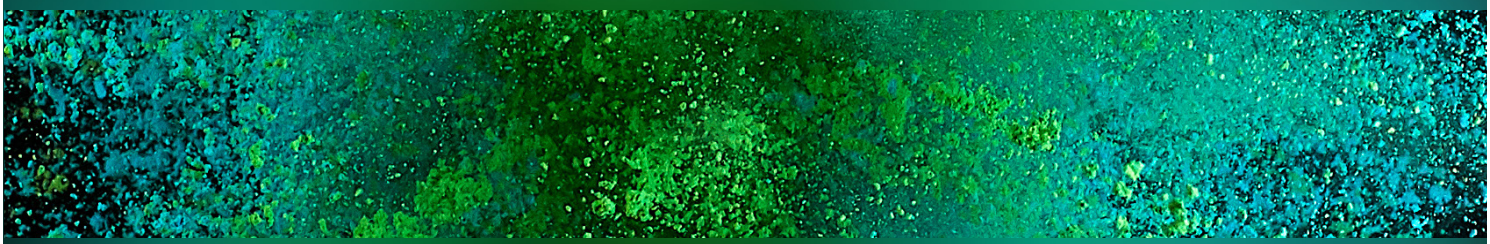
CLIFFORD

CHANCE



AN OVERVIEW OF THE EU DATA GOVERNANCE ACT

AN OVERVIEW OF THE EU DATA GOVERNANCE ACT

The **Data Governance Act** (DGA), which creates a framework for increased data availability and re-use within the European Union (EU), entered into force on 23 June 2022. Following a grace period of 15 months, it will be applicable from 24 September 2023. The DGA is a key pillar of the European Strategy for Data, seeking to promote the re-use of protected data held by public sector bodies. While access to such data could bring opportunities for innovation and technological advancement, as well as facilitate business models relating to data intermediation and data altruism, attention will need be paid to the conditions and safeguards for data sharing and re- use in the DGA. In this article we explore key aspects of the DGA.

Context and purpose of the EU Data Governance Act

Data has become central to our day-to-day lives and, as such, become a resource for economic and societal growth, competitiveness, efficiency, and innovation.

In recent years, the volume of data generated has grown exponentially, yet there has been limited data sharing despite its various societal and economic benefits. Three primary issues have been identified by the European Commission (EC) as hindering effective data sharing:

- Lack of appropriate data sharing structures;
- Technological obstacles; and
- Low trust in data re-users and data collection for the common good.

In order to address these concerns, in November 2020, the EC published its proposal for the DGA as part of the European Strategy for Data, which aims to develop a single market for data that will support EU data sovereignty and global competitiveness.

The stated aim of the DGA is to improve the availability of data by fostering trust in data intermediaries and by strengthening data-sharing mechanisms.

These goals are envisaged to be achieved by implementing the following set of measures:

- Mechanisms to foster access to and the re-use of certain categories of data held by public sector bodies that cannot be made available as open data due to the protections that apply to the data.

- Measures to help ensure that data intermediaries will function as trustworthy organisers of data sharing or pooling in the common European data spaces.
- Measures to encourage citizens and businesses to make their data available for "the common good", such as certain research, healthcare, education, or scientific purposes.
- Measures to facilitate data sharing, specifically to enable the use of data across sectors and for certain purposes.

Scope of the DGA

The DGA establishes conditions and frameworks for the re-use, within the EU, of data held by public sector bodies which are protected due to commercial or statistical confidentiality, intellectual property rights of third parties or the protection of personal data.

While the DGA does not set out in more detail the circumstances in which it applies to organisations outside the EU, some of its provisions and recitals indicate that it has an extraterritorial reach. In particular, any entity that is not established within the EU but which offers services within the EU and which meets the requirements to qualify as a data altruism organisation or as a data intermediary under the DGA, has to appoint a legal representative in one of the Member States where those services are offered. This means that non-EU based entities wishing to participate in the data reuse frameworks established by the DGA should also pay attention to the provisions of the DGA.

Mechanism for re-using certain protected data controlled by public sector bodies

The DGA complements and strives to fill in the gap left open by the Open Data Directive, which addresses only the re-use of public data and does not address protected data. In order to do this, the DGA focuses on the establishment of safeguards for the re-use of protected data held by public sector bodies, such as the State, regional or local authorities, or bodies governed by public law. According to the definition in the DGA, re-use encompasses the use by natural or legal persons of data controlled by public sector bodies both for commercial and non-commercial purposes. However, the DGA does not create an obligation for public sector bodies to allow the re- use of protected public sector data. Rather, the DGA merely offers a set of harmonized basic conditions under which such data re-use might be permitted. The DGA provides for the following measures for the access and re-use of public sector-controlled data:

- Prohibitions relating to arrangements containing an exclusive right to re- use.
- Requirements for the relevant public sector bodies to fulfil certain technical requirements to ensure that the privacy and confidentiality of data is respected during the process. This may include measures such as anonymization or pseudonymization, contractual means like confidentiality agreements, or the creation of data rooms to ensure the security of the processing environment.

- The re-use must satisfy the principles of proportionality, non-discrimination and objective justification and it must comply with intellectual property rights.
- Public sector bodies will have two months to decide on the re-use request and they may charge fees for the re-use of data, but only to an extent that does not exceed the necessary costs.
- Confidential information, such as trade secrets may only be disclosed if permission or consent has been given.

As a result of this new mechanism, public sector bodies are expected to encourage the re-use of data. An example of how data can be re-used for beneficial purposes is the practice of DAMAE Medical, a French company, that uses data made available through the French Health Data Hub to improve its technology to identify signs of skin cancer more efficiently.

Data transfer to Third Countries

In relation to transfers of personal data, the DGA defers to the GDPR. The recitals to the DGA make clear that it is not intended to prevent cross-border transfers of personal data in accordance with the GDPR and that, in event of any conflict between the DGA and any EU law on the protection of personal data, the latter prevails.

In relation to the other protected categories of data, the DGA introduces certain measures in order to safeguard the flow of data with third countries. In particular, the DGA establishes the EC's power to adopt delegated acts, where deemed necessary, that lay down the criteria for transfers to third countries. These conditions may include, amongst other things, limitations concerning the re-use of data in third countries, the categories of persons who are allowed to transfer such data to third countries and, in exceptional cases, restrictions regarding these transfers.

Furthermore, the DGA requires that a natural or legal person, who is re-using data under the DGA must inform the public sector body from whom the data is obtained of its intention to transfer such data and the purpose of that transfer at the time of requesting re-use of the data. Public sector bodies may only transfer data confidential non-personal data or data protected by intellectual property rights to a re-user intending to transfer that data to a third country if (1) the re-user contractually commits to complying with certain obligations and accepting the jurisdiction of the Member State of the transmitting public sector body, or (2) the EC has declared that the relevant third country:

- ensures protection of trade secrets and intellectual property in a way that is essentially equivalent to that in the EU;
- has legal, supervisory and enforcement arrangements that ensure such protections are effectively applied and enforced; and
- provides effective judicial redress,

The DGA also anticipates circumstances in which courts and authorities of third countries may require a public sector body, data re-user, data intermediation services provider or recognised data altruism organisation to transfer or give access to non-personal data falling within the scope of the DGA and sets conditions relating to such transfer or access.

Regulation of data intermediation service providers

The DGA offers an alternative model for data-handling practices through the concept of providers of data sharing services: data intermediaries. According to the DGA, providers of data sharing services have a key role in the data economy as they contribute to the effective pooling of data and facilitate the bilateral exchange of data. Such data intermediaries are expected to function in the public, private and third sectors as neutral third parties that will link individuals and companies with data users. Organisations offering only data intermediation services as well as companies that provide data intermediation services in addition to other services, can qualify as data intermediaries provided that, in the case of the latter, there is legal and economic separation from the other services they offer. By way of guidance, the regulation specifies that a company or organisation that wishes to qualify as a data intermediary must satisfy the following criteria:

- Their main objective must be the establishment of a business.
- They facilitate legal and technical connection between data holders and potential data users.
- They facilitate services focused on intermediating between data holders and data users.
- They offer services to data subjects with a focus on personal data as defined under the GDPR.

To ensure the safety of data, data intermediaries will be subject to strict requirements that are intended to guarantee their neutrality and prevent conflict of interest. In practice, this means that they will have to separate their data intermediation services from the other services they provide. Moreover, under the DGA, data intermediaries will also have to comply with notification requirements, as they will be required to notify their intention to provide data intermediation services to the competent authority designated by each member state to carry out the tasks related to the notification framework. The responsibility of the competent authority will be to make sure that the notification service is non-discriminatory and does not distort competition. If the data intermediary has adequately submitted the notification with all the necessary information, it will be granted confirmation which will enable the data intermediary to use the label ‘data intermediation services provider recognized in the Union’ and operate accordingly.

As one of the aims of the European digital strategy is to address the dominance of big tech companies in the flow of data, the following categories of entities cannot be considered providers of data sharing services under the regulation:

- Cloud service providers;
- Data brokers;
- Services with a focus on the intermediation of content – e.g. social network companies, search engines;
- Data exchange platforms;
- Platforms developed in the context of objects and devices connected to the IoT (IoT platforms); and
- Data sharing services that are meant to be used by a closed group of data holders and users.

For non-EU entities it will be more complicated to qualify as a data intermediary as they will have to meet further standards such as registration with a regulatory authority and placing their data sharing services in a separate legal entity.

Data altruism

"Data altruism" under the DGA means the voluntary sharing by individuals and companies of data generated by them – without receiving any reward – so that it may be used for objectives in the general public interest. To reach this aim, the DGA introduces a common European data altruism consent form that will facilitate the collection of data across member states in a uniform format, while guaranteeing that consent can be given and withdrawn easily. This is expected to give legal certainty to researchers and companies who wish to use this data., and create a trusted framework that will encourage data altruism and facilitate the sharing of data for societal benefits, such as helping further the research in certain areas such as healthcare and climate change, or developing better functioning products and services in areas of public interest. The DGA also envisages the development of a "Rulebook" specifying requirements relating to data altruism (such as technical and security requirements) and the establishment of recognised data altruism organisations, which must fulfil certain criteria (including operating on an independent, not-for-profit basis) and be registered in a public national register.

Establishment of the European Data Innovation Board

As the last piece of the puzzle, the DGA puts forward the creation of the European Data Innovation Board (the Board) to help the EC develop a consistent approach to data intermediaries, data altruism, cross-sectoral data sharing, and the re-use of protected data, and to facilitate cooperation between relevant competent authorities. The Board will have the form of an expert group and will consist of the representatives from various entities, such as the competent authorities of each member state, the EC, the European Data Protection Board and the representatives of data spaces and specific sectors (e.g. health, transport, agriculture or statistics), and other relevant stakeholders.

Monitoring compliance with the DGA and possible penalties

Under the DGA, each Member States must appoint competent authorities for (1) supporting public sector bodies in the granting or refusing of data access for re-use (2) data intermediation services and (3) the registration of data altruism organisations. Competent authorities for data intermediation services and the registration of data altruism organisations are required to monitor and supervise compliance with the provisions of the DGA falling within their remit. and will be empowered to take certain actions (such as requiring the suspension or cessation of data sharing service, or removal of a data altruism organisation from the public national register) or, in relation to data intermediation services, impose dissuasive financial penalties (including penalties with retroactive effect) in relation to breach of the relevant DGA provisions. In other cases, each Member State is required to lay down rules on penalties applicable to infringements of particular provisions of the DGA. Such penalties must be proportionate, effective and dissuasive.

How does the DGA relate to the EU GDPR?

The DGA applies to "any digital representation of acts, facts or information", including personal data. However, the DGA does not create any new legal basis for data processing under the EU General Data Protection Regulation (GDPR) and is not intended to prevent cross-border transfer of personal data in accordance with the GDPR. Whenever personal data is concerned, if there is any inconsistency between the DGA and the GDPR, the GDPR prevails.

How does the DGA relate to the EU Data Act?

The EU's proposed regulation on harmonised rules on fair access to and use of data, commonly referred to as the "Data Act", another key pillar of the European Strategy for Data, is currently making its way through the EU legislative process (see our article: "**The Data Act: A proposed new framework for data access and porting within the EU**").

Both the DGA and the Data Act seeks to promote data accessibility and reuse withing the EU. The DGA does so through setting out broad frameworks for data to move freely within the EU, in particular through setting conditions for re-use of protected public sector data and providing for trusted mechanisms for access to data. The DGA does not, however, create obligations to share data. The draft Data Act complements the DGA by specifying who can use certain types of privately held data and under what circumstances, introducing mechanisms and standards to enable companies and individuals to exercise more control over data generated by their use of IoT devices or stored in data processing services such as cloud services. This includes introducing rights for companies and individuals to require that data holders make certain data available to them or to third parties in certain circumstances. The draft Data Act also introduces a framework for access by public sector bodies to data held by private data holders in cases of "exceptional need".

AUTHORS

Andrei Mikes
Senior Associate
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Rita Flakoll
Senior Associate
Knowledge Lawyer
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

CONTACTS

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Fernando Irurzun
Partner
Madrid
T: +34 91 590 4120
E: fernando.irurzun@cliffordchance.com

Gunnar Sachs
Partner
Düsseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Susanne Werry
Counsel
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

Thomas Voland
Partner
Düsseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Andrea Nagy co-authored this article.

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2211-003787