Kluwer Competition Law Blog

The EU's Data Act: Capstone of the EU Data Strategy

Jay Modrall (Norton Rose Fulbright, Belgium) · Thursday, March 3rd, 2022

On 23 February 2022, the EU Commission published its long-awaited Data Act, the last major building block of the Commission's February 2020 Data Strategy. The Data Act Is an ambitious piece of legislation with implications for consumers and businesses across the economy, not limited to the technology sector. The act aims to facilitate access to data by consumers and businesses; provide for government use of data in cases of "exceptional data need" (in some cases without compensation); facilitate switching between cloud and edge services; prevent unlawful data transfer by cloud service providers; promote interoperability across European data spaces; and set standards for "smart contracts" between "data holders" and data recipients.

The Data Act will likely provoke resistance, especially from companies that advocated a voluntary approach to data sharing. The Data Act's requirements that manufacturers and data processing service companies employ technical standards to permit interoperability and data portability may also prove difficult (and expensive) to implement in the envisaged one-year implementation period.

Background

The Data Act will work closely with:

- The recently agreed Data Governance Act, which will create a new category of neutral data intermediary.
- EU initiatives to promote so-called European Data Spaces; and
- Recent initiatives in relation to European standards and standard-essential patents.

The Data Act also ties into ongoing EU antitrust reforms, such as:

- The Commission's recently concluded sector inquiry into the consumer Internet–of-Things (IoT).
- The proposed Digital Markets Act, which will impose new data-related obligations on so-called "gatekeeper platforms".
- The treatment of information sharing under the Commission's forthcoming rules on information sharing, which are currently subject to a consultation and will be finalized later this year.

Joining an already crowded EU digital agenda, the Data Act may take a back seat to measures such as the Digital Markets Act, the Digital Services Act and the AI Regulation, all of which were

proposed in 2021. The Data Act's complexity may also slow progress and generate significant resistance in key areas, such as new obligations for data processing service providers, mandatory data sharing with public authorities in cases of "exceptional need," requirements for data processing services to ensure interoperability, and discriminatory treatment of so-called "gatekeeper platforms," among other things.

Expanding data access and interoperability: relationship to other EU digital regulatory measures

The Data Act is an important regulatory initiative in its own right, but as the last building block in an ambitious regulatory agenda laid out in the Commission's February 2020 Data and AI Strategies, it also knits together a wide range of other EU regulatory measures. A brief overview of such legislation may help clarify how the Data Act builds on this framework:

- *Database Directive*: the 1996 Database Directive provides for the *sui generis* protection of databases created as a result of a substantial investment, even if the database itself is not an original intellectual creation protected by copyright. The Data Act *excludes* application of the *sui generis* right that might otherwise exclude databases generated by products collecting data (essentially machine-generated data from IoT and similar technologies) from the reach of the data sharing requirements under the Data Act. The net effect is that the Data Act's data sharing requirements apply to such data.
- *GDPR*: the 2016 GDPR created a right of portability of personal data for data subjects, but did not set out detailed technical requirements to operationalise this right. The Data Act extends the portability right to non-personal data and creates a legal framework for users and third parties to exercise this right with respect to data generated by products and related services.
- *Free Flow of Non-Personal Data Regulation*: the 2018 Free Flow of Non-Personal Data Regulation limited geolocation requirements for data within the EU and presented a self-regulatory approach to the problem of "vendor lock-in" at the level of providers of data processing services, by introducing codes of conduct to facilitate switching data between cloud services. The Data Act supplements the Free Flow of Non-Personal Data Regulation by imposing legal requirements to facilitate switching and adds safeguards for the transfer of non-personal data outside the EU.
- *Platform to Business Regulation*: the 2019 Platform to Business Regulation requires platforms to describe for business users the data generated from the provision of the service. The Data Act broadens this requirement and extends it to end users of products that collect data.
- *Open Data Directive*: the 2019 Open Data Directive encourages sharing of data held by the public sector and publicly funded research data, but does not apply to data held by private persons. The Data Act extends the Open Data Directive by creating an obligation for private persons to share data with public authorities in situations of exceptional need.
- *Data Governance Act*: the recently agreed Data Governance Act facilitates the voluntary sharing of data by individuals and businesses and harmonises conditions for the use of certain public sector data, but does not mandate data sharing or access to data held by private persons. The Data Governance Act also creates a new category of neutral data intermediaries who may benefit from data sharing under the Data Act. The Data Act mandates sharing of data generated by products with end users and third parties (other than gatekeeper platforms), potentially including neutral data intermediaries.
- *AI Regulation*: many of the data-generating products addressed by the Data Act are likely to use

"AI systems" within the meaning of the AI Regulation. The AI Regulation imposes strict rules on developers, resellers, and even business users of AI systems and products incorporating them, especially if the AI systems qualify as "high risk." These include extensive obligations relating to data sets used in AI systems, such as obligations to monitor the data set's quality and correct any issues. Those rules will presumably carry across to data shared with users and third parties under the Data Act.

- *European Data Spaces*: the 2020 Data Strategy envisaged the creation of a large number of sector-specific "data spaces" to encourage the collection and use of data in those sectors. Each of these data spaces will entail its own implementing measures, but the Data Act provides a horizontal framework for interoperability across all of them.
- *Standards initiative*: the Data Act envisages the development of a variety of European industry standards to permit interoperability and switching among data processing services and portability of data. The Data Act will likely prove a leading test of the EU's recently announced, proactive approach to standards.

You say "data," I say "competitively sensitive information": Relationship to EU antitrust reform

The growing recognition of the competitive importance of big data has prompted debates starting around 2015 as to whether antitrust principles, such as access to "essential facilities," could compel large technology companies to share data with competitors. The conditions for application of the essential facilities doctrine are very strict, however, and no such obligation has been imposed to date.

Frustrated by traditional antitrust rules, the Digital Markets Act will impose new obligations for gatekeeper platforms to share certain data with business users of the gatekeepers' core platform services. The Data Act's obligations are broader, in that they require sharing of product-generated data: With end users and third parties, not only business users of core platform services, and in a more targeted way, in that data shared under the Data Act will be subject to strict controls, potentially monitored by smart contracts.

Encouraging the collection and sharing of valuable data for use by businesses is a core objective of the Data Act, the Digital Markets Act and other EU policies. Under EU antitrust law, however, the exchange of competitively sensitive information, especially among competitors, can constitute a serious antitrust violation. Neither the Data Act nor other related measures addresses the dividing line between valuable data and competitively sensitive information whose sharing may violate EU antitrust rules.

Late this year, the Commission will adopt new guidelines on horizontal cooperation agreements discussing, among (many) other things, the antitrust treatment of information sharing. The draft horizontal guidelines, published on March 2, 2022 and currently open for comments, address the antitrust treatment of data sharing in more detail than the current guidelines. The draft guidelines note that, "The assessment under Article 101(1) will depend on elements such as the nature of the data shared, the conditions of the data sharing agreement and the access requirements, as well as the market position of the relevant parties" (para 442). The draft guidelines focus on the competitive significance of data pools and potential foreclosure of competition by companies who do not have access. The draft guidelines apparently do not address the sharing of data pursuant to

mandatory or voluntary EU digital regulatory frameworks.

Data Act: Overview

B2C and B2B data sharing

The main provisions applicable to business-to-consumer (B2C) and business-to-business (B2B) data sharing are set out in Chapters II and III. Chapter II imposes sweeping new obligations on manufacturers of products that collect data to share such data with the users of their products and related services and with third parties at users' request. Chapter III sets out requirements relating to the compensation and other conditions for such sharing.

Manufacturers (other than micro or small enterprises) will have to design and manufacture products and related services so that data they generate will be, by default, easily, securely and directly accessible to the user. Likely inspired by the Commission's findings on virtual assistants in its consumer IoT sector inquiry, products and related services include virtual assistants insofar as they are used to access or control a product or related service, but the implications of this provision are not clear where the product manufacturer and virtual assistant provider are unrelated companies.

Contracts to purchase, rent or lease products or use related services that collect data will have to include extensive data-related information. Information to be provided includes:

- The nature and volume of the data likely to be generated by the use of the product or related service.
- Whether the data is likely to be generated continuously and in real-time.
- How the user may access those data.
- Whether the manufacturer intends to use the data itself or allow a third party to use the data.
- Whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder.
- How the user can contact the data holder.
- How the user may request sharing with a third party.

Where data cannot be directly accessed from a product, the data holder – e.g., the product's manufacturer – must make the data available without undue delay, free of charge and, where applicable, continuously and in real-time.

At the user's request, data holders must make such data available to third parties in the same manner, free of charge to the user. The Data Act does not limit the third parties with whom users may require data holders to share data, except notably to exclude "gatekeeper platforms" subject to the Digital Markets Act. Here the Commission likely has in mind aftermarket service providers and the new category of neutral data intermediaries to be created under the Digital Governance Act.

A third party shall process the data made available to it only as agreed with the user (subject to the rights of the data subject insofar as personal data are concerned) and shall delete the data when they are no longer necessary.

Data holders will enjoy some protections. They need only disclose trade secrets subject to specific,

necessary protections to ensure confidentiality. Users cannot use data to develop a competing product. As discussed below, data holders may use smart contracts to ensure compliance.

Chapter III imposes obligations on data holders required to make data available:

- Data holders obliged to make data available to a data recipient must enter into agreements on fair, reasonable and non-discriminatory terms and in a transparent manner. Any compensation will have to be reasonable, and in the case of SMEs, cannot exceed the costs incurred for making the data available.
- A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user.
- Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or compliance with their obligations under the regulation or other applicable law.

Data holders may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with the Data Act and the agreed contractual terms.

However, data holders cannot assert a *sui generis* right under the EU Database Directive, because the Data Act provides that such rights do not apply to databases containing data obtained from or generated by the use of a product or a related service (essentially, machine-generated data).

A data recipient that has provided inaccurate or false information, deployed deceptive or coercive means or abused evident gaps in the data holder's technical infrastructure, or used the data for unauthorised purposes or disclosed those data to another party without authorisation, is required to destroy the data made available by the data holder and any copies thereof.

Such a data recipient can also be required to end the production and marketing of goods, derivative data or services based on knowledge obtained through such data and destroy any infringing goods (except where the use of the data has not caused significant harm or such a remedy would otherwise be disproportionate).

Unfair contractual terms imposed on SMEs

Chapter IV prohibits unfair contractual terms unilaterally imposed in data sharing contracts on micro, small or medium-sized enterprises. Chapter IV includes a list of clauses that are either always unfair or presumed to be unfair, relating (among other things) to limitations of liability or restrictions on remedies or data usage.

Public sector data access for exceptional needs

Chapter V allows for the use by public sector bodies of data held by businesses in cases of exceptional need. In public emergencies, such as public health emergencies or major disasters, data would be made available for free. In other cases of exceptional need, including to prevent, or assist with the recovery from, a public emergency, a data holder would be required to make data

available but would be entitled to compensation covering costs related to making the relevant data available, plus a reasonable margin.

Switching between data processing services

Chapter VI introduces new contractual, commercial and technical requirements for providers of cloud, edge and other data processing services to enable switching between such services.

In particular, providers of data processing services will be required to remove commercial, technical, contractual and organisational obstacles inhibiting customers from:

- Terminating their agreements.
- Concluding new agreements with a different provider covering the same service type.
- Porting its data, applications and other digital assets to another provider of data processing services.
- Maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type.

Contracts with data processing service providers will be required to set out the parties' rights and obligations in relation to switching. These will include clauses allowing the customer, to request:

- To switch to a data processing service offered by another provider of data processing service or to port all data, applications and digital assets generated directly or indirectly by the customer to an on-premise system on no more than 30 days' notice (during which a data processing service provider shall assist and, where technically feasible, complete the switching process and ensure full continuity).
- An exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service, including, but not limited to, configuration parameters, security settings, access rights and access logs.
- A minimum 30-day period for data retrieval.

Data processing service providers will initially be able to charge customers for costs directly linked to the switching process, but such charges must be phased out within three years.

Providers of data processing services that concern infrastructural elements, such as servers, networks and related virtual resources, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall ensure that the customer enjoys functional equivalence in the use of the new service after switching.

Other data processing service providers shall make open interfaces publicly available free of charge, ensuring compatibility with open interoperability specifications or European standards for interoperability under Chapter IX (see below).

Where open interoperability specifications or European standards do not exist, data processing service providers must export all data generated or co-generated, including the relevant data

formats and data structures, in a structured, commonly used and machine-readable format.

Safeguards for non-personal data transfers outside the EU

Chapter VII addresses unlawful third party access to non-personal data held in the EU by data processing services offered in the EU.

The Data Act will require data service providers to take all reasonable technical, legal and organisational measures to prevent access to non-personal data that conflicts with competing obligations to protect such data under EU law, unless strict conditions are met.

More specifically, any decision or judgment of a non-EU governmental body requiring a provider of data processing services to transfer from or give access to non-personal data held in the EU may only be recognised or enforceable if based on an applicable international agreement, such as a mutual legal assistance treaty.

Absent such an agreement, a provider of data processing services that is required to transfer from the EU, or give access to, non-personal data held in the EU, and compliance with such a decision would conflict with EU or Member State law may provide such access only where the requirement is specific, reasoned and proportional, it is subject to court review, and the non-EU body or reviewing court is empowered to take into account the legal interests of the data provider under EU or Member State law.

Interoperability for data spaces and data processing service providers

Chapter VIII provides for essential requirements for interoperability for operators of European data spaces, data processing service providers and smart contracts for data sharing.

Operators of data spaces will have to facilitate interoperability of data, data sharing mechanisms and services. More specifically:

- The dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data; the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner.
- The technical means to access the data, such as application programming interfaces, and their terms of use and quality of service, shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format.
- The means to enable the interoperability of smart contracts within their services and activities shall be provided.

Data processing service providers will also be subject to essential requirements in relation to interoperability. Open interoperability specifications and European standards for the interoperability of data processing services shall:

- Be performance-oriented towards achieving interoperability.
- Enhance portability of digital assets.
- Guarantee, where technically feasible, functional equivalence between different data processing services.
- Address the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioral interoperability and policy interoperability.
- Address the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability.
- Address the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

Smart contracts for data sharing: A different set of essential requirements will apply

Smart contract application providers shall comply with the following essential requirements:

- Safe termination and interruption.
- Data archiving and continuity.
- Access control.

Such providers must perform a conformity assessment and issue an EU declaration of conformity. A smart contract that meets harmonised EU standards shall be presumed to be in conformity with the essential requirements.

Similarly, operators of European data spaces that meet EU harmonised standards shall be presumed to be in conformity with the essential requirements.

The Commission may request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements. Where harmonised standards do not exist, or the Commission considers them insufficient, the Commission shall adopt common specifications.

The Commission may also adopt guidelines laying down interoperability specifications for the functioning of common European data spaces, such as architectural models and technical standards implementing legal rules and arrangements between parties that foster data sharing (such as regarding rights to access, and technical translation of consent or permission).

Implementation and enforcement

In line with many other EU regulatory frameworks, but unlike the Digital Markets Act, the Data Act will be enforced at the Member State level by designated national authorities.

The Data Act, as proposed, would apply one year after adoption and publication in the EU Official Journal. Two years later, the Commission will conduct an evaluation of the regulation, in particular as regards the inclusion or exclusion of categories or types of data or the exclusion of gatekeeper platforms as beneficiaries of the data transfer right.

Our key observations

The Data Act:

- Is a complex piece of legislation combining elements of digital regulation, consumer protection, contract law, data protection, and intellectual property laws.
- Must be read in conjunction with other EU regulations on a wide range of topics.
- Supplements, and reinforces, a number of recent initiatives – for example, by extending mandatory data sharing obligations in place for public bodies to data held by private parties.
- Adds teeth to previously voluntary measures to facilitate switching between data processing service providers and to increase transparency for users on the data generated by products and services they use.
- Extends the GDPR right of portability of personal data to non-personal data.
- Will likely create significant challenges for manufacturers of products and providers of services that collect data, who will need to design their offerings to ensure data access, portability and interoperability well beyond what currently exists.
- These obligations will entail the development of numerous new technical standards having a legal value under EU law under the Commission's new, more proactive approach to EU standard setting. These provisions will doubtless prove controversial, as will other provisions such as exclusion of gatekeeper platforms from receiving data even if users so request and the imposition of safeguards against data processing services sharing data held in the EU with non-EU governmental bodies (except as provided by mutual assistance treaties).

The Data Act's extensive data sharing obligations align with those of the Digital Markets Act, and both reflect years of discussion and frustration with the limits of antitrust enforcement to mandate data sharing. However, companies sharing data under the Data Act (and the Digital Market Act) remain subject to EU antitrust rules, including limitations on the sharing of competitively sensitive information. The Data Act's effectiveness, if and when it is adopted, will depend to a significant extent on the guidance the Commission will provide late this year on its evolving approach to information sharing.

This entry was posted on Thursday, March 3rd, 2022 at 9:00 am and is filed under Data protection, European Commission, European Union
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.