WilmerHale's Guide to the European Union's Data Act

September 2024

WILMERHALE

Attorney Advertising

A New European Legal Framework with Rules for Data Access, Switching Cloud Providers and Interoperability

What Is the Data Act and Why Does it Matter?

The Data Act (Regulation (EU) 2023/2854) is a new EU regulation providing harmonised rules on access to data, switching cloud providers and interoperability requirements across the EU.

It is widely expected that the Data Act will have a significant impact on most companies doing business in the EU and will require significant preparation.

The Data Act, which will apply from 12 September 2025 onwards, will be relevant far beyond the EU's borders, including in the UK and the U.S., where no comparable legislation exists at present.

Context and Objectives

The adoption of the Data Act takes place in the context of the EU's ambitions to boost the EU's data economy and to create a Digital Single Market. The intended role of the Data Act is to set requirements for the use and value creation of data by providing users of connected products or services with more rights, and increasing competition in digital markets, especially by strengthening SMEs' competitive position.

To that end, the Data Act defines the conditions for a right of access to product and service data generated by connected products and related services. In this context:

— The Data Act provides safeguards against unlawful third-party use, the disclosure of trade secrets and unfair contractual provisions (**Chapter 1**).

— International and third-country governmental access and transfer of nonpersonal data held in the EU is subject to restrictions. In addition, the Data Act provides for interoperability standards on providers of cloud and other data processing services to facilitate switching (**Chapter 2**).

— Noncompliance can lead to penalties set and enforced by EU countries (**Chapter 3**).

Scope

From a business perspective, most of the provisions of the Data Act will apply to data holders, i.e., typically (but not always) manufacturers of connected products and providers of related services, if they place products or services on the EU market (and to data holders making data available to data recipients in the EU), irrespective of their place of establishment. However, the Data Act's provisions on data sharing only apply to users located in the EU.

Relationship With the GDPR

The Data Act is without prejudice to the GDPR and the ePrivacy Directive 2002/58, including with regard to the powers of supervisory authorities and the rights of data subjects. The Data Act complements the rights of access and data portability under Articles 15 and 20 of the GDPR. In the event of a conflict between the Data Act and EU or national law on the protection of personal data or privacy, the law on the protection of personal data or privacy will prevail.

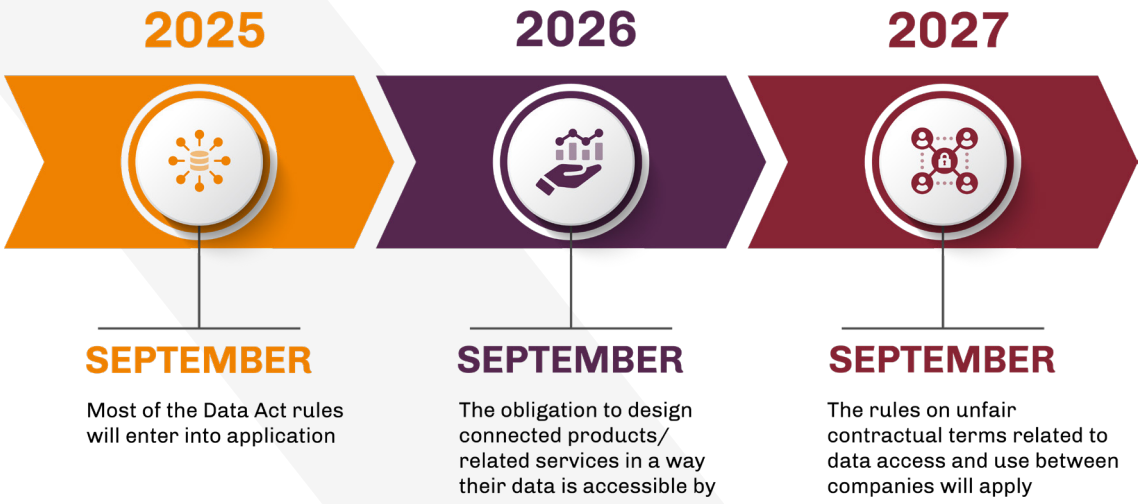
Timeline

Most of the Data Act rules will enter into application as from 12 September 2025.

The obligation to design connected products/related services in such a way that product and related service data is accessible by default will apply as from 12 September 2026.

The rules on unfair contractual terms related to data access and use between companies will apply as from 12 September 2027 to contracts concluded on or before 12 September 2025 if they are of indefinite duration, or due to expire at least on 11 January 2034.

While these may appear to be rather generous timelines, several categories of actors may face significant redesigns of their products and services, which should be initiated as soon as possible.



What You Will Find in This Guide

The European Union's Data Act is a highly complex and technical legislative text. Some of the concepts to which it refers require prior knowledge of European law and of data protection law in particular.

This guide offers a simplified presentation of the Data Act's requirements, focusing on the most relevant aspects to help companies comply with them.

To this end, this guide covers the topics listed below. For any additional information on data-related issues under EU law, **please contact our teams in Brussels, Frankfurt, and London**.

How We Can Help

WilmerHale has a leading practice in EU law and regulation, advising clients on high-profile matters in both established and emerging market sectors across a wide variety of industry sectors. With 1,000 lawyers located throughout 13 offices in the U.S., UK, Europe and Asia, we offer a global perspective to EU law issues and offer single-team transatlantic and Europe-wide services. We practice at the very top of the legal profession and offer a cutting-edge blend of capabilities that enables us to handle cases of any size and complexity.

Our European offices in Brussels, Frankfurt, Berlin are best known for high quality regulatory work before authorities and appellate work before EU Courts. Clients entrust us with complex cases because of our expertise, reliability, responsiveness, precision, and reputation with authorities. Our European team is involved in a huge number of cases in various areas of EU law, including several major data protection and competition law cases setting breakthrough principles. In addition, many of our lawyers are qualified in several jurisdictions across the EU, its neighbouring countries, and the U.S. and can handle the most complex cases in several languages at native level.

For more information on this guide or other data-related matters, please contact one of the authors.

Dr. Martin Braun

Partner
Frankfurt/Brussels

Anne Vallery

Partner-in-Charge
Brussels

Itsiq Benizri

Counsel
Brussels

Chapter 1: Data Access Rights and Obligations in the Data Act

Data access rights and obligations in the Data Act rely on four principles, which can be summarized as follows.

1. Manufacturers of connected products and providers of related services must design and manufacture/provide such products and services in a way that allows direct access to product data and related service data, including metadata.

General

— **Access to data by design and by default.** Connected products/related services must be designed and manufactured/provided in such a way that product and related service data is accessible by default. This includes the relevant metadata necessary to interpret and use the data (together, the data). Access must be easy, secure, comprehensive, structured, and provided in a commonly used and machine-readable format. Access by users must be free of charge.

— **Direct access.** When relevant and technically feasible, the data must be directly accessible to the user, which means that no data access request is needed.

Associated transparency obligations of data holders

— **Before entering into a contract for the purchase**, rent or lease of a connected product, the seller, renter or lessor (which may be the manufacturer) must provide specific information to users in a clear and comprehensible format. Examples include the type and volume of data that the product can generate; whether the product can generate data continuously and in real time; whether it can store data on-device or remotely and for how long; and how the user may access, retrieve or delete the data.

— **Similar information must be provided to users of services related to a connected product**. Additional examples include who will use the data and for what purpose, how users may request that the data be shared with a third party, and how users may end the data sharing or lodge a complaint alleging a violation of the Data Act.

2. If direct access is not possible, data holders must make the data readily available to users. Users may also request that data holders make the data available to a third party.

General

— **Data access request**. Where the data cannot be directly accessed by users, the data holder (usually the provider of a connected service) must make the data readily available to the user upon request, without undue delay. Where relevant and technically feasible, the data must be of the same quality as is available to the data holder, continuously and in real time.

— **Third parties**. Upon request by a user, or by a party acting on behalf of a user, the data holder must make the data available to a third party in the same manner as described above. While access must be free of charge for the user, this would not necessarily be the case for the third party.

Key requirements for data holders when handling data access requests

— **Do not make things complicated**. Data holders cannot make users' choices or rights unduly difficult to implement or enforce. Typically, data holders cannot offer choices in a non-neutral manner or subvert or impair users' autonomy, decision-making or choices through the structure, design, function or mode of operation of a user interface.

— **Do not ask for unnecessary information**. Data holders may ask the persons requesting access to data to provide the necessary information to confirm that they are users or third parties acting on users' behalf. Data holders cannot keep any information on users' access to the data requested beyond what is necessary for the sound execution of the access request and for the security and maintenance of the data infrastructure.

B2B contractual provisions governing data access conditions

— **Contract**. Where, in B2B relationships, a data holder is required to make the data available to a third party (data recipient), the modalities for doing so must be determined in a contract between them. Such a contract must be based on fair, reasonable, nondiscriminatory and transparent terms.

— **Do not discriminate**. Data holders cannot discriminate between comparable categories of data recipients. If a data recipient believes that it has been discriminated against, it is up to the data holder to demonstrate that this was not the case.

— **Reasonable compensation**. The data holder and the data recipient may agree that access to data will be subject to compensation. Unless the data recipient is a small or medium-sized enterprise or nonprofit organization, the compensation may include a margin, but it must remain reasonable.
The European Commission will publish guidelines on the calculation of the compensation, and EU law or EU countries' laws may provide more specific rules. In any event, data recipients must be provided with sufficiently detailed information on the calculation of the compensation.

- Examples of relevant factors to calculate the compensation include the costs incurred for making the data available and the investment in the collection and production of the data. The compensation may also depend on the volume, format and nature of the data.

— **Unfair terms**. The Data Act prohibits contractual terms concerning the access to and use of data or the liability and remedies for the breach or the termination of data-related obligations where such terms have been unilaterally imposed and are unfair. These rules provide additional specificity to the Unfair Contract Terms Directive, which safeguards consumers (but not businesses) from unfair standard contract terms in contracts for goods and services. Under the Data Act:

- A contractual term is unfair if it grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing. Typically, a contractual term is unfair if its object or effect is to exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence or if it gives that party the exclusive right to determine whether the data supplied is in conformity with the contract.
- The Data Act includes a list of terms that are presumed to be unfair. Examples include terms that allow the party that unilaterally imposed them to access and use data of the other contracting party in a way that is significantly detrimental to the legitimate interests of that party and terms that prevent that party from terminating the agreement within a reasonable time period.
- The contracting party that supplied the contractual term bears the burden of proving that the term has not been unilaterally imposed.

3. Data access and use may be restricted under certain conditions, including for security purposes and for protecting trade secrets.

Data holders may only restrict access to the data by users under certain narrow conditions

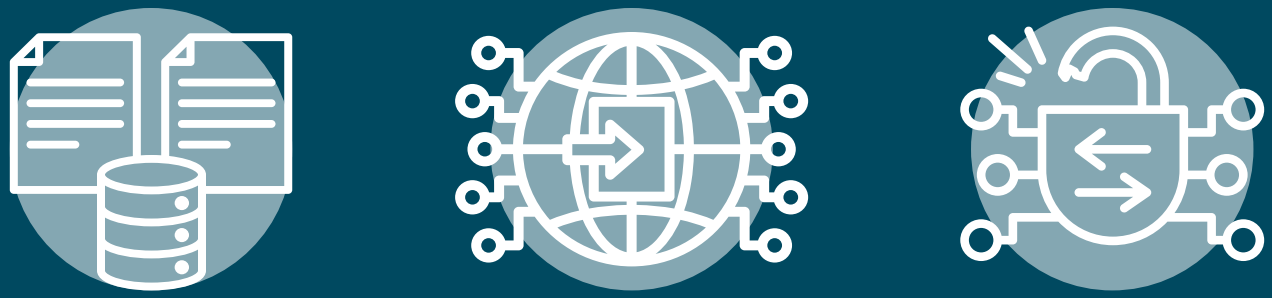
— **Security**. Users and data holders may agree on restricting or prohibiting the access, use or further sharing of data where this could undermine security requirements of the product set by the law of the EU or of an EU country and providing access would result in serious adverse effects on the health, safety or security of human beings. Data holders must notify the competent authority of any refusal to share data.

— **Trade secrets**. Trade secrets must only be disclosed if the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality, especially regarding third parties. To that end, the Data Act establishes rules designed to ensure the delicate balance between data access and the protection of trade secrets. These rules, however, remain a source of anxiety given that they aim to find a way of providing access to data and that, once the user has obtained such data, the risk of disclosure still exists.

- **Agreement-based rules**. The data holder (or the trade secret holder when it is not the data holder) must identify the data protected by trade secrets and agree with the user proportionate technical and organisational measures to preserve their confidentiality (e.g., confidentiality agreements, strict access protocols or technical standards). It will be challenging to identify appropriate measures to limit the risk of disclosure as much as possible.

- **Suspension of trade secret sharing.** If there is no agreement on the necessary measures, the user fails to implement them or the user undermines the confidentiality of the trade secrets, the data holder may withhold or suspend the sharing of trade secrets.

- **Refusal of trade secret sharing**. In exceptional circumstances, when the data holder is highly likely to suffer serious economic damage from the disclosure of trade secrets despite the measures adopted, the data holder may refuse on a case-by-case basis the request for access. Any refusal or suspension decision must be substantiated and notified to the competent authority. Thus, refusals of trade secret sharing are permitted in very limited cases and closely monitored by authorities.



Data holders may also restrict access to the data by third parties in situations where the user requests that the data is made available to a third party

— **Not on the market.** The users' right to have a data holder share the data with a third party does not apply to readily available data in the context of testing of other new products, substances or processes that are not yet placed on the market, unless use by a third party is contractually permitted.

— **No data sharing with gatekeepers**. The users' right to have a data holder share the data with a third party does not apply to the largest digital platforms offering core platform services in Europe, the so-called gatekeepers under the Digital Markets Act. This means that third parties cannot make the data they receive from data holders available to gatekeepers. The Data Act approach is surprising, since it limits users' right to choose how to make use of their data. The Data Act approach also restricts gatekeepers' freedom to compete, and it is unclear whether such a restriction is justified and proportionate, especially in circumstances where data holders are not prohibited from directly and voluntarily granting gatekeepers access to data.

— **Trade secrets.** See above.

Data holders are subject to restrictions regarding the data they have in their possession

— **Only use data if you have a contract with the user**. Data holders may only use readily available nonpersonal data on the basis of a contract with a user.

— **Do not use data to derive insights**. Data holders can only use readily available nonpersonal data on the basis of a contractual agreement with users. Data holders cannot use such data to derive insights about the economic situation, assets and production methods of, or the use by, users that could undermine users' commercial position in the markets in which they are active. The same applies to third parties unless they have given permission to such use and have the technical ability to easily withdraw that permission at any time.

— **Data sharing with third parties**. Data holders cannot make available nonpersonal product data generated by a product to third parties for purposes other than the fulfilment of their contract with users. Where relevant, data holders should contractually bind third parties not to further share data received from them.

Users are subject to restrictions regarding their own use of the data obtained from a data holder

— **Do not use data to derive insights**. Users cannot use the data obtained pursuant to a data access request to derive insights about the manufacturer or the data holder.

— **Unfair competition**. Users cannot use the data obtained pursuant to the Data Act to develop a connected product that competes with the connected product from which the data originates, or share the data with another third party with that intent.

Third parties that receive the data following a request by the user to a data holder are subject to restrictions regarding the use of that data

— **No profiling**. Third parties cannot use the data they receive from data holders for profiling purposes, unless this is necessary to provide the service requested by the user. Profiling consists of any form of automated processing of personal data evaluating users' personal aspects (e.g., to analyze or predict aspects concerning work performance or economic situations) and producing legal effects on them or similarly significantly affecting them.

— **No sharing with another third party**. Third parties cannot make the data they receive available to another third party, unless contractually agreed with the user and provided that the other party takes all measures to protect trade secrets (see above).

— **Security**. Third parties cannot use the data they receive in a manner that adversely impacts the security of the product or related service.

— **Unfair competition and deriving insights**. See above.

4. The GDPR takes precedence where data governed by the Data Act is "personal data"

The Data Act does not affect rights and obligations under the GDPR and does not create any new legal basis for processing personal data. This means that the access rights described above require data holders to check whether personal data is involved and whether there is a legal basis for making available such personal data (e.g., if the requestor requests personal data of several users).

Data holders must therefore identify which parts of the data qualify as personal data. Erring on the side of caution by treating data with uncertain status as personal data will cease to be an option.

Overall, aligning compliance with the GDPR and with the Data Act will be challenging given data protection authorities' restrictive interpretation of the GDPR and the principle of data minimization, which requires that no more personal data than necessary is processed. Businesses will therefore need to define a well-thought-out policy and consider appropriate options, especially data anonymization, which may be a complex, time-consuming and resource-intensive process.

Chapter 2: Switching Between Providers of Data Processing Services

Background

The Data Act aims to ensure effective switching between providers of data processing services and tackle a cloud vendor lock-in effect by removing contractual, technical and commercial barriers. To this end, the Data Act lays down rules that will have a major impact by creating statutory provisions for topics that have usually been dealt with in contracts between providers and customers. In the view of the legislator, existing approaches have not achieved the desired results in these areas:

- **Antitrust**. Traditional antitrust concepts, such as the essential facilities doctrine, have not been applied in data processing markets thus far.
- **Digital Markets Act**. The Digital Markets Act imposes switching and interoperability obligations only on so-called gatekeepers, i.e., the largest digital platforms offering core platform services in Europe. Data processing services have not been in the scope of the designations so far.
- **Nonpersonal data regulation**. The 2018 Regulation on the free flow of nonpersonal data encourages data processing vendors to develop and apply self-regulatory best practice codes of conduct to facilitate switching between data processing vendors and improve data portability.
- **General Data Protection Regulation (GDPR)**. In the view of the European Commission, the GDPR provisions on data portability have not played the important role it expected. The Data Act is intended to complement the right of data portability under the GDPR with more specific rules. It will also apply to nonpersonal data. The Data Act is without prejudice to the GDPR, including regarding the powers of supervisory authorities and the rights of data subjects.

Unfortunately, the material and personal scopes of these different sets of rules could overlap, and the interactions between them are not clearly defined or discussed in the Data Act.

Who Is Subject to the Obligations?

The Data Act applies to providers of a data processing service, defined as "a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction." However, the obligations do not apply "to data processing services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where those data processing services are not offered at broad commercial scale via the service catalogue of the provider of data processing services." Unfortunately, it seems likely that these provisions leave a significant grey area of uncertainty for a number of services that do not clearly fall into one of these categories.

What Are the Switching Obligations?

Although the Data Act imposes many obligations on providers of data processing services, those providers are not required to develop new technologies or services, to disclose IP-protected digital assets or trade secrets to customers or vendors, or to compromise the customer's or their own security and integrity of service. In addition, customers and destination vendors must cooperate in good faith with the source vendor to ensure efficient transition processes. The obligations of providers of data processing services can be summarized as follows.

— **General Obligations**. Providers of data processing services are subject to a general obligation to not impose and to remove pre-commercial, commercial, technical, contractual and organizational obstacles, which inhibit customers from:

- terminating, after the maximum notice period and the successful completion of the switching process, the contract of the data processing service;
- entering into new contracts with a different provider of data processing services covering the same service type;
- porting the customer's exportable data and digital assets to a different provider of data processing services or to an on-premises Information and Communication Technology (ICT) infrastructure, including after having benefitted from a free-tier offering;
- achieving functional equivalence in the use of the new data processing service in the ICT environment of a different provider of data processing services covering the same service type; and/or
- unbundling, where technically feasible, certain data processing services from other data processing services provided by the provider of data processing services.

— **Minimum Contract Requirements**. In order to achieve these goals, the Data Act especially provides a list of minimum provisions that must be included in contracts for the provision of data processing services irrespective of the service delivery model.

- **Reasonable Assistance**. The vendors must provide reasonable assistance to customers and third parties in the switching process, including by providing all relevant data, providing the processing services and maintaining a high level of security during the transition period.
- **Data Specification**. The contract must include exhaustive specifications of all categories of data and digital assets that can be ported and those that cannot.
- **Data Erasure**. The contract must guarantee the erasure of all digital assets, including all exportable data, generated directly by the customer and/or relating to the customer directly after the expiration of the data retrieval period, unless agreed otherwise.
- **Termination**. The contract must be considered as terminated automatically once the switching process is completed or after the expiration of the data retrieval period, if customers only want to have their data deleted.

Timeline Requirements for Switching

Initiation of the Switching Process. Contracts should provide for a maximum notice period for initiation of the switching process, which must not exceed two months.

Transferring the Data. Contracts should also provide that customers can, upon request, switch to another data processing service or port all exportable data to an on-premises ICT infrastructure without undue delay, and in any event no longer than the mandatory maximum transition period of 30 calendar days.

Data Retrieval. Contracts should provide for a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period.

Longer Transition Period. Where the maximum 30-day transition period for data transferring and retrieval is technically unfeasible, the provider of data processing services must notify the customer within 14 working days after the switching request has been made, explain the technical unfeasibility, and indicate an alternative transition period, which may not exceed seven months. The customer should have the right to extend the transition period once, by a period that the customer deems more appropriate.

— **Functional Equivalence**. Vendors providing data processing services that concern infrastructural elements, such as servers (known as "infrastructure as a service" or IaaS), must take all reasonable measures in their power to facilitate the customer's achieving functional equivalence in the use of the destination service. To that end, such vendors should provide capabilities, adequate information, documentation, technical support and, where appropriate, the necessary tools. Importantly, this applies only to the features that are common to the source and destination services. The source vendors are not expected to create a new product or service, or to rebuild service within the destination infrastructure.

— **Open Interfaces Available**. Data processing vendors providing platform-based services ("platform as a service" or PaaS) and software-based services ("software as a service" or SaaS) must make open interfaces available to all their customers and relevant destination service providers free of charge to facilitate switching. These interfaces must include sufficient information on the service concerned to enable the development of software to communicate with the service, for the purposes of data portability and interoperability. In addition, PaaS and SaaS vendors must ensure compatibility with the interoperability specifications and standards that will be adopted by the EU. Absent such specifications and standards, vendors must, at the request of the customer, export the exportable data in a structured, commonly used and machine-readable format.

— **Gradual Withdrawal of Switching Charges**.

- **During the Transition Period**. For three years after the Data Act enters into force, vendors may impose switching charges that should not exceed the direct cost incurred by the vendor in the switching process. Examples of common switching charges are costs related to the transit of data from one provider to the other. However, customers should generally not bear costs arising from the outsourcing of services arranged for by the source provider. Before entering into a contractual agreement, vendors must provide customers with clear information on switching charges.

- **After the Transition Period**. After the expiration of the transition period, vendors will no longer be able to impose switching charges, except in cases of in-parallel use of services (in which case switching charges cannot exceed the costs incurred).

- **Exceptions**. The functional equivalence requirement, the gradual withdrawal of switching charges, and the requirement for PaaS and SaaS vendors to ensure compatibility with EU interoperability and standards do not apply to data processing services of which the majority of main features have been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where these data processing services are not offered at broad commercial scale via the service catalogue of the data processing service provider. In addition, none of the Data Act switching obligations apply to data processing services provided as a non-production version for testing and evaluation purposes, and for a limited period of time.

— **Unbundling**. The Data Act treats unbundling as a type of switching and requires vendors to not impose and to remove any obstacles that prevent customers from unbundling a specific individual infrastructure-based service from other processing services under the contract and moving to another vendor. This obligation is subject to the absence of major and demonstrated technical obstacles.

What Are the Restrictions for Certain International Transfers of Nonpersonal Data?

The Data Act introduces certain restrictions for the export of nonpersonal data to recipients outside the EU/European Economic Area. This adds another layer of complexity for companies with international operations, as these new provisions apply in addition to the existing restrictions for international transfers of personal data under the GDPR.

Providers of data processing services must take all adequate technical, legal and organizational measures to prevent international and third-country governmental access to and transfer of nonpersonal data held in the EU where this would create a conflict with EU law or an EU country's law. The Data Act does not contain provisions similar to Chapter V of the GDPR, meaning that it does not foresee items such as adequacy decisions, standard contractual clauses and/or binding corporate rules to address these challenges.

- Vendors must describe on their website the measures they adopted to prevent illegal access to and transfer of nonpersonal data held in the EU. Vendors must also indicate the jurisdiction to which their IT infrastructure is subject.
- Any decision of a non-EU court or administrative authority requiring access to or transfer of nonpersonal data held in the EU is only recognised or enforceable in the EU if it is based on an international agreement between the requesting third country and the EU or the relevant EU country.
- In the absence of such agreement, the vendor is only allowed to give access to or transfer the requested data if the third-country systems require the decision in question to be reasoned, proportionate, specific and subject to appeal, and to take into account the vendors' legal interests. Unfortunately, this will require providers of data processing services to undertake complex assessments of foreign laws, most likely under time pressure. It remains to be seen whether the envisaged European Commission guidelines in this area will provide sufficient assistance in these situations.

Chapter 3: The Enforcement System of the Data Act

Competent Authorities

— **EU Countries**. It is up to each EU Member State to designate the competent authorities responsible for the enforcement of the Data Act. EU countries may create one or several authorities or entrust these tasks to an existing authority. Countries that designate several competent authorities need to designate a data coordinator to facilitate cooperation between them.

— **Data Protection**. National data protection authorities will remain responsible for monitoring and enforcing the Data Act insofar as the protection of personal data is concerned.

— **EU Institutions**. The European Data Protection Supervisor (EDPS) will be responsible for monitoring the Data Act insofar as it concerns the European Commission, the European Central Bank and European Union bodies.

— **European Data Innovation Board**. The Data Act creates a new expert group called the European Data Innovation Board (EDIB), consisting of representatives of the competent authorities of all EU countries, the European Data Protection Board (EDPB) (which gathers data protection authorities from EU Member States and the EDPS), the EDPS, ENISA (the EU agency for cybersecurity), the European Commission, the EU body for the implementation of the EU SME strategy (EU SME Envoy), and other representatives of bodies in specific sectors and with specific expertise.

- **Cooperation**. The EDIB will facilitate cooperation between competent authorities through capacity building and the exchange of information. It does not have powers comparable to the powers of the EDPB. The EDIB is also intended to help ensure the consistent and effective application of the Data Act. On paper, this approach may be understandable. However, the EDPB's work to ensure the consistency of the GDPR is giving rise to many questions and controversies. One may therefore expect the EDIB's work to be very complex. This work will be even more delicate since it will involve reconciling various EU bodies attached to the rules for which they are responsible and that are unlikely to give up their own reading grid.
- **Advice**. The EDIB will advise and assist the Commission regarding the drafting of essential requirements regarding interoperability of data spaces, implementing and delegated acts, and guidelines laying down interoperability specifications.

Judicial Remedies

If natural or legal persons consider that their rights under the Data Act have been violated, they can lodge a complaint individually or collectively with the competent authority in the EU country where they usually live or work (for natural persons) or where they are established (for legal persons).

Natural and legal persons also have a right to an effective judicial remedy against competent authorities' binding decisions. They have such remedy where competent authorities fail to act on a complaint. Alternatively, in such a case, natural and legal persons can request a review by an impartial body with the appropriate expertise.

Sanctions

Sanctions under the Data Act must be effective, proportionate and dissuasive. This wording is very much inspired by the GDPR.

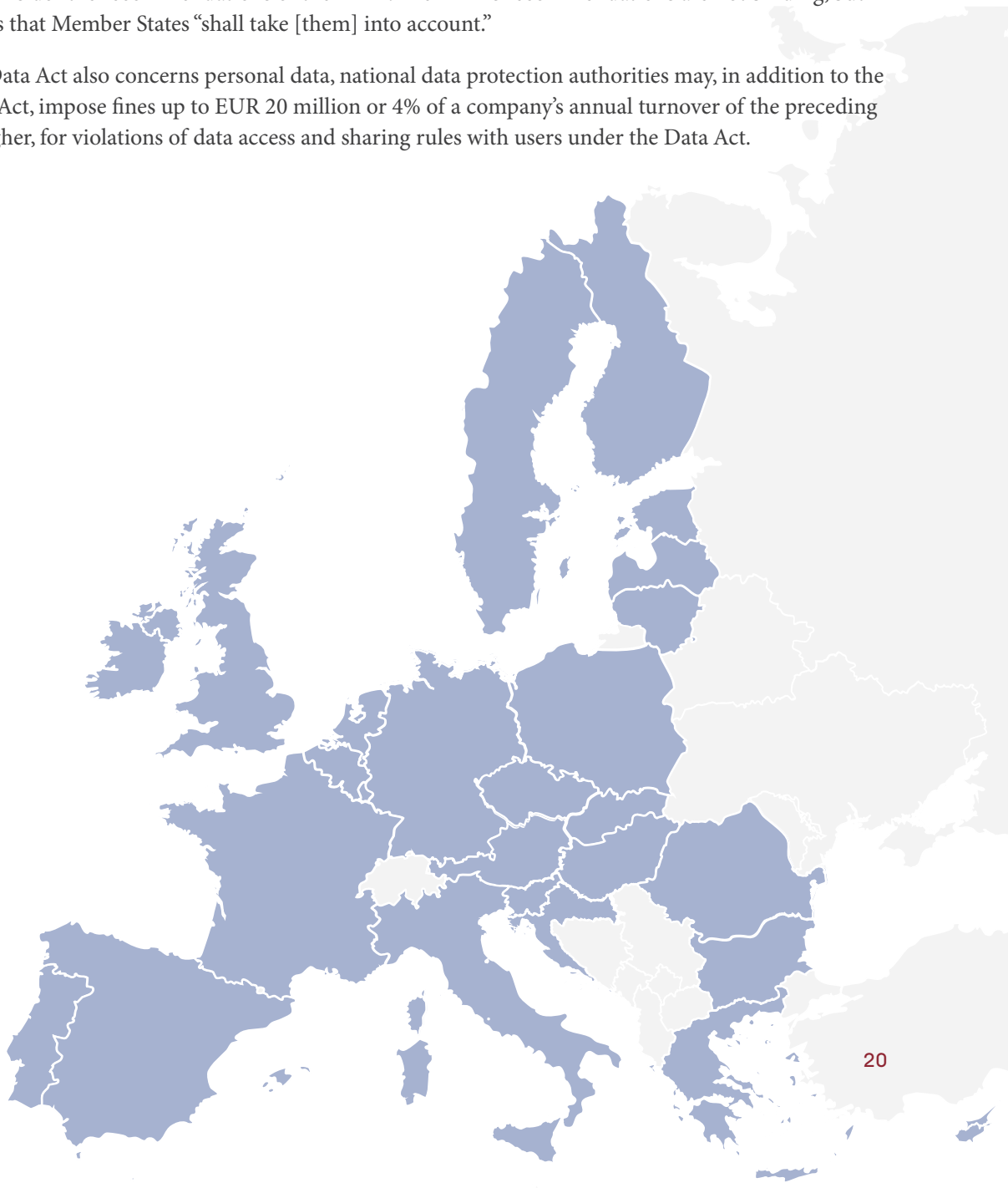
The Data Act also states that certain criteria for the imposition of fines must be taken into account, namely:

- the nature, gravity, scale and duration of the infringement;
- any action taken to mitigate or remedy the damage caused by the infringement;
- any previous infringements by the infringing party;
- the financial benefits gained or losses avoided by the infringing party due to the infringement, insofar as such benefits or losses can be established;
- any other aggravating or mitigating factors; and
- the infringer's annual turnover of the preceding financial year in the EU.

It is up to EU countries to lay down national rules on penalties implementing these requirements and to take all measures necessary to ensure that they are implemented. Penalties will therefore likely vary from country to country.

EU countries must consider the recommendations of the EDIB. The EDIB's recommendations are not binding, but the Data Act provides that Member States "shall take [them] into account."

If a violation of the Data Act also concerns personal data, national data protection authorities may, in addition to the fines under the Data Act, impose fines up to EUR 20 million or 4% of a company's annual turnover of the preceding year, whichever is higher, for violations of data access and sharing rules with users under the Data Act.



Contact Our Teams

For any additional information on data-related issues under EU law, please contact our teams in Brussels, Frankfurt, and London.

BRUSSELS

Anne Vallery

Partner-in-Charge
anne.vallery@wilmerhale.com

Frederic Louis

Partner
frederic.louis@wilmerhale.com

Itsiq Benizri

Counsel
itsiq.benizri@wilmerhale.com

FRANKFURT

Dr. Martin Braun

Partner
martin.braun@wilmerhale.com

Prof. Dr. Hans-Georg Kamann

Partner
hans-georg.kamann@wilmerhale.com

LONDON

Cormac O'Daly

Partner
cormac.o'daly@wilmerhale.com

Connect with us

wilmerhale.com

24_0184 9/24