SLAUGHTER AND MAY/

Digital Regulation Essentials: The Data Act

The EU Data Act entered into force on 11 January 2024 and most of its rights and obligations started applying on 12 September 2025. Here we highlight some of the key aspects of the Data Act.

OVERVIEW – WHAT YOU NEED TO KNOW

Broad ambition: The Data Act aims to enhance the EU's data economy and foster a competitive data market by making data more accessible and usable, encouraging innovation and increasing data availability.

Wide impact: Businesses across the economy are affected, including anyone using connected products and those manufacturing such products or providing apps/software interacting with them. Organisations sharing data or providing or procuring cloud and edge services are also likely to be affected.

Key benefits and risks: Enhanced access to connected product data provides scope for innovation and operational efficiencies. The Act's rules on unfair contract terms and cloud/edge switching may open-up opportunities for a better deal. At the same time, businesses may be subject to new requests for data access from customers and other businesses, implicating device design, security and operational considerations.

Extra-territorial scope: The Act applies to products, services or data being made available in the EU - so affects international organisations with EU activities (irrespective of their place of domicile).

Developing regime: While most of the Data Act's obligations are now in force, the Digital Omnibus is set to amend the Act while key pieces of guidance and Member States' approaches to enforcement are still in development. In-scope organisations should stay abreast of changes as they navigate the Act's impact.

Enforcement and penalties: Maximum fines are set at Member State level, with penalties required to be 'effective, proportionate and dissuasive'. National regulators will oversee enforcement, with data protection authorities continuing to enforce any GDPR-related infringements.

TIMING

- **Jan 2024** – Act in force
- **Sep 2025** – Act applies generally (subject to some exceptions)
- **Sep 2026** – Design and manufacturing requirements for connected products/ related services apply
- **Sep 2027** – Unfair terms requirements apply to contracts executed pre-Sept 2025 (i.e. older contract terms will need amending)

DATA ACT – AREAS COVERED

Connected product data sharing: Business and consumer users of connected products/related services can access data created by their usage or have it shared directly with a third party.

B2B data sharing: Where holders of data must share it with others under the Data Act or other EU Law, certain mandatory data sharing rules apply.

Interoperability: New specifications support interoperability in EU data spaces, with additional support for interoperability between cloud/edge data processing services.

Cloud switching: Seamless customer switching between cloud/edge data processing services is facilitated (including via minimum requirements for cloud contracts and, ultimately, the removal of switching charges).

Unfair terms for data access/use: In a B2B context, companies cannot impose unfair contract terms for data access and use.

Unlawful third country government access: Providers of cloud/edge data processing services must implement appropriate safeguards to prevent unlawful data access by (or transfer to) a third country government.

Business to government data sharing: Public bodies can access data held by private bodies where there is an exceptional need (e.g. in a public emergency), subject to certain safeguards.

SLAUGHTER AND MAY/

Digital Regulation Essentials: The Data Act

Connected product data sharing

KEY PROVISIONS

Access to data unlocks a wide range of opportunities for organisations, from better utilisation of new technologies (such as AI) and innovative services, to more understanding of customer and business needs. Users of connected products and related services can now access the data that they co-create by using connected products/related services, subject to certain provisions. At the same time, the Act creates new challenges for businesses that may be subject to requests for access from customers and other businesses, potentially implicating product design, security and ongoing operational considerations. The key obligations under the Act in this context include:

Manufacturing obligations

- Connected products and related services must be designed and manufactured in such a manner that product data and related service data are, by default, easily, securely (and where relevant and technically feasible), directly accessible to the user.
- Challenges are anticipated in operationalising these requirements, due to the breadth of product and data types in scope (encompassing 'raw' and 'pre-processed' data, ranging from user inputs, to speed and temperature data). There will be no one-size-fits-all approach to how data should be provided.

Manufacturing obligations

- Where users cannot directly access data from the connected product/service, data holders must make data 'easily' available to them, e.g. via request. The data provided must be of the same quality as available to the data holder, provided without undue delay and for free (where feasible, on a continuous, real-time basis).
- Users can share this data themselves, or they can ask the data holder to send it to a third party. There is no obligation for a data holder to share data with third parties based outside the EU.
- Certain exemptions apply for micro and small companies.
- Specific rules apply in B2B arrangements – e.g. data holders should make data available to third parties under fair, reasonable and non-discriminatory terms and in a transparent manner and may agree compensation with them (which must be reasonable).

Provision of information

- Before entering into a contract for the purchase, rent, or lease of a connected product, manufacturers and providers must provide information about the data collected and generated by the product.

Restrictions and measures to protect trade secrets and cyber security

- The data obtained cannot be used to develop a competing connected product (but it can be used to compete in related or aftermarket services, such as repair and maintenance services).
- The data holder and the user or third party may agree on measures to preserve the confidentiality of trade secrets. When such measures are not respected, the data holder may withhold or suspend data sharing. The data holder may refuse to share the data, but only where it can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets.
- Limits can also be put on data sharing if there is a risk that the security requirements of the connected product could be undermined, resulting in serious adverse effects to the health, safety or security of people.

KEY TERMS FOR CONNECTED PRODUCT DATA SHARING

"Connected product"

- Items that obtain, generate or collect data concerning their use or environment and can communicate product data; and whose primary function is not the storing, processing or transmission of data on behalf of parties other than the user. Connected products can include consumer products such as connected cars and smart home devices, as well as industrial products such as planes and industrial machines.

"Related service"

- Digital services which are connected with the product in such a way that their absence would prevent the connected product from performing one of its functions or are subsequently added to update or adapt the functions of the connected product. Related services can include apps which make connected products behave in a specific manner (e.g. an app to adjust the settings of a smart home thermostat). There is current uncertainty about the breadth of this definition, e.g. how central 'a function' needs to be to a connected product to bring a service interacting with it within the rules.

"Data holder"

- Person that has the right or obligation, in accordance with the Data Act or other EU law, to use and make available data (which could include product data or related service data retrieved or generated during the provision of a related service). Further guidance is expected to clarify this definition, as industry commentary has noted a degree of circularity in its drafting.

"Aftermarket" and "ancillary" services

- Data recorded by connected products or related services are an important input for aftermarket, ancillary and other services. Those services include things like repair and maintenance services and data-based insurance.

SLAUGHTER AND MAY/

Digital Regulation Essentials: The Data Act

Latest updates and key questions

LATEST UPDATES

The Digital Omnibus proposes changes to the Data Act

- Changes in the Digital Omnibus include adding new streamlined rules for re-use of public sector data (currently in the Data Governance Act and Open Data Directive) and bolstering protections for trade secrets in connected product data, to address concerns about unlawful leakage to foreign entities. The Omnibus would also introduce a lighter-touch switching regime for 'custom-made' data processing services (e.g. cloud/edge services).

Two sets of model contractual terms issued by the European Commission to support Data Act compliance

- One set supports B2B sharing of connected product data under the Act and the other relates to cloud switching. Unlike GDPR standard contractual clauses, the use of these terms is voluntary and they can be amended. While many organisations may choose to develop (or amend) their own bespoke terms, the model terms provide useful insights, including via drafting notes, into how the European Commission (EC) interprets the Act's requirements.

New helpdesk and guidance

- A new Data Act Legal Helpdesk has been launched by the EC to support organisations with compliance. Organisations can submit queries via an online portal and receive tailored replies, within 15 days in most cases.
- On 2 February, the EC published draft guidelines on calculating reasonable compensation (under Article 9) of the Data Act, for consultation. The guidance is relevant to B2B data sharing mandated under the Data Act and under other EU legislation coming into force after 12 September 2025.
- Following EC industry workshops in January, new guidance on key definitions in the Data Act is expected in Q1 2026.

5 KEY QUESTIONS TO ASK

1. Do I understand how my organisation uses connected products?
2. Do I know how the Data Act's classifications (user, data holder, data recipient) apply to us?
3. Is my organisation exposed under the Data Act (e.g. to new data or switching requests), or does the Act provide opportunities (e.g. to drive efficiencies or new product features)?
4. As an organisation, do we have a plan for complying with the Data Act? Can our existing compliance processes (e.g. GDPR privacy notices and data access/portability pathways) be leveraged for Data Act compliance?
5. Do I know if our service agreements contain cloud or data sharing provisions within the scope of the Data Act? And whether the Act's rules could support us getting a better deal?

Digital Regulation at Slaughter and May

Our Digital Regulation practice covers the full spectrum of digital rules, from AI regulation, competition-focused platform regulation, to online harms and content regulation, and data access and portability. Clients look to us to offer practical, risk-adjusted advice that helps them navigate this ever more complex landscape – and to innovate at speed.

For more information, see our Digital Regulation Practice page or our blog

JORDAN ELLISON
Partner
jordan.ellison@slaughterandmay.com
+32 (0)2 737 9414

LAURA HOUSTON
Partner
laura.houston@slaughterandmay.com
+44 (0)20 7090 4230

WILL MANLEY
Head of Digital Regulation
will.manley@slaughterandmay.com
+32 (0)2 737 9431

NATALIE DONOVAN
Head of Knowledge, Tech and Digital
natalie.donovan@slaughterandmay.com
+44 (0)20 7090 4058