation, claims and reimbursement data) could constitute such a category. In cases where the transfer of such data to third countries would pose a risk to the public policy objectives of the EU (in this example, public health) and in order to assist the public sector bodies granting re-use permissions, the Commission will set additional conditions that must be met before such data can be transferred to a third country.

Redress

Anyone directly affected by a re-use decision taken by a public sector body shall have the right to complain or seek a judicial remedy in the Member State of that public sector body (***Article 9***).

Fees

According to ***Article 6***, public sector bodies may charge fees for allowing re-use. Fees should only cover the costs arising from making the data available for re-use, such as costs of anonymisation or of providing a secure processing environment. This would include the costs of handling requests for re-use. Member States must publish a description of the main categories of costs and the rules used for the allocation of costs.

To encourage the re-use of data for innovation and for the public good, public sector bodies should consider offering re-use at a discounted rate or free of charge when re-use is requested for not-for-profit purposes or for scientific research. The same should be considered when SMEs and start-ups request re-use.

Competent bodies to assist public sector bodies granting re-use

Member States should designate one or more competent bodies whose function is to support public sector bodies that grant re-use **(*Article 7*)**. The competent bodies shall have adequate legal, financial, technical and human resources to carry out the tasks assigned to them, including the necessary technical knowledge. To fulfil this task, competent bodies may, for example, provide public sector bodies with guidance and technical support on how to best structure and store data to make those data easily accessible. They may also provide technical support for pseudonymisation or offer a secure processing environment in which data from different registries could be processed. As the competent bodies will not supervise the public sector bodies and will thus not exercise public powers, the DGA does not set specific requirements as to their legal status or form. For example, a department of a public sector body can be designated as such a competent body, or a Member State may decide to set up a completely new entity for this purpose. Member States can also decide that the competent body has the mandate to allow re-use itself.

Single information point – a one-stop shop

To make it easier to find out what data are available for re-use, Member States will have to designate a single information point **(*Article 8*)** which will transmit enquiries and requests to relevant public sector bodies and will maintain an asset list with an overview of available data resources (metadata). The single information point may be connected to local, regional or sectoral information points where they exist. At EU level, the Commission created the European Register for Protected Data held by the Public Sector (ERPD), 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.

CHAPTER III – Requirements applicable to data intermediation services providers

The DGA defines a **set of rules** for providers of data intermediation services that connect the supply and demand of data (for the purpose of this document, 'data intermediaries' will be used to express data intermediation services providers that fall within the scope of the DGA). These rules will also ensure that such intermediaries will function as trustworthy organisers of data sharing or pooling within the Common European Data Spaces. Entities that provide data intermediation services within the meaning of ***Article 10*** will have to comply with the rules set out in this Chapter, including registration with the relevant competent authority.

Key provisions

- Article 11: provides details of the notification process for data intermediaries
- Article 12: lays out the conditions to be fulfilled by data intermediaries
- Articles 13 and 14: each Member State shall designate one or more competent authority(ies) to carry out the tasks related to the notification procedure and to monitor the compliance of providers

What is (not) a data intermediation services provider?

Article 2(11) defines a 'data intermediation service' as a service aiming to establish commercial relationships for data sharing between an undetermined number of individuals or companies on the one hand and data users (individuals or entities) on the other. This can be done through technical (platforms/ apps where data can be stored), legal or other means.

According to ***Article 10***, data intermediaries may include bilateral or multilateral exchanges of data or the creation of platforms or databases for the exchange or joint use of data, as well as the establishment of other specific infrastructures for the interconnection of data holders with data users. While remaining open to novel technical mechanisms and business models, the notion of 'data intermediation services provider' was inspired by the following existing or emerging models:

1. data marketplaces that match supply and demand within or even outside any organised ecosystem;
2. orchestrators of ecosystems, e.g. (Common European) Data Spaces in which the participants accept certain rules (legal and/ or technical) of participation in the ecosystem;
3. data pools established by companies or natural persons where the benefits of the use of the pool are directly given back to the contributors of the pool;
4. data 'cooperatives' or 'unions' that have a mechanism of collective deliberation or decision-making on the use of data that members of the cooperative or union have; and
5. 'personal data wallet or cloud' services, i.e. services offered to individuals that can store personal data about them currently held by other companies and allow the processing of such data by third parties, either within their 'personal data cloud' ('bringing the algorithm to the data' in order to maximise data privacy) or by transmitting such data to that third party.

The DGA explicitly excludes the following services from the definition of data intermediary services providers:

1. services that obtain data from data holders and aggregate, enrich or transform the data to add substantial value to it and to license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;
2. services that focus on the intermediation of copyright-protected content (e.g. certain online content-sharing service providers);
3. services used in a closed group;
4. IoT platforms, understood as platforms established by manufacturers of IoT objects in order to continuously communicate with the objects they manufacture, exchange data and potentially propose added-value services;
5. data-sharing services offered by public sector bodies in order to facilitate either the re-use of protected data held by public sector bodies in accordance with the DGA or the use of any other data, insofar as those services do not aim to establish commercial relationships. This exempts data exchange platforms set up by public sector bodies purely for digitising interactions between them and individuals and business. This does not mean that public sector bodies cannot have a role in data-sharing ecosystems. It means that they have to notify intermediation services only when such services have the intention to facilitate data

exchanges of a commercial character and are thus comparable to privately offered data intermediation services, making it fair to make them subject to the same rules.

One important consequence of these rules is that the business model of the data intermediary may not depend on any onward sharing of the data by the intermediary to recipients not chosen by the user of the service ('data holder'). This is a deliberate means to create trust of the users of such services. It will reassure them that only the users (data holder and user of the data) can benefit from the value of such data and that data holders are in full control of the parties with whom they want to share the data.

Secondly, data intermediation services may be possible between individuals that seek to make their personal or non-personal data available, and potential data users. This includes making available the technical or other means to enable such services (B2C).

Thirdly, services of data cooperatives (data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structure) would have as main objective to support their members in the exercise of their rights with respect to certain data.

What must data intermediaries do?

Article 11 – Intermediaries will be required to **notify** the competent authority of their intention to provide such services. They may start the intermediation activities upon the notification.

***Article 11(2)* –** Data intermediaries with establishments in more than one Member State shall be under the jurisdiction of the Member State in which it has its main establishment, without prejudice to Union law regulating cross-border actions for damages and related proceedings.

Data intermediaries must:

- submit a **notification** to the competent authority for data intermediaries; the following information should be included in the notification (paragraph 6):
  (a) the name of the data intermediary;
  (b) the data intermediary's legal status, form, ownership structure, relevant subsidiaries and, where the data intermediary is registered in a trade or other similar public national register, registration number;
  (c) the address of the data intermediary's main establishment in the Union, if any, and, where applicable, of any secondary branch in another Member State or that of the legal representative;
  (d) a public website where complete and up-to-date information on the data intermediary and the activities can be found, including as a minimum the information referred to in points (a), (b), (c) and (f);
  (e) the data intermediary's contact persons and contact details;
  (f) a description of the data intermediation service that the data intermediary intends to provide, and an indication of the categories listed in Article 10 under which such data intermediary falls;
  (g) the estimated date for starting the activity, if different from the date of the notification;

- designate a **legal representative** in one of the Member States in which those services are offered (if the data intermediary is not established in the Union, but offers the data intermediation services within the Union);
- **notify** the competent authority for data intermediaries of any **changes** to the information provided pursuant to paragraph 6 within 14 days of the date of the change.

Competent authorities for data intermediaries

The competent authority for data intermediaries will ensure that the notification procedure is non-discriminatory and does not distort competition. At an intermediary's request, the competent authority must issue, within 1 week of a duly and fully completed notification, a standardised declaration, confirming that the intermediary has submitted the notification and that it contains the information referred to above.

At a data intermediary's request, the competent authority must confirm whether the intermediary complies with the notification requirements and the conditions for providing intermediation services under the DGA. Upon such a confirmation, the intermediary *may* use the label 'data intermediation services provider recognised in the Union' in its written and spoken communication, and *must* clearly display the common logo, established by the Commission, on every online and offline publication that relates to their data intermediation activities.

The competent authority shall notify the Commission of each new notification by electronic means without delay. The Commission shall keep and regularly update a public register of all intermediaries providing their services in the Union. The information referred to in ***Article 11(6)***, points (a), (b), (c), (d), (f) and (g), shall be published in the public register.

Article 12 defines the **conditions for providing data intermediation services**, enabling data intermediaries to function as neutral third parties. They cannot share the data with parties other than those chosen by the user and any data and metadata acquired can be used only to improve the data intermediation service (when processing personal data to do so, this would require a legal basis under the GDPR). Data intermediaries will have to comply with strict requirements to ensure this neutrality and avoid conflicts of interest. In practice, this means that for entities currently also offering other services, there must now be a legal separation between the entity offering the data intermediation service and the entity providing any other services (i.e. the data intermediation service should be provided through a separate legal person). 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.

According to ***Article 13***, each Member State shall **designate one or more competent authority(ies)** to carry out the tasks related to the notification procedure for data intermediaries. Member States were to notify the Commission of the identity of those competent authorities by 24 September 2023, as well as of any change to the identity of those competent authorities.

Article 14 states that the competent authorities for data intermediation services shall **monitor and supervise compliance** of data intermediation services providers with the requirements of

this Chapter. This may also happen on the basis of a request by a natural or legal person. Chapter V determines the requirements that these competent authorities must meet. ***Article 15*** specifies that recognised data altruism organisations and other organisations that engage in data altruism (but are not registered under Article 19) are not subject to Chapter III unless they aim to establish commercial relationships between an undetermined number of data holders or data subjects on one hand with data users on the other.

CHAPTER IV – Data altruism

Data altruism is about individuals and companies giving their consent or permission to make available data relating to them – voluntarily and without reward – to be used for objectives of general interest. Such objectives can include healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policymaking as well as supporting scientific research. The notion of what constitutes an 'objective of general interest' is left for national law to define, and there are differences between Member States. National rules on charitable organisations can give an indication as to whether an objective pursued by an organisation is an 'objective of general interest' in the sense of the DGA. Data subjects and data holders should be able to receive compensation related only to the costs they incur when making their data available.

The DGA aims to create trusted tools that will allow data to be shared in an easy way for the benefit of society. Entities that make available relevant data based on data altruism will be able to register as 'data altruism organisations recognised in the Union'. Such entities will have to comply with a Rulebook, which will lay down certain requirements. In addition, the Commission will develop a European data altruism consent form to allow the collection of data across Member States in a uniform format.

Key provisions

- Article 16: Member States may have in place organisational or technical arrangements, or both, to facilitate data altruism
- Article 17: each Member State will keep a public national register of recognised data altruism organisations, and the Commission will maintain a register at EU level
- Articles 18-22: there are certain requirements an entity must meet with in order to register as a recognised data altruism organisation
- Articles 23-24: each Member State will designate one or more competent authorities responsible for its public national register and for monitoring compliance of recognised data altruism organisations with the requirements
- Article 25: the Commission, in consultation with relevant stakeholders, will develop a European data altruism consent form

According to ***Article 16***, Member States may have in place organisational or technical arrangements, or both, to facilitate data altruism. In practice, as mentioned in recital 45, this could include making available user-friendly tools for data subjects or data holders for giving consent or permission for the altruistic use of their data, the organisation of awareness campaigns or a structured exchange between competent authorities on how public policies (such as improving traffic, public health and combating climate change) benefit from data altruism.

The EDIB could be a forum for competent authorities to share information on their national data altruism practices and policies (recital 54) and could provide a channel for Member States to inform the Commission thereof.

Article 17 requires Member States to set up a register of recognised data altruism organisations. This could be a simple website listing the recognised data altruism organisations within a Member State and containing the information provided in ***Article 19(4)***. The Commission shall keep and regularly update a public register at EU level, compiling information from the national registers.

What is a recognised data altruism organisation?

Entities that are registered as recognised data altruism organisations *may* use the label 'data altruism organisation recognised in the Union' and *must* display the common logo, established by the Commission, clearly on every online and offline publication that relates to their data altruism activities. The logo will be accompanied by a QR code linked to the EU register.

Article 18 lists the requirements to be met to qualify as a recognised data altruism organisation as well as the information to be included in applications and the national registers. To qualify, a data altruism organisation needs to operate on a not-for-profit basis and be legally independent from any entity that operates on a for-profit basis. The data must be used for an objective of general interest. Furthermore, its data altruism activities must be done through a structure that is functionally separate from its other activities. The intention behind this is to ensure a high level of trust in recognised data altruism organisations.

Recognised organisations can collect data directly from individuals/ companies using the consent form or process data collected by others. They can also allow the data they collected to be processed by third parties.

The DGA obligations only apply to recognised data altruism organisations who have chosen to register with the competent authority.

In order to register as a recognised data altruism organisation, an organisation must (***Article 19***) submit an application to the competent authority containing certain information (e.g. legal status, registration number, statutes), in order to ensure transparency on the entity itself.

Whenever an organisation that is not established in the Union wishes to become a recognised data altruism organisation and apply for the label, it must also designate a legal representative in one of the Member States in which those services are offered.

Furthermore, a data altruism organisation must inform the competent authority of any changes to the information provided within 14 days of the date of the change.

Once registered in the Member State in which it is established (or, for organisations established in more than one Member State, where it has its main establishment), the registration is recognised throughout the EU.

Competent authorities for data altruism organisations

The competent authority must register the organisation in its national register within 12 weeks of the receipt of application. It must also notify the Commission of any registration or changes to existing registrations.

Article 20 lays out the transparency requirements that recognised data altruism organisations need to adhere to, in particular as regards the records they need to keep as well as the minimum information to be included in the annual activity report that they submit to the competent authority.

Article 21 details how registered organisations are required to protect the rights of data subjects and data holders, notably in terms of the information to be provided, purpose limitation and obtaining consent to process personal data. This article also includes measures to ensure the secure storage and processing of data.

Additional oversight mechanisms could include ethics councils or boards, including representatives from civil society, to ensure that the data controller maintains high standards of scientific ethics and protection of fundamental rights.

Recognised data altruism organisation will have to comply with the Rulebook once such Rulebook is adopted. In laying out detailed rules on a number of elements, including technical and security requirements as well as communication roadmaps and interoperability standards (***Article 22***), the Rulebook aims to increase trust in recognised data altruism organisations. It is being prepared by the Commission, in close cooperation with all stakeholders – including data altruism organisations and competent authorities. Recognised data altruism organisation will have to comply with the Rulebook at the latest 18 months after its entry into force. Organisations may already register with their competent authority; there is no need to wait until the Rulebook has been adopted.

Member States were to notify the Commission of the identity of their competent authority by 24 September 2023 (***Article 23***). The competent authorities should be selected on the basis of their capacity and expertise. They should not be linked to any data altruism organisations, and should be transparent and impartial.

Specific requirements for competent authorities are laid out in ***Article 26*** (Chapter V) (see below).

Article 24 details how competent authorities are expected to monitor the compliance of recognised data altruism organisations, for example through requests for information and, if

necessary, appropriate and proportionate action. When a recognised organisation is active in more than one Member State, the competent authorities of those Member States should cooperate on the abovementioned tasks.

The last article in this Chapter (***Article 25***) provides a basis for the Commission, in consultation with relevant stakeholders (including the European Data Innovation Board), to develop a European data altruism consent form in order to facilitate the granting and withdrawal of consent. The objective is to create a modular form that can be customised to specific sectors and for different purposes, and that is in compliance with the GDPR (in particular its Article 7) where personal data is concerned.

CHAPTER V – Competent authorities and procedural provisions

The competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations have to comply with ***Article 26*** requirements. The requirements relate to the structuring, cooperation, independence and transparency of those authorities. As these competent authorities have supervisory powers, the independence requirement concerns also their top management and personnel. The same authority can be nominated as both the competent authority for data intermediation services and for the registration of data altruism organisations.

Article 27 gives the right to anyone to lodge a complaint with the relevant competent authority in matters that fall in the scope of the DGA. The competent authority receiving the complaint must inform the complainant of the progress of the proceeding and of the decision taken as well as inform them of the available judicial remedies.

Any affected individual or legal person has the right to an effective judicial remedy regarding a legally binding decision of the competent authority designated under the DGA (***Article 28***).

CHAPTER VI – European Data Innovation Board

To help make the DGA work in practice, the Commission has established the European Data Innovation Board (EDIB) in the form of a Commission expert group. The EDIB facilitates the sharing of best practices, in particular on data intermediation, data altruism and the use of publicly held data that cannot be made available as open data, as well as on the prioritisation of cross-sectoral interoperability standards (***Articles 29 and 30***). For example, the EDIB has the power to propose guidelines for Common European Data Spaces on the adequate protection for data transfers outside of the Union.

The EDIB consists of representatives from relevant national and EU authorities and bodies as well as from representatives of other relevant bodies.

It includes a subgroup made up of representatives from the competent authorities.

The Commission (CNECT.G) chairs the meetings of the EDIB and provides the secretariat.

CHAPTER VII – International access and transfers

While the DGA may help strengthen the open strategic autonomy of the European Union, it also contributes to creating trust and confidence in international data flows. It offers protection concerning non-personal data in the context of jurisdictional reach of third countries. Whereas Chapter V of the GDPR has put in place all the necessary safeguards in the context of personal data, ***Article 31*** of the DGA creates similar safeguards for access requests from third countries' governmental authorities or courts relating to 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 organisations.

Article 31 requires that the relevant parties take all the reasonable technical, legal and organisational measures, including contractual arrangements possible in order to prevent access by third countries' governments (or courts) to non-personal data held in the European Union that would be in conflict with EU or national law. Relevant parties in this context are the public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation. It is not intended to cover other situations of international transfers.

There are two exceptions to this rule:

First, the decision or judgement of a third country court, tribunal or a decision by an administrative authority to transfer or give access to non-personal data is based on an international agreement (a mutual legal assistance treaty). Such an international agreement must be in force between the requesting third country and the Union or between the requesting third country and a Member State.

Second, in the absence of such an international agreement and where compliance with such a decision would risk putting the addressee in conflict with Union law or national law, transfer to or access to such data by that third-country authority will take place exclusively under specific conditions. These conditions are the following: (a) the third-country system requires the reasons and proportionality of such a decision or judgment to be set out and to be specific in character; (b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and (c) the competent third-country court, tribunal or administrative authority issuing the decision or judgment is empowered to take duly into account the relevant legal interests of the data provider as protected by EU or national law (international law principle of 'comity').

The public sector body, the natural or legal person to which the right to re-use the data was granted, the data intermediation services provider or the recognised data altruism organisation must inform the data holder about any request from a third country to access its data before complying with this request. The only exceptions from this rule include requests for law enforcement purposes or the preservation of the effectiveness of the law enforcement activities.

CHAPTER VIII – Delegation and committee procedure

This Chapter sets the procedural rules that the Commission will have to follow when adopting delegated and implementing acts pursuant to the DGA, including:

- model contractual clauses for contracts relating to the international transfers of non-personal, protected data, to be used by re-users and public sector bodies (implementing act, Article 5);
- equivalency decisions declaring certain third countries to provide a level of protection of data equivalent to that of the EU (implementing act, Article 5);
- conditions applicable to the transfers of highly sensitive non-personal data to third countries (delegated act, Article 5);
- logo for data intermediation service providers in the Union (implementing act, Article 11)
- logo for data altruism organisations recognised in the Union (implementing act, Article 17);
- Rulebook for data altruism (delegated act, Article 22);
- European data altruism consent form (implementing act, Article 25).

CHAPTER IX – Final provisions

According to ***Article 34***, it is the responsibility of Member States to lay down the rules on penalties applicable to infringements of the obligations regarding transfers of non-personal data to third countries, notification obligation, conditions for providing data intermediation services and conditions for the registration as a recognised data altruism organisation. Member States must notify the Commission of their specific rules and measures on their national set of penalties. Such rules and measures are expected to take into account the recommendations of the European Data Innovation Board.

In accordance with ***Article 35***, the Commission will carry out an evaluation of the Regulation by 24 September 2025. Then a report will be submitted on the findings of the evaluation to the European Parliament, the Council and the European Economic and Social Committee. Member States will be required to provide the Commission with all the information necessary for the preparation of the evaluation report. The report will be accompanied, where necessary, by any relevant legislative proposals.

The report itself must assess:

(a) the application and functioning of the rules on penalties;
(b) the level of compliance of the legal representatives of data intermediation services providers and recognised data altruism organisations that are not established in the Union with this Regulation and the level of enforceability of penalties imposed on them;
(c) the type of data altruism organisations and an overview of the objectives of general interests for which data are shared in view of establishing clear criteria in that respect.

Article 36 provides detailed amendments *vis-à-vis* the entry 'Starting, running and closing a business' in the table in Annex II to Regulation (EU) 2018/1724.

Article 37 specifies transitional arrangements regarding data intermediaries: entities that have been providing intermediation services referred to in Article 10 at the time of the entry into

force of the DGA have to comply with the obligations set out in Chapter III of the Regulation by 24 September 2025.

Article 38 explains that the Regulation enters into force on the twentieth day following its publication in the Official Journal, i.e. on 23 June 2022. It became applicable 15 months after the date of entry into force, i.e. on 24 September 2023.