EU Data Governance Act (DGA)

TaylorWessing

Purpose

The DGA aims to increase trust in data sharing, creates new EU rules on the neutrality of data marketplaces and facilitates the reuse of certain data held by the public sector, e.g. certain health, agricultural or environmental data. It also sets up common European data spaces in strategic domains, such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration, and skills.

Scope

The DGA establishes the conditions and frameworks for the re-use of data held by EU public sector bodies, covering data protected by various forms of confidentiality and personal data rights. It also has extraterritorial reach, affecting non-EU entities offering services within the EU, who must appoint legal representatives in EU Member States.

Application

The DGA came into force on 23 June 2022, and became applicable in September 2023 after a 15-month grace period.

Reuse of certain categories of publicly held data	Public sector bodies hold vast amounts of data protected by third-party rights (such as trade secrets, personal data, or intellectual property) that cannot be used as 'open data' (under the Open Data Directive) but could be reused under specific EU or national rules. Whenever such reuse is allowed, public sector bodies must comply with the reuse conditions laid down by the DGA. These conditions should be non-discriminatory, transparent, proportionate, justified, and made publicly available. The DGA also prohibits public sector bodies from entering into agreements that grant exclusive rights for the reuse of certain data unless justified and necessary for providing a service or product in the general interest that would otherwise not be possible. Such exclusive arrangements should comply with competition law, be limited to 12 months, and be subject to regular review. They must also be transparent, compliant with state aid rules, and published online. Public sector bodies must ensure that the protected nature of data is preserved by anonymising personal data and modifying or aggregating commercially confidential information. Access and reuse of data should be conducted remotely within a secure processing environment controlled by the public sector body or on the physical premises with high security standards if remote access cannot be secured. Public sector bodies have the right to verify the process, means, and results of data processing by the re-user to ensure the integrity of data protection and may prohibit the use of results that compromise the rights and interests of third parties. Re-users intending to transfer non-personal data protected by intellectual property rights to a non-EU country must comply with DGA-specific rules and contractually commit to obligations protecting the data even after transfer, accepting the jurisdiction of the courts of the Member State of the transmitting public sector body.
Data intermediation services	The DGA regulates providers of data intermediation services, which are neutral third parties that connect data holders with data users. Requirements for these services ensure that data intermediaries act as trustworthy organisers of data sharing, promoting neutrality and transparency, while giving individuals and companies control over their data. Entities wishing to provide data intermediation services must comply with strict requirements to ensure neutrality and avoid conflicts of interest, maintain structural separation from any other value-added services provided, ensure price terms are independent of other services used by data holders or users, and register with a competent authority.
Data altruism	Data altruism involves individuals and companies voluntarily making their data available for the public interest without reward. This is data which has significant potential to advance research and improve products and services in health, climate action, mobility, and more. Member States may develop policies to encourage data altruism, and entities can apply to be recognised as 'data altruism organisations' at the EU level. The Commission will maintain a register of these organisations.
European Data Innovation Board (EDIB)	The EDIB, established by the EU Commission, will include representatives from national authorities, the European Data Protection Board, the European Data Protection Supervisor, the European Union Agency for Cybersecurity, the EU SME envoy, and other experts. The EDIB will advise the Commission on developing consistent practices for data reuse requests, enhancing data and data-sharing service interoperability, and enforcing requirements for data intermediation service providers.
International data flows	To protect non-personal data from unlawful access by non-EU authorities, the DGA introduces safeguards for secure data flows outside the EU. Public sector bodies, data intermediation services, and recognised data altruism organisations must take reasonable technical, legal, and organisational measures, including contractual arrangements, to prevent international transfers or governmental access to non-personal data that would conflict with Union or national law. Decisions or judgments by third-country courts requiring a data transfer will only be recognised if based on an international agreement, such as a mutual legal assistance treaty. In the absence of such an agreement, any decision by a third-country authority requiring a data transfer must meet specific criteria: it must be proportionate, specific, subject to review by a competent third-country court, and consider the legal interests of the data provider under Union law. If these conditions are met, only the minimum amount of data permissible should be provided. Furthermore, entities must inform the data holder about the request from a third-country administrative authority, unless it's for law enforcement purposes.
Penalties	Member States must establish rules on penalties for infringements regarding non-personal data transfers to third countries, notification obligations of data intermediation services, conditions for providing data intermediation services, and conditions for registration as a recognised data altruism organisation. These penalties must be effective, proportionate, and dissuasive, considering recommendations from the European Data Innovation Board. By 24 September 2023, Member States had to notify the Commission of these rules and any subsequent amendments. When imposing penalties, Member States must consider the nature, gravity, scale, and duration of the infringement, actions taken to mitigate or remedy the damage, any previous infringements, financial benefits gained or losses avoided due to the infringement, and other aggravating or mitigating factors. These criteria ensure penalties are fair and appropriate to the circumstances of each case.
Compliance and Enforcement	Member States are responsible for designating competent authorities to monitor and enforce compliance with the DGA. These authorities will oversee the registration of data intermediaries and data altruism organisations, ensure adherence to the DGA's requirements, and address any infringements. The European Data Protection Board will also ensure consistency with existing data protection frameworks, such as the EU General Data Protection Regulation (EU GDPR).