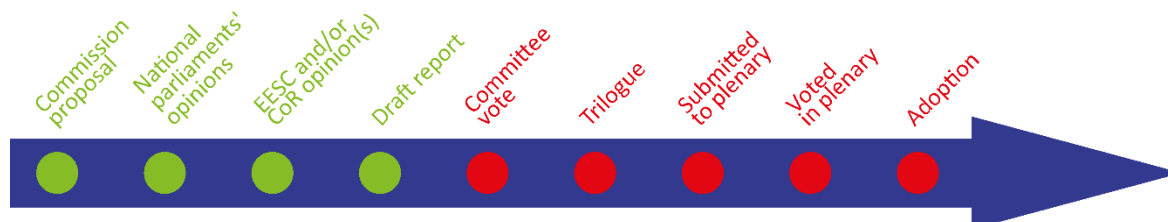


The Data act

OVERVIEW

On 23 February 2022, the European Commission unveiled a proposal for an EU regulation – the data act – laying down harmonised rules on fair access to and use of data. The aim is to remove barriers before consumers and businesses' access to data in a context in which the volume of data generated by humans and machines is increasing exponentially and becoming a critical factor for innovation by businesses (e.g. algorithm training) and by public authorities (e.g. shaping of smart cities). The proposed act establishes common rules governing the sharing of data generated by the use of connected products or related services (e.g. the internet of things, industrial machines) to ensure fairness in data sharing contracts and to allow public sector bodies to use data held by enterprises where there is an exceptional need (e.g. public emergency). Furthermore, the proposed act introduces new rules to facilitate switching between providers of cloud services and other data processing services, and puts in place safeguards against unlawful international data transfer by cloud service providers. The Council and Parliament are working on defining their respective positions.

Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)		
<i>Committee responsible:</i>	Committee on Industry, Research and Energy (ITRE)	COM(2022)0068 23.2.2022
<i>Rapporteur:</i>	Pilar del Castillo Vera (EPP, Spain)	2022/0047(COD)
<i>Shadow rapporteurs:</i>	Miapetra Kumpula-Natri (S&D, Finland) Alin Mituța (Renew, Romania) Damian Boeselager (Greens/EFA, Germany) Elena Lizzi (ID, Italy) Margarita De La Pisa Carrion (ECR, Spain) Elena Kountoura (The Left, Greece)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
<i>Next steps expected:</i>	Vote in committee on draft report	



Introduction

On 23 February 2022, the European Commission submitted a proposal for a regulation¹ – the data act – seeking to harmonise rules on fair access to and use of data in the EU. The proposal builds on the assumption that innovation rests increasingly on the use of industrial data, i.e. data generated by machine-to-machine interaction (e.g. connected factory machines) and by human-to-machine interaction (e.g. connected devices). Such data, which are said to have become [the new oil](#), are critical for innovations by business (e.g. algorithm training) and by public authorities (e.g. for shaping smart cities).

In its 2020 [communication on a European strategy for data](#), the Commission highlighted that data are at the centre of the digital transformation and that data-driven innovation is poised to bring enormous benefits to citizens, such as improved personalised medicine and new mobility as well as contributing to the European Green Deal. However, the Commission also found that while the volume of data generated by humans and machines has been increasing exponentially in recent years, most data remain unused or their value is concentrated in the hands of a relatively few large companies, with only 8 % of smaller companies and businesses capturing value from data.² As a result, EU policymakers started reflecting on how to unlock the untapped potential of **'business to business' (B2B) data sharing** by providing opportunities for the reuse of data.

Furthermore, the Commission appointed an [expert group](#) to identify good practices on **'business to government' (B2G) data sharing**, assess the legal, economic and technical obstacles preventing B2G data sharing, and give recommendations to the Commission on how to further develop its B2G data-sharing policy. The B2G expert group produced a [report](#) highlighting that to date, local authorities' access to private sector data was exceptional and fragmented. The B2G expert group recommended that the Commission explore the creation of an EU-wide regulatory framework to ease B2G data sharing, among other things by removing existing limitations to data sharing. Further academic [research](#) showed as well that data donorship (i.e. companies freely providing data to certain cities) may pose ethical dilemmas and that organising public procurement of data and data partnerships for smart cities is legally difficult.

In addition, the Commission carried out debates on ways to foster access to data in **trusted and collaborative cloud infrastructures** in the EU, notably in the context of ongoing initiatives for a [European federated cloud](#).

Following this preparatory work, in February 2020 the Commission published the [European strategy for data](#), paving the way to a genuine single market for data. This was followed by an [inception impact assessment](#) (of the proposed data act) in May and a [public consultation](#) in December 2021. According to the findings, stakeholders encounter obstacles in B2B data sharing; agree on the need for action at EU or national level on B2G data sharing for public interest purposes; and demand legislative initiatives that would establish a more competitive market for cloud computing services and safeguards for non-personal data in the international context.

Existing situation

EU legislation adopted in recent years has focused on removing barriers to the free flow of data across the internal market, safeguarding personal data protection, increasing trust in data sharing and enhancing the supply of public and private sector data for innovative reuse. The [Free Flow of Non-personal Data Regulation](#) ensures that non-personal data can be stored, processed and transferred anywhere in the EU. The [General Data Protection Regulation](#) (GDPR), which enshrines a general access and portability right (Article 20 GDPR) in EU law may cover data generated by connected products and related services according to the Commission's [impact assessment](#). However, the exercise of this right has proven largely theoretical, because it does not cover continuous or real-time access to data (which is essential for products that are always connected to the internet) and because interpretations regarding the types of data that fall under this obligation

tend to differ.³ Furthermore, although the recently adopted [Digital Markets Act](#) (DMA) and [Digital Services Act](#) (DSA) both include rules on data access, the obligation to ensure it falls primarily on gatekeepers and large providers and does not create portability between cloud providers. Likewise, the Commission's [impact assessment](#) to the current proposal stresses that the [Data Governance Act](#), which sets out rules on fostering voluntary data-sharing agreements, does not apply to cloud and edge services.

In addition, the Commission has proposed to revise the [Database Directive](#), which provides for the sui generis protection of databases created through a substantial investment, even if the databases themselves are not original intellectual creations protected by copyright. However, in today's digital world where data are often generated in vast volumes and automatically by sensors, machines and related technologies, it becomes difficult to clearly distinguish which databases may be protected by the sui generis right and which may not. There is a risk that data holders (such as original equipment manufacturers) could use their sui generis right to prevent access to the IoT data gathered in a database to any third party in a way that leads to lock-in situations.⁴ This would present an obstacle to the sharing and use of data. The Database Directive should therefore be amended to prevent the sui generis protection from being extended to machine-generated data.

Consequently, in its [impact assessment](#) accompanying the proposal, the Commission highlights that there is an insufficient availability of data for use and reuse in the EU economy or for societal purposes, and that a range of legal, economic and technical issues related to data use affect a range of sectors.

Parliament's starting position

In its 2021 [resolution](#) on a European strategy for data, the European Parliament urged the Commission to submit legislation to foster data access and interoperability in the forthcoming data act. The EP also highlighted the need for creating common European data spaces for the free flow of non-personal data across borders and sectors and between businesses, academia, relevant stakeholders and the public sector.

Council and European Council starting position

The European Council's [conclusions](#) of 21-22 October 2021 underlined the importance of unlocking the value of data in the EU by means of a comprehensive regulatory framework conducive to innovation; facilitating better data portability and fair access to data; and ensuring interoperability.

Preparation of the proposal

The proposal builds on the Commission's above-mentioned communication on a European strategy for data, on the latest revision of the Database Directive and on the Commission [study](#) supporting the revision. Furthermore, as mentioned above, the Commission held a public consultation on the proposed data act from 3 June to 3 September 2021 and conducted an impact assessment accompanying the proposal. EPRS issued an [initial appraisal](#) of the Commission impact assessment of the data act in July 2022.

The changes the proposal would bring

Principle and objectives

The underlying premise of the proposal is that the right to use non-personal data is valuable and that value should be allocated fairly across different sectors of the economy. The proposed data act, therefore, intends to **ensure fairness** in the allocation of value from data among the players in the data economy and to **foster access to and use of data** in a context characterised by the proliferation of cloud services and products connected to the internet of things (IoT). The overall

principle underlying the proposal is that companies will have to open up their non-personal data, namely the data generated by the use of their services or products.

The proposed data act is a **horizontal piece of legislation** based on [Article 114](#) of the Treaty on the Functioning of the EU. It aims to ensure that EU businesses across all sectors are in a position to innovate and compete, to empower individuals with respect to their data, and to equip businesses and public sector bodies with mechanisms enabling them to use data to tackle public emergencies and other exceptional situations. The proposal complements the recently adopted Data Governance Act, which aims to facilitate the voluntary sharing of data by individuals and businesses and harmonises the rules on the use of certain public sector data. The proposal might be supplemented by additional, secondary legislation in specific sectors (e.g. car industry).

More concretely, the proposal for a data act aims to fulfil a range of **specific objectives**:

- facilitate access to and use of data by consumers and businesses, while preserving incentives to invest in ways that generate value through data. This implies bringing legal certainty to the sharing of data in the EU and clarifying the application of the Database Directive;
- enable the use by national public sector bodies and EU institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need;
- facilitate the switching between cloud and edge services;
- put in place safeguards against unlawful data transfers, without notification, by cloud service providers; and
- provide for the development of interoperability standards for data to be reused between sectors.

Scope

The proposed data act harmonises data sharing rules in a range of situations: between businesses, between businesses and public bodies, in the context of data infrastructure such as cloud services, or when non-personal data are transferred across borders into non-EU territories. The proposed legislation will lay down rules about data access and use in each of these situations.

Accordingly, the proposed regulation would apply to and create obligations for:

- manufacturers of products and suppliers of related services placed on the EU internal market as well as the users of such products or services;
- data holders that make data available to data recipients in the EU;
- data recipients in the EU to whom data are made available;
- public sector bodies and EU institutions, agencies or bodies that request data holders to make data available where there is an exceptional need;
- providers of data-processing services (e.g. cloud) offering them to customers in the EU.

Both **products** (i.e. connected devices) and **related services** would fall within the scope of the draft act. However, products that are primarily designed to display or play content, or to record and transmit content (e.g. personal computers, servers, tablets and smart phones, cameras) would be excluded from the scope) (Recital 15). Data generated by the use of a product or related service include data recorded intentionally by the user and data generated as a by-product of the user's action, such as diagnostics data. Data stemming from the interaction between the user and the product through a virtual assistant falls within the scope of the proposed regulation, while **data produced by a virtual assistant** unrelated to the use of a product does not.

Main provisions

Business to consumer and business to business data access and sharing measures

Right to access data

Chapter II (Articles 3-7) establishes a harmonised legal framework for making data generated by the use of a product or a related service available to the user of that product or service. In practice, the proposed data act would grant users (consumers or businesses) a new **right to access the data** generated by the use of products or related services (e.g. connected devices such as vehicles, consumer goods and industrial machinery).

Manufacturers would have to design their products in a way that allows the user to access the generated data easily by default and be transparent on what data will be accessible and how to access them. **Users** would be able to request access to their data by means of a simple request by electronic means whenever technically feasible. Where data cannot be directly accessed by the user from the product, the data holder should make them available to the user without undue delay, free of charge and, where applicable, continuously and in real time.

Data recipients can be any persons or businesses to whom the data holder makes its data directly available, but also a third party (such as an enterprise, a research organisation or a not-for-profit organisation) to whom data are made available at the request of the user (Recital 29). However, an important caveat is that large providers designated as '**gatekeepers**' under the Digital Markets Act would not be allowed to request or be granted access to users' data (Recital 36). Therefore, third parties to whom data are made available at the request of the user should not make the data available to a designated gatekeeper.

Data recipients would be subject to a set of further **limitations**, including the obligation not to use the data they receive to develop a product that competes with the product from which the accessed data originate (Article 6). Businesses' information protected under the [Trade Secrets Directive](#) would only be disclosed if all necessary measures are taken to preserve its confidentiality. In case of access to **personal data**, such data should be made available only if there is a valid legal basis under the GDPR (Recital 30). Finally and importantly, the proposed data act would 'not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities' (Recital 59).

Right to share data (enhanced portability right)

The proposed data act would also create a user's **right to share data with third parties**, complementing Article 20 the GDPR that establishes a right to data portability for data subjects (individuals). Such a right to share data would be much broader in scope than the GDPR portability right, as it would be granted to individuals and companies alike and cover both personal and non-personal data. Accordingly, **at the request of a user or a party acting on behalf of the user**, data holders would have to make available to third parties all the data that have been generated using a product or related service, i.e. data generated by IoT-connected devices and services.

SMEs exemption

In principle, micro- and small enterprises would be exempt from the obligations related to data access and data sharing under the proposal. In practice, such obligations would not apply to data generated by the use of products manufactured or related services provided by micro or small enterprises.

Obligations of data holders

Chapter III (Articles 8-12) imposes a number of **general obligations** on data holders. These include making data available under fair, reasonable and non-discriminatory terms and in a transparent manner; agreeing with the data recipient the terms for making the data available; not discriminating between comparable categories of data recipients, including partner enterprises or linked enterprises, of the data holder, when making data available; and not making data available to a data recipient on an exclusive basis unless requested by the user. Data holders **may receive compensation** for making data available, which should be reasonable and agreed with the data recipient. This does not preclude other EU or national legislation from excluding compensation or providing for lower compensation for making data available. In addition, any compensation set for SMEs would not exceed the costs incurred for making the data available, unless otherwise specified in sectoral legislation. In addition, a data holder '**should not abuse its position**' to seek a competitive advantage in markets where the data holder and a third party may be in direct competition (Recital 29). Finally, **dispute settlement bodies** certified by the Member States may assist parties that disagree on the compensation or conditions, to come to an agreement.

Unfairness of contractual terms in data sharing contracts between businesses

Chapter IV (Article 13) addresses the unfairness of contractual terms in data sharing contracts between businesses, with the aim to protect micro enterprises and SMEs. To this end, an **unfairness test** would have to be conducted according to a set of criteria, to assess if a contractual term is either always unfair or presumed to be unfair. This test would protect the weaker contractual party by ensuring that contracts remain fair in situations of unequal bargaining power. To the same end, clauses that do not pass this test would not be binding on micro and SMEs. Furthermore, the Commission would develop and recommend **non-binding model contractual terms on data access and use** (Article 34) to assist parties in negotiating agreements.

Exceptional mandatory business-to-government data sharing

Chapter V (Articles 14 to 22) creates a harmonised framework for the use by public sector bodies (and EU institutions, agencies and bodies) of data held by enterprises in situations where there is an exceptional need for such data. The proposed data act would thus oblige data holders to make data they hold available upon request to public sector bodies in two different scenarios in which an 'exceptional need to use data' can be established.

Under the first scenario, an exceptional need is deemed to exist where data are necessary to **respond to a public emergency** (Article 15(a)) or where data are necessary (for a limited time and for a limited scope) to **prevent or assist recovery from a public emergency** (Article 15(b)). In this case, an exceptional need would be justified when: a) the data are necessary to prevent or respond to a public emergency (e.g. public health emergency, natural disasters, major cybersecurity incidents); and b) the lack of data prevents public sector bodies from carrying out a task in the public interest (e.g. compilation of official statistics).

Under the second scenario, an exceptional need is deemed to exist where the lack of available data prevents a local authority from fulfilling a specific task explicitly provided by law in the **public interest** (Article 15(c)). Public authorities may then resort to the new provision to access data if they were unable to obtain such data by alternative means (including by purchasing the data on the market at market rates) or if the procedure set out in Chapter IV would reduce the administrative burden of collecting data.

In case of an exceptional need to respond to a public emergency data holders would be required to make data available **without delay and free of charge**. In other cases, including preventing a public emergency or assisting recovery from it, the data holder making the data available would be entitled to **compensation** that includes the costs related to making the relevant data available plus a

reasonable margin. Certain activities, such as the prevention, investigation, detection or prosecution of criminal or administrative offences, are explicitly excluded from the scope of exceptional needs.

Public sector bodies would be entitled to sharing the requested data with individuals or organisations carrying out **scientific research or analytics** or with national statistical institutes and Eurostat for the compilation of official statistics. Furthermore, the proposal envisages mutual assistance and **cross-border cooperation** between public sector bodies to ensure data exchange.

Switching between data-processing services, and interoperability requirements

Chapter VI (Articles 23–24) introduces a set of **minimum regulatory requirements to facilitate switching** between providers of cloud services and other data processing services. Given that the current self-regulatory approach under the [Free Flow of Non-personal Data Regulation](#) (i.e. codes of conduct on cloud switching) did not affect market dynamics significantly, the Commission intends to introduce regulatory measures to **avoid 'vendor lock-in'** concerns arising at the level of providers of data processing services.

Against this backdrop, the proposed data act would oblige providers to **remove commercial, technical and contractual restrictions** that make it difficult for customers to terminate a contract, conclude one or multiple new contracts with or port their data to another provider, among other things. In particular, it ensures that customers remain with a functional equivalence of the service after they have switched to another service provider. Furthermore, the Commission could mandate the use of **interoperability standards** or specifications for specific types of data processing services through delegated acts if necessary (Article 29).

In addition, Chapter VIII envisages the imposition of **interoperability requirements and data sharing mechanisms and services for operators of data spaces** that could be supplemented by way of delegated acts (Articles 28 to 30).

All those provisions would make it easier to move data and applications (from private photo archives to entire business administrations) from one provider to another without incurring any costs.⁵

Safeguards on access to data in an international context

Chapter VII (Article 27) puts in place safeguards to **address unlawful third-party access to non-personal data** held in the EU. The proposal requires data processing service providers to implement a set of technical, legal and organisational measures to handle access requests from authorities in non-EU countries to non-personal data held in the EU. Third-country court decisions or judgments requiring a provider to transfer or give access to non-personal data should, in principle, only be recognised or enforceable if based on an international agreement (e.g. a mutual legal assistance treaty). In the absence of such an agreement, transfer or access to such data by third-country authorities would be allowed only if specific requirements and safeguards are met (e.g. the third-country system requires a reasoned and proportionality-based assessment subject to a review by a competent court in the third country).

Databases

Chapter X (Article 35) amends the 1996 [EU Database Directive](#) to clarify that the specific legal protection envisaged under that directive (the sui generis right) does not apply to databases containing data obtained from or generated by the use of IoT products or related services (e.g. connected devices).

Enforcement and penalties

Chapter IX (Articles 31 to 34) lays down the implementation and enforcement framework. Member States would need to designate one or more competent authorities as responsible for the application and enforcement of the new rules. When more than one competent authority is

designated, the Member State should also designate a coordinating competent authority. Member States should also lay down the rules on penalties applicable to infringements of the regulation and notify the Commission of the designated competent authority or authorities and the rules on penalties.

Advisory committees

The [European Committee of the Regions](#) (CoR) and the [European Economic and Social Committee](#) (EESC) adopted their opinions on the proposed EU data act in June 2022.

National parliaments

The deadline for the submission of reasoned opinions on the grounds of subsidiarity was 16 May 2022. The [German Senate](#) (Bundesrat) and the [Czech Chamber of Deputies](#) submitted 'reasoned opinions'.

Stakeholder views⁶

Some of the main contentious points raised so far are listed below.

Objectives, scope and impact on innovation

BusinessEurope [calls](#) on EU lawmakers to preserve the contractual freedom businesses enjoy when it comes to data sharing, inter alia, by including rules that making data available would be adequately compensated and by ensuring clear enforceable obligations for third parties receiving data. Allied for Startups [recommends](#) using alternative approaches to mandatory obligations as a way to foster data access and re-use. Similarly, Digital Europe [argues](#) that some provisions will undermine companies' contractual freedom and have the opposite effect than intended. The organisation believes that it is important that data sharing agreements remain voluntary and commercially viable. It proposes that, instead, the EU should support and incentivise companies to share data, for instance, through schemes allowing companies to closely cooperate without falling under antitrust legislation. It also thinks that separate and targeted approaches to business-to-business and business-to-customer data access and sharing should be set out in the final text.

VDMA, representing European companies in the mechanical engineering industry, [argues](#) that the proposed data act should refrain from a general and undifferentiated obligation to make B2B machine data available, that data sharing in a B2B context should in general remain voluntary and based on contractual freedom. VDMA also believes that an obligation to share data might endanger investment in research and development. Along the same line, the Alliance for the Internet of Things Innovation (AIOTI) [asks](#) for clarifications on the scope of B2B and the B2G data sharing provisions. The European Automobile Manufacturers' Association (ACEA) [fears](#) that some of the requirements set by the proposal are simply unworkable and calls upon lawmakers to introduce and define a notion of 'accessible data', among other things. The Software Alliance [warns](#) that mandating data sharing – or, equally, restricting organisations from sharing or transferring data to third countries – would prevent EU businesses from reaping the full benefits of the digital transition and would render them less able to innovate and compete effectively in global markets.

BEUC, the EU consumer protection organisation, [stresses](#) that the proposed data act should ensure that customers are in control of their data, for instance, through a more simple-to-exercise data portability right that extends beyond personal data (so that they can, for example, take all their data from one service to another if they want to). DigitalEurope [stresses](#) that the proposed data act should apply to finished connected products (not to components embedded or integrated into another product), clarify that it is only applicable to raw data, and identify data holders based on the notions of control and ability to make data available. ACM, the Dutch competition law authority, [argues](#) that the proposed act could still be improved in terms of solving interoperability problems, in particular, by fostering the use of open standards for interoperability (and not only for switching).

Making data available to public sector bodies in exceptional circumstances

BusinessEurope is in [favour](#) of enshrining in EU law a limited set of 'exceptional need' situations that would entitle public sector bodies across the EU to claim data access. DigitalEurope also [stresses](#) the need for more stringent conditions to prevent the risk of public bodies misusing data supplied to them. The EDPB and the EDPS have expressed deep [concerns](#) about the lawfulness, necessity and proportionality of the obligation to make data available to public sector bodies and EU institutions, agencies or bodies in case of 'exceptional need'. The EDPB and the EDPS recall that any limitation on the right to personal data must have a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope. In accordance with the principles of necessity and proportionality, the legal basis must also define the scope and manner of the exercise of the competent authorities' powers and be accompanied by sufficient safeguards to protect individuals against arbitrary interference. The EDPB and the EDPS observe as well that the circumstances justifying the access are not narrowly specified and consider it necessary for the legislator to define much more stringently the hypotheses of emergency or exceptional need. Moreover, the EDPB and the EDPS consider that certain public sector bodies and EU institutions, agencies and bodies should be excluded from the scope of the regulation.

IP protections and trade secrets

DOT Europe [proposes](#) providing more robust safeguards for trade secrets, competition and IP to avoid undermining investments in innovation. AIOTI [recommends](#) expanding the scope of protection to cover not only trade secrets, but also confidential business data.

Cloud regulation, data portability and free-flow of data

AIOTI [recommends](#) clarifying data sharing requirements on design, manufacturing and mandatory elements to contracts, aligning data sharing obligations with industrial reality and promoting cooperation between providers to enable cloud switching. BusinessEurope [asks](#) for the removal of the proposed restrictions on the transfer of non-personal data, arguing, in particular, that SMEs would have to perform investigations on the laws of a third country, something that even large enterprises find challenging when it comes to compliance costs and business opportunities.

Enforcement

ACM [calls](#) upon EU lawmakers to set up an effective oversight mechanism to implement the proposed data act and coordinate the individual Member States' supervisory authorities. BEREC, the EU-wide group of telecom regulators, [calls](#) for the involvement of the national electronic communications regulators in the implementation of the future regulation. BusinessEurope [proposes](#) to set up a formal coordination and establish consistency, allowing for the identification of one single lead competent authority and an EU-level body able to make binding decisions. The organisation also wants a longer transition period of 36 months to allow for the development of relevant interoperability standards and for companies to prepare for compliance.

Academic views

Objectives, scope and impact on innovation

A study for the European Parliament⁷ suggests a data governance model based less on the commodification of data (i.e. enhancing access and sharing data for private profit) and more on the use of data in the public interest and on the recognition of collective data needs and rights.

More concretely, a range of concerns have been expressed about the provisions enshrined in the draft data act. Some experts warn that the design of the proposed user rights mechanism suffers from multiple problems (i.e. insufficient scope of data, lacking technical interoperability, high transaction costs) that will make it weak and largely ineffective.⁸ They argue the act should instead focus on setting easier data sharing and user empowerment mechanisms, especially for enabling more innovation in the data economy.⁹ The Centre on Regulation in Europe (CERRE) experts [warn](#)

that the proposal relies on an oversimplified definition of both the products and the relationship between users and data holders, which does not adequately reflect the complexity of the IoT scenario. They recommend clarifying the relevant definitions. Coherence with other legislative instruments including the Database Directive, the Open Data Directive and the Digital Markets Act has also been called into question.¹⁰ In that regard, a [European Parliament study on IPR](#)¹¹ proposes to amend the draft text, inter alia, in order to extend the scope of the new data access, sharing and use rights to certain larger (not purely data-processing, but data-driven) services that are not gatekeepers under the Digital Markets Act.

The Center for Data Innovation [warns](#) as well about the potential negative effects on the EU market economy and asks EU lawmakers to, inter alia, minimise the burdens of compliance and barriers to entry for all IoT companies seeking to provide their services to European consumers and clarify the effect on international data flows.

Making data available to public sector bodies in exceptional circumstances

The proposed act's data sharing requirements to the benefit of public sector bodies in exceptional circumstances are unclear. Some highlight that even though one could understand what constitutes 'exceptional circumstances' under Article 14 (e.g. the coronavirus pandemic), the situations covered by Article 15 are not clear-cut and the requirements set by Article 15(c) may prove challenging to meet.¹² In its abovementioned IPR study, the European Parliament asks EU lawmakers to reconsider whether the provisions on data sharing based on exceptional need should be extended to small and micro-sized enterprises.

CERRE [stresses](#) that the circumstances under which an exceptional need arises so that public bodies may request data access would require a clearer and narrower definition. Along the same lines, the Center for Data Innovation [believes](#) the Commission should further amend the proposed data act to clarify issues such as: the maximum period over which public institutions can hold business data; the security measures that must be in place to protect data shared with the public sector; and the steps a government agency needs to take to request B2G data sharing.

IP protections and trade secrets

Commentators [stress](#) that it is unclear how effectively any trade secrets will be protected in practice and there are calls for clarifying the relationship with intellectual property (IP) rights (especially with trade secrets legislation).¹³ The Max Planck Institute for Innovation and Competition welcomes the initiative but warns about a number of loopholes regarding how the proposed rules will interact with existing IP protection.¹⁴ The experts call, inter alia, for providing guidance on the applicability of programming interfaces (APIs) and the possible conflict that might exist if IP rights such as copyright and patents protect these APIs. The abovementioned European Parliament IPR study asks EU lawmakers to, inter alia, clarify that fair, reasonable, and non-discriminatory (FRAND) licences would cover necessary and justified-use acts for trade secrets.

Data protection and expansion of the scope of data portability rights in EU law

Experts have highlighted the interplay between the proposed data act and the EU data protection regime. Some authors [warn](#) that the proposed act might undermine the rules on personal data protection by giving more legitimacy to profit-driven personal data processing, and that the proposed act might be inconsistent with the goals of the GDPR, consequently precluding the consistent application of both sets of rules. Others are calling for clarification on how the free-of-charge requests for GDPR data portability relate to data access in the proposed act, given that it *does* foresee compensation, and warn that the prohibition on the data receiver to use the data it receives to develop a competing product may create legal risks.¹⁵ They also stress that the proposed data act's exclusion of gatekeepers from data access risks having little impact without further alignment with the scope of the GDPR's right to data portability.¹⁶ They therefore call upon EU lawmakers to amend the text by providing that the exclusion of gatekeepers from data access should also apply in the context of the GDPR's right to data portability.

Cloud regulation and free-flow of data

A [CEPS study](#) warns that the provisions on preventing international transfer of or governmental access to non-personal data held in the EU as well as the ones on cloud switchability are likely to deepen divides between national governments that are traditionally supportive of the principle of the free flow of (non-personal) data and those keen to localise industrial data within the EU. Similarly, CERRE [shares](#) the same concerns about data localisation in the EU and calls on EU lawmakers to delete this provision. Critics [warn](#) that the EU is struggling to build an EU cloud infrastructure and fear that the proposed data act will go toward data protectionism by favouring EU cloud providers over US ones. With regard to the provisions on switching between cloud and edge services, the European Parliament IPR study mentioned earlier proposes to envisage an exception for SMEs as providers (at least for B2B relations), to revise the relation to the DMA and to clarify the concept of 'functional equivalence'. Some have also argued that excluding online content services from switchability is unjustified and that the new right should be applicable to imported, (co-)created and (co-)generated data, applications and digital assets.¹⁷

Enforcement

Experts call upon lawmakers to consider aligning enforcement with the proposed data governance act in order to achieve synergies and to include a mechanism in the proposed data act determining which Member State is competent to act in cases of cross-border relevance.¹⁸ The European Parliament IPR study mentioned earlier proposes to clarify and strengthen the role of private law enforcement, to make the proposed public enforcement structures optional for the Member States, and to streamline them, at best by a one-stop shop approach including an EU 'meta authority' for data related topics.

Legislative process

In **Parliament**, the file has been assigned to the Committee on Industry, Research and Energy (ITRE) and Pilar del Castillo Vera (EPP, Spain) has been appointed as rapporteur. She unveiled her [draft report](#) in September 2022. She proposes, inter alia, to clarify the scope of the prospective regulation and how it applies to the different players; strengthen trade secret protection; extend SME exemption; clarify the implementation and enforcement rules; and impose fair remuneration as a matter of principle for making data available to public sector bodies in exceptional circumstances.

In the **Council**, the ministers supported the main objectives of the proposal and took note of [the progress report](#) presented by the French Presidency in May 2022. The Czech Presidency presented its [first compromise text](#) in September 2022. So far, discussions have focused on issues such as the scope of the proposal, the conditions according to which data would have to be exceptionally provided to public sector entities, restrictions for gatekeepers and SME exemptions.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

[Data act](#), initial appraisal of a Commission impact assessment, EPRS, European Parliament, July 2022.

[Governing data and artificial intelligence for all](#), EPRS, European Parliament, July 2022.

[IPR and the use of open data and data sharing initiatives by public and private actors](#), study, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, May 2022.

OTHER SOURCES

[Data Act](#), Legislative Observatory (OEIL), European Parliament.

ENDNOTES

- ¹ See European Commission, [Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data](#), 23 February 2022.
- ² See European Commission, [Impact Assessment report and support studies accompanying the Proposal for a Data Act](#), 2022.
- ³ *ibid.*
- ⁴ *ibid.* See Annex 4 explaining the challenges in implementing the Database Directive 96/9/EC.
- ⁵ See European Commission, [Data Act – Questions and Answers](#), 2022.
- ⁶ This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'.
- ⁷ See European Parliament, [Governing data and artificial intelligence for all – Models for sustainable and just data governance](#), July 2022.
- ⁸ See W. Kerber, [Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives](#), 2022.
- ⁹ *ibid.*
- ¹⁰ A. Fernandez, ['The Data Act: The Next Step in Moving Forward to a European Data Space'](#), *European Data Protection Law Review*, Vol. 8 (2022), Issue 1, pp. 108-114.
- ¹¹ See European Parliament, [IPR and the use of open data and data sharing initiatives by public and private actors](#), May 2022.
- ¹² See A. Christofi and B. Peeters, [B2G data sharing for smart city development in Europe: a first look at the Data Act Proposal](#) (Part II), 2022.
- ¹³ See I. Graef and M. Husovec, [Seven Things to Improve in the Data Act](#), 2022.
- ¹⁴ See J. Drexler and others, [Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data \(Data Act\)](#), Max Planck Institute for Innovation & Competition Research Paper No 22-05. See as well V. Moscon, [A Closer Insight into Copyright related Issues in the Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Proposal for a Data Act](#), June 2022.
- ¹⁵ See I. Graef and M. Husovec, above.
- ¹⁶ *ibid.*
- ¹⁷ See S. Geiregat, [The Data Act: Start of a New Era for Data Ownership?](#), September 2022.
- ¹⁸ See I. Graef and M. Husovec, above.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2022.

epprs@ep.europa.eu (contact)

www.epprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

<http://epthinktank.eu> (blog)

First edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.