Volume 1, Number 1 January–February 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 1, No. 1 January–February 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL (ISSN 2995-7486) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

The photo on this journal's cover is by Gaël Gaborel—A Picture of the Earth on a Wall—on Unsplash

Cite this publication as:

The Global Regulatory Developments Journal (Fastcase)

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and others interested in global regulatory developments.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at morgan.wright@vlex.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2995-7486

What You Should Know About the EU Data Governance Act

Alice Portnoy and Wim Nauwelaerts*

In this article, the authors provide an overview of the EU's new Data Governance Act and discuss how the new law may impact businesses on both sides of the pond.

Data has become an essential resource for any modern economy. There is, however, a common perception that most data is not used efficiently and only a small group of businesses is able to extract value from it. To address this issue, EU legislators have adopted the Data Governance Act (DGA), which is now applicable.

In February 2020, the European Commission (EC) released its European Strategy for Data, designed to explore new ways to handle and create value from data. The strategy lays the foundation for a single market for data within the European Union, where data can circulate freely for the benefit of all while respecting the EU's fundamental values and principles.

As part of this strategy, the EC has taken several legislative initiatives with a view to facilitating data sharing across sectors and EU Member States. In May 2022, the EC adopted the first new law in this context: the DGA, which became effective on September 24, 2023. The DGA introduces new definitions, concepts, and enforcement mechanisms for the re-use of data by both public and private organizations. The DGA also includes new rules intended to encourage the voluntary sharing of data by individuals and organizations and establishes a regulatory framework for organizations acting as data-sharing intermediaries. The DGA's ultimate goal is to foster a new type of data governance that enables all stakeholders to (re)use data for innovative purposes.

The DGA is complemented by the Data Act, another legislative initiative that is part of the European Strategy for Data. The Data Act aims to optimize the accessibility and use of data generated by connected devices in the European Union (such as smart watches) by clarifying who can use such data and create value from it.

The Global Regulatory Developments Journal / January–February 2024, Vol. 1, No. 1, pp. 43–50.

ISSN 2995-7486.

The DGA is intended to supplement and interact with other EU laws that regulate data use, such as the General Data Protection Regulation (GDPR) and the Digital Markets Act. Organizations subject to the DGA may also have to consider these other regulatory frameworks.

Focal Areas of the DGA

The main goal of the DGA is to boost the development of reliable data-sharing platforms within the European Union and across sectors. To that end, EU legislators have focused on four key topics:

1. Re-use of data held by public sector bodies (PSBs) such as state, regional, or local authorities or other bodies and associations governed by EU public law.
2. Data intermediation services (DIS) that facilitate data sharing.
3. A new "data altruism" framework that encourages individuals and organizations to voluntarily share their data for the common good.
4. Rules to protect non-personal data against unlawful access by foreign authorities.

Re-Use of Data Held by Public Sector Bodies

In 2019, the EC adopted the Open Data Directive to regulate the re-use of publicly available information held by the public sector in each EU Member State. However, this directive does not cover the re-use of data that has a protected status and can therefore not be re-used as open data. This includes commercially sensitive data, data subject to confidentiality requirements, data protected by intellectual property rights, and individuals' personal data.

The DGA is meant to address this gap by setting the conditions under which the re-use of protected data held by PSBs (which can include both personal data as defined by the GDPR and non-personal data) is permitted. In practice, individuals, organizations, or companies will have the possibility to submit requests to PSBs for re-use of protected data, and the PSBs will have to decide whether they want to grant or refuse access to the data for re-use purposes.

In addition, PSBs will have to comply with a range of requirements, such as the obligations to:

- Refrain from granting exclusive rights relating to the re-use of protected data;
- Inform the public about the conditions for re-use of protected data (which must be non-discriminatory, transparent, proportionate, and objectively justified based on the sensitivity of the protected data);
- Implement technical measures to safeguard protected data that will be re-used (i.e., through anonymization, aggregation, or modification of protected data);
- Ensure that remote access to protected data only occurs within a secure processing environment (controlled by the PSB itself); and
- Impose confidentiality obligations on re-users of protected data.

The DGA's rules on re-use of protected data held by PSBs may create opportunities for a wide spectrum of sectors and industries that so far had only limited access to public sector information. In the area of medical research, for example, it is expected that new studies and trials will benefit from the ability to access (and use) existing data that is held by PSBs. There is a recent use case in France, where a public interest group named the French Health Data Hub has made re-use of medical data its main mission. Based on training data made available through the hub, a medical device company in France was able to develop technology that can help identify potential signs of skin cancer at an early stage.

Data Intermediation Services

Individuals and organizations are typically reluctant to make their (personal or non-personal) data available to others for various reasons, including potential abuse or competition concerns. The DGA attempts to address these concerns by enabling specialized organizations to provide DIS, with a view to facilitating the exchange of data. This can be achieved through technical, legal, or other means, such as by setting up data-sharing platforms between:

- Individuals or organizations that wish to grant access to or share personal or non-personal data (data subjects or data holders), and
- Those that want to have access to personal or non-personal data and re-use it for commercial or non-commercial purposes (data users).

The new DIS framework encourages voluntary data sharing and tries to increase trust among data subjects, data holders, and data users. Organizations that want to provide DIS services (in the form of data information management systems, data marketplaces, or data-sharing pools, for example) will have to comply with strict requirements to guarantee their independence and neutrality toward the parties that are exchanging data. For instance, the DGA requires DIS providers offering various types of services to ensure a strict separation between the DIS and any other services they provide to customers. Also, DIS providers will not be able to use the data exchanged via their data-sharing platform for their own purposes—other than improving their data-sharing facilities or detecting fraud.

Before offering their data-sharing services to potential customers, DIS providers will have to submit a notification to the competent supervisory authority (i.e., the authority of the EU Member State of their main establishment). Organizations that are not established in the European Union but wish to offer DIS within the European Union are required to designate a legal representative for DGA purposes in one of the EU Member States where they intend to offer their services.

The DIS concept may entice organizations to share, under strict conditions and via a neutral trustee, commercially sensitive information with non-profit organizations and even commercial companies. For example, a prominent telecommunications provider in Germany has set up a dedicated data-sharing platform for companies to upload, manage, and share production data for (process and supply chain) optimization purposes.

Data Altruism

The DGA also aims to encourage individuals and organizations to make their data available for general interest purposes (e.g., to improve health care systems, combat climate change, or optimize

the provision of public services) voluntarily and without reward. With that objective, the DGA introduces a new regime of "data altruism," which enables individuals and organizations to easily and safely authorize the altruistic use of their data by others.

Under this new regime, it will be possible to share data via recognized data altruism organizations (RDAOs) that pursue not-for-profit goals. These RDAOs will be subject to a range of strict requirements to make sure that individuals and organizations that make their data available can trust that the data will only be used to serve the public interest. For instance, RDAOs will have to comply with reporting and transparency obligations and implement specific measures to safeguard the rights of individuals and organizations sharing their data.

Organizations that want to become an RDAO will have to register with the competent supervisory authority in the relevant EU Member State. Like DIS providers, RDAOs without an establishment in the European Union will have to designate a legal representative for DGA purposes that is located in the European Union. Registered RDAOs will be able to use the European RDAO logo when communicating about their new activities and may be listed in the EU public record of RDAOs.

The DGA's provisions on data altruism are likely to fuel research activities in the European Union, particularly in the medical field. They will, for instance, enable individuals to make their health-related data available to researchers in a secure manner and for specific purposes that serve the public interest. For example, a German public health institute developed an application to help track the spread of COVID-19 in Germany. Thanks to citizens willing to share their health data (collected mainly through fitness bracelets or smart watches), the institute was able to paint a comprehensive picture of COVID-19 infection patterns. In another case, residents of the Spanish city of Barcelona agreed to share insightful data on the levels of noise, air pollution, temperature, and humidity in their city (collected through the use of sensors inside and outside their homes) with start-ups, cooperatives, and local communities.

Data Transfers

Transfers of personal data to recipients in countries outside the European Union are heavily restricted under the GDPR. The

DGA supplements the GDPR's data transfer regime by imposing restrictions on cross-border transfers of non-personal data.

The DGA requires PSBs, data users, DIS providers, and RDAOs to implement reasonable technical, legal, and organizational measures to prevent unlawful international transfers of or governmental access to non-personal data held in the European Union if that transfer or access would create a conflict with EU law or EU Member State law. This means that a "conflict assessment" will need to be conducted before the data can be transferred.

A foreign decision or judgment requiring transfer of or access to non-personal data held in the European Union can only be acted upon if it is supported by an international agreement, such as a mutual legal assistance treaty. If there is no such agreement and complying with the decision or judgment would risk putting the PSB, data user, DIS provider, or RDAO in conflict with EU law or EU Member State law, the data transfer or access can take place only if strict conditions are met (as set out in the DGA). Only minimum data should be provided in response to a request from a foreign court or authority and, when possible, the relevant data holders should be informed of the request.

In addition, the DGA imposes specific data transfer requirements on data users that wish to transfer non-personal protected data outside the European Union. They will have to:

- Inform, in advance, the relevant PSBs about their intention to transfer non-personal protected data outside the European Union;
- Commit to respect the specific conditions imposed by the PSBs;
- Submit to the jurisdiction of the EU Member State of the PSB that allowed the re-use of protected data; and
- In some cases, obtain data holders' authorization before transferring protected data.

Enforcement

Each EU Member State will have to designate a supervisory authority to oversee compliance with the DGA. These authorities will have the power to take enforcement action against organizations that do not comply with their DGA obligations. This includes

imposing administrative fines. The DGA leaves it up to the EU Member State authorities to determine the amounts of potential fines, taking into consideration the nature, gravity, and duration of the DGA violation, as well as any aggravating and mitigating circumstances.

The DGA also establishes a new expert group, the European Data Innovation Board (EDIB), which will be in charge of advising and assisting the EC in developing guidelines and best practices for PSBs handling requests for the re-use of protected data and to support DIS providers and RDAOs in complying with their obligations under the DGA. The EDIB is also tasked with providing guidance to EU Member States and their competent supervisory authorities and facilitating cross-border cooperation.

Interplay Between the DGA and the GDPR

The DGA regulates access to and re-use of data, both personal and non-personal, whereas the GDPR deals with processing of personal data only. Organizations that engage in sharing, accessing, or re-using personal data (or mixed sets of personal and non-personal data) under the DGA may therefore have to ensure compliance with the provisions of the GDPR as well. This means, for example, making sure that there is a valid legal basis for processing personal data (e.g., individuals' consent), complying with reporting requirements in case of a personal data breach, or implementing a data transfer tool if personal data is sent outside the European Union.

How Can the DGA Impact Businesses in the United States?

The DGA can be of relevance to any business that wants to make good use of the new data-sharing opportunities that the new law is expected to create. They would be well-advised to assess to what extent the DGA may apply to their activities and, if necessary, design a DGA compliance plan. Also, businesses in the United States that, for example, wish to offer DIS services or act as an RDAO will have to consider the DGA requirement to appoint a legal representative in the European Union. In addition, the DGA's data transfer restrictions may impact businesses in the United

States that are on the receiving end of non-personal data that is transferred by, for instance, a DIS provider in the European Union. In order to have access to that data, U.S. businesses may be asked to agree to contractual obligations and implement measures that aim to ensure the same level of data protection as under EU law.

Conclusion

In summary:

- The DGA introduces new rules to encourage sharing of personal and non-personal data across sectors;
- The DGA supplements other EU laws that regulate data use, such as the GDPR and the Digital Markets Act; and
- Businesses in the United States that receive non-personal data under the DGA might face data transfer restrictions.

Note

* The authors, attorneys with Alston & Bird LLP, may be contacted at alice.portnoy@alston.com and wim.nauwelaerts@alston.com, respectively.