CLIFFORD

CHANCE

THE DATA ACT: A PROPOSED NEW FRAMEWORK FOR DATA ACCESS AND PORTING WITHIN THE EU

THE DATA ACT: A PROPOSED NEW FRAMEWORK FOR DATA ACCESS AND PORTING WITHIN THE EU

On 23 February the European Commission (the "**Commission**") published a much-anticipated proposal for a Regulation on harmonised rules on fair access to and use of data, commonly referred to as the "**Data Act**". The content of the published proposal largely follows that of an earlier, leaked version, and confirms that the Commission is determined to push forward with its strategic vision on data, which it regards as an "*essential resource*" for digital and green transitions.

What is the Data Act and what does it aim to achieve?

The proposed Regulation seeks to redefine rules and practices on data access and use in order to foster data (re)use. The draft Act's declared objective is to ensure fairness in how the value of data is allocated among actors who are active on different levels of the data value chain, and ultimately, to unlock the potential of the data economy in the era of cloud computing and the Internet-of-Things ("**IoT**").

The key objectives of the proposed Data Act are: (i) to give IoT device users more control over the data they generate and its use; (ii) to enable use of privately held data by the national and EU public sector bodies in cases of "exceptional" data need; (iii) to improve switching between cloud and edge services; (iv) to restrict access by non-EU / non-European Economic Area ("**EEA**") governments to data held in the EU by providers of cloud and edge services; and (v) to remove barriers to data sharing by developing interoperability standards for data reuse.

The rules set out in the proposal would be directly applicable to all sectors and across the EU as minimum standards, though future revisions of sectoral regulations (*e.g.*, in the health, energy, finance, and automotive sectors) may go beyond these rules.

To which companies, products and services does the Data Act apply to?

By imposing requirements on the design and use of IoT products, the Data Act applies to basically all the players in the IoT chain, with particular focus on the IoT product manufacturers and the suppliers of related services, data holders (if different from the manufacturer / supplier), and the consumer or business user (who owns, rents or leases a product or receives a service). The proposed Data Act also contains provisions applicable to providers of certain digital data processing services and, in relation to sharing data with public bodies, provisions that apply to "data holders" more broadly.

The Data Act applies to the following products and services:

- **IoT products (referred to in the proposal as "products")**: Devices that generate or collect data concerning their use or environment and are able to communicate that data via a public network. These products may include vehicles, home equipment, consumer

goods, medical and health devices, and agricultural or industrial machinery. Devices for which the primary function is to store or process data do not fall within the scope of products to which the Data Act applies – which is likely to render items such as computers and smart phones out of scope.

- **Related services**: The digital services that are embedded in the IoT product or connected with it and are necessary for an IoT product to perform one of its functions.
- **Data processing services (such as cloud and edge services)**: Digital services that are provided to a consumer and which "*allow on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature*" are subject to provisions that seek to enable users to switch between these services more easily. This broad definition includes a wide spectrum of cloud and edge services.
- **Data holders:** The proposal also includes obligations on "data holders" to share data with public sector bodies and EU institutions in certain circumstances, and under the current drafting these obligations are not limited to those providing the products and services referred to above (see "*Business-to-Government Data Sharing Obligations*" below for further information).

Article. 1(2) of the proposal limits the territorial scope to the IoT products and related services that are "*placed on the market in the [European] Union*," and to providers of data processing services "*offering such services to customers in the [European] Union*".

Business-to-Consumer and Business-to-Business data sharing obligations

The proposed Data Act foresees far-reaching data sharing obligations. As a starting point, manufacturers of IoT products and related services, including voice assistants, will need to ensure data access by design: by default, personal and non-personal data generated by the use of in scope products and related services must be easily accessible to users. This includes data generated when the device is in stand-by mode or switched off. However, according to the proposal, output data inferred or derived from the analysis of the data collected or generated by the IoT product (*e.g.*, data produced by machine learning software) is not covered.

Users must be provided with clear pre-contractual information on a number of points including the nature and extent of collected data, how data might be used (including by third parties), and how users can access the data.

Scope of obligations on data holders to provide data access to users upon request. Where a user requests access to their data, the data holder is obliged to make available to the user the data generated by their use of a relevant product or service, without undue delay, free of charge, and, where applicable, continuously and in real time. The proposed Data Act does not set out the scenarios in which data would need to be provided continuously and in real time. Data holders should already start thinking about the practical aspects for providing access to data in line with this obligation, as some of the practical implications are likely to be burdensome.

The proposed Data Act puts further important constraints on the data holder, which will be allowed to use non-personal data generated by the product or related

Which Products will the Data Act apply to?

… A virtual assistant acting as the single gateway in a smart home environment? **Yes.** Virtual assistants may record a vast amount of data on how users interact with connected home appliances.

… Automated robots deploying machine learning software? **No.** The recitals of the proposed Data Act suggest that it will not apply to data resulting from software processing, such as machine learning, that calculates derivative data.

… A smart TV with pre-installed voice command? **Yes.** The voice command runs on a public network and processes data about the user (*e.g.*, voice, selected service, etc.)

What does the Data Act mean for you if you are an IOT manufacturer?

Product development considerations: The Data Act requires manufacturers to make data collected by, or generated by the use of, their IoT products accessible to users by default in an easily readable and downloadable format.

User contract considerations: The Data Act requires IoT manufacturers and data holders to be transparent as to what data will be accessible to users and how to access the data. The Data Act pushes for transparent data monetisation contracts (including data licensing and data sharing/ transfer agreements), detailing how data may be exploited throughout the 'data chain' (from the user to data recipients).

Data sharing considerations: The Data Act provides that, if a manufacturer stores the data the IoT product collects or generates, it must make the stored data available to third parties upon the request of the user. The data holder must apply fair and non-discriminatory conditions for access, and compensation requested for the data must be reasonable.

service only based on a contract with the user. This rule could greatly hinder data holders' ability to exploit data and may require important adaptations to obtain user consent prior to data use.
For example, providers of connected agricultural equipment will be allowed to use the information generated about an agricultural machine's performance only on the basis of a contractual agreement with the user.

Users will also be able to request that data generated by their use of a product or related service be provided to third parties. Those third parties can process such data only for the purposes and under the conditions agreed with the user and must delete such data when it is no longer necessary for the agreed purpose. The Data Act sets out a number of limitations on the use of such data, including an obligation to respect trade secrets and to abstain from obtaining data via coercive or abusive means. In addition, third parties must not use such data to develop products that compete with the product from which the data originates.

The proposal prohibits data holders from using the data generated by a product's use to gain insights about the economic situation of users or authorised third parties, or other similar business-sensitive information that could undermine their commercial position. While the specifics of such information are not spelled out in in the proposal, data holders may potentially need to set up data silos and/or introduce strict internal data access policies, in order to comply with this obligation.

The Data Act contains a significant carve-out in terms of third parties that may receive data under the Act, prohibiting the transfer of such data to any undertakings designated as "gatekeepers" under the proposed Digital Markets Act ("**DMA**").

What are the terms of data access under the Data Act? The proposed Data Act also aims to set regulatory standards for the *conditions* of data access and use. Consistent with its approach to data as a non-rivalrous good, the proposal prohibits data access on an exclusive basis, except when this is directly requested by the user. Moreover, when data sharing is mandated by national or EU rules, data holders will have to provide access on fair, reasonable and non-discriminatory ("**FRAND**") terms. Notably, the proposal provides that any data-related compensation must be reasonable and must not discriminate between comparable categories of data recipients. Using data to give an advantage to data holders' partners or linked enterprises is also prohibited. The question as to what constitutes FRAND terms is complex and has given rise to abundant litigation (*e.g.*, in the context of licensing standard essential patents). The Data Act foresees specialised national dispute settlement bodies, to rule on disputes between data holders and data recipients. The European Commission will further, similar to the standard contractual clauses (SCCs) under the GDPR, put in place model clauses to assist parties in complying with the Data Act.

Although the proposed Data Act provides for the relevant parties to agree on the terms of access to data, certain provisions seek to protect micro, small, or medium-sized enterprises against (non-price-related) unfair contractual terms. An overarching definition of unfair contractual terms is provided in the proposal, *i.e.*, terms that "*grossly deviate from good commercial practice in data access and use, contrary to good faith and fair dealing.*" The proposal also contains a list of terms deemed to be unfair per se (such as *e.g.*, unilateral exclusion of liability, unilateral exclusion of legal remedies, or unilateral interpretation rights with regard to data-related contractual provisions) and

"Gatekeepers" within the meaning of the DMA prohibited from receiving data under the Data Act

The proposed Data Act intends to prohibit the transfer of data under the Data Act to any undertaking designated as a "gatekeeper" under the yet to be adopted DMA.

If an undertaking is designated as a gatekeeper under the DMA, the data sharing prohibitions under the Data Act apply to all group companies of that undertaking (*i.e.*, not only the relevant legal entity that provides the core platform service which designates it as a gatekeeper). The gatekeeper and its group companies must ensure that they do not request (or receive) access under the Data Act to any user data generated by the use of a product or related service, or by a virtual assistant, from any third-party data holder. Gatekeepers will be prohibited from incentivising or soliciting users to share the data with them, and even from accepting the data that the user obtained by exercising data access rights described above. Third party recipients of user data are also prohibited from sharing data with the gatekeepers under the proposed DMA.

For any companies considering whether they are at risk of being designated as a gatekeeper, they may wish to consider in parallel what safeguards they might put into place to ensure that they do not solicit – or receive – data under the proposed Data Act.

a list of contractual terms that are presumptively unfair (such as *e.g.*, limitation of legal remedies in cases of breach of contract, unduly limiting data use, unilateral termination of contract, *etc.*).

Business-to-Government data sharing obligations

Mandatory business-to-government data sharing in cases of exceptional need. Specific provisions of the proposed Data Act create a framework for access by public sector bodies (including Member States' national, regional or local authorities as well as EU institutions and agencies, together, "**Public Bodies**") to data held by private data holders, such as companies (excluding small and microenterprises). Under the current drafting of the proposed Data Act the business-to-government data sharing requirements apply to a broader range of data than the business-to-business data sharing obligations: the "data holders" who may receive data requests from Public Bodies includes any legal or natural person who has the right or obligation under EU laws (and implementing Member State laws) to make available certain data, in addition to those who have the ability to make data available through their control of the design of IoT products and related services.

Under this proposed framework, Public Bodies will be able to request access to such data in cases of exceptional need. The proposal published by the Commission contains a longer list of "exceptional needs" than was set out in the leaked draft of the Data Act. In the current proposal, the need to respond, prevent or assist with recovery from a public emergency (*e.g.*, natural disasters, pandemics, terrorist or cyber-attacks) qualifies as exceptional. Another exceptional need would arise where it is impossible for the Public Body to fulfill a specific mission of public interest provided for by law due to the unavailability of data (subject to certain additional conditions). It will be interesting to follow how the concept of "exceptional need" develops as the proposal goes through the legislative procedure, where the recitals of the proposed Data Act already note that the existence of a public emergency would be determined according to the respective procedures in the Member States, and hint that other situations may be covered by the concept of "exceptional need," such as the need for timely compilation of official statistics under specific conditions.

In addition to the requirement for Public Bodies to justify requests made under these provisions, such requests must be proportionate with respect to their scope and granularity, must preserve the confidentiality of data revealing trade secrets, and Public Bodies must only use obtained data for the defined purpose and delete it as soon as it is no longer needed (unless agreed otherwise with the data holder). Notwithstanding these procedural limitations, Public Bodies can share obtained data with other entities (including national statistics institutes and Eurostat) under certain conditions, including where necessary for scientific research or analytical activities compatible with the purpose of the data access request, which the Public Body cannot perform itself. Public Bodies would also be allowed to exchange obtained data with other Public Bodies to address the exceptional needs for which the data has been requested.

What about sharing mixed data sets in response to a Public Body request? The Data Act contains specific guidance on making available mixed data sets (*i.e.*, containing both personal and non-personal data) to Public Bodies pursuant to an access request. The relevant data holder must prioritise sharing of anonymous data if possible. If not, the

The Data Act and the GDPR

The proposed Data Act will complement existing rights and obligations under data protection laws such as the GDPR, and should be read in parallel with such laws. The recitals to the proposal make clear that the Data Act should not be applied and interpreted in any way that would diminish the protection of data provided for under the GDPR.

The Data Act aims to facilitate the exercise of certain rights that have proven to be difficult to exercise in practice, such as the right to data portability. The right to data portability (as laid down in Article 20 of the GDPR) provides for the right of data subjects to receive personal data concerning them, in a structured, commonly used, and machine-readable format, and to port that data to other controllers. Under the Data Act, the scope of the right to data portability is broadened and includes any data generated by the use of a product or related service regardless of the nature or origin of the data (whether personal and non-personal, passively or actively provided) or, in relation to personal data, the legal basis for its acquisition under GDPR. The provisions facilitating switchability between data processing services also appear to have been loosely inspired by the GDPR's portability rights.

The proposal's restrictions on international transfers of non-personal data by data processing services providers somewhat echo the international transfer restrictions under the GDPR but do not mirror them exactly – *e.g.*, they do not include the exceptions to the restrictions that are available under the GDPR.

data holder must pseudonymise or aggregate data prior to making it available to the extent that the request can be fulfilled with pseudonymised/ aggregated data. Thus, unless data is completely anonymous, GDPR rules may also apply to the process of making data available, including the requirement to have a valid legal basis for processing.

Possible justifications for refusing a Public Body's data access request. The Data Act specifically sets out possible bases for requesting the modification or the cancellation of an access request, namely where the requested data is unavailable or the request does not meet the conditions set out for requesting access to data based on an exceptional need. Where the data holder can show that the request for access to data in a public emergency is similar or identical to a previously submitted request for the same purpose by another Public Body, the data holder may potentially refuse to provide access.

Financial compensation for data holders. Except for requests related to a public emergency, where data requests are based on exceptional need – including for the prevention of or recovery from public emergencies – data holders are entitled to (limited) compensation from the relevant Public Body for granting data access.

Relationship to other business-to-government data sharing regulatory frameworks. These new business-to-government data sharing rules envisaged by the proposed Data Act are without prejudice to voluntary public-private sector arrangements for data sharing, other legal frameworks providing for mandatory data sharing between private entities and Public Bodies (*e.g.*, pursuant to reporting and single market obligations), data access for the purposes of compliance verifications by Public Bodies, and sectoral legislation providing for data access by Public Bodies for law enforcement purposes.

Additional requirements specific to data processing services

Data processing service providers (*e.g.* cloud and edge service providers) will be obliged to facilitate user switching between data processing services. The proposal seeks to remove contractual, economic, and technical barriers to switching of data processing services by, *inter alia*, facilitating contract termination and making it easier for users to enter into contracts with new service providers and to port data (including meta-data) generated by customers' use of the service. The proposal requires that data processing service providers provide assistance to customers to enable them to achieve functional equivalence when switching toa new IT environment, and that charges related to switching between data processing service providers be fully eliminated three years after the Data Act comes into force (and gradually diminished beforehand).

Promotion of interoperability envisaged. The proposed Data Act requires compliance with open standards and interfaces, where these exist, and contains provisions that would empower the Commission to adopt common specifications where it considers that existing harmonised standards are insufficient in relation to certain interoperability requirements.

Limitations on ex-EU/EEA data transfers. The proposed Data Act also seeks to limit access to European non-personal data by non-EU/EEA governments. The proposal obliges data processing services to prevent international transfer or governmental

The Data Act and the EU-UK Trade and Cooperation Agreement

With respect to transfers of data from the EU to the UK, it is unclear how the proposed Data Act would interact with the provisions protecting the free-flow of data in Article 201 of the Trade and Cooperation Agreement ("**TCA**") between the EU and the UK, which entered into force 1 May 2021. The TCA provides for these provisions to be kept under review and for their functioning to be assessed within three years of the date the TCA came into force, so this interaction may be clarified either as part of this anticipated assessment or as part of the legislative development of the Data Act.

The Data Act and IP protections

The proposed Data Act intersects with existing rules in the areas of intellectual property and the legal protection of trade secrets.

Under the Data Act, users can demand access to information that would fall under the scope of Directive (EU) 2016/943 (the "**Trade Secrets Directive**"), thus covering data information that would be considered a trade secret. The Data Act states that trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of the trade secrets. Although the proposal states that the data holder and the user can agree on measures to preserve the confidentiality of the shared data, in particular in relation to third parties, and that trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party, it is unclear how effectively any trade secrets will be protected in practice

Directive 96/9/EC (the "**Database Directive**") establishes, under certain circumstances, a *sui generis* **IP** protection for databases. The proposed Data Act stipulates that the *sui generis* right established in the Database Directive, does not apply to databases containing data from or generated by the use of IoT products or related services.

access to non-personal data held in the EU where such transfer or governmental access would create a conflict with EU law.

How will the obligations in the Data Act be enforced?

National competent authorities. Each Member State must designate at least one competent authority as responsible for applying and enforcing the Data Act, whether it be an existing authority or a new one established for the purpose. Where there is overlap with laws governing the protection of personal data, or where specific sectoral data exchange issues arise, the competence of relevant data protection or sectoral authorities (respectively) must be respected..

Penalties. Each Member State must lay down rules for "*effective, proportionate and dissuasive*" penalties for violations of the Data Act. The proposed Data Act suggests that these are envisaged as being mainly in the form of administrative fines. As this suggests a national rather than EU-wide penalty regime, it should be noted that fines could vary from country to country for the same violations. For infringements involving overlap with existing data protection laws, the supervisory authorities established under such laws may impose penalties in line with such laws.

What happens next?

The draft Data Act will now pass to the European Parliament and Council for adoption according to the ordinary legislative procedure. While it is difficult to predict the length of time required for Parliament and Council to reach consensus, this it is likely to take between 18 months and two to three years. A reasonable estimate for formal adoption of the Data Act would be sometime between late 2023 and early 2024. The next European Parliament elections will be held in spring 2024, providing an obvious target date for reaching agreement. The Commission has proposed that the new rules should apply 12 months following their publication in the Official Journal. Given that the Commission has proposed an EU Regulation (as opposed to a Directive), the Data Act will be directly applicable once adopted, rather than dependent on individual Member States enacting national provisions to bring the Data Act into force. It will be key, therefore, for affected data holders to be prepared in advance to comply with the access and data sharing obligations set out in the final form of the Data Act.

CONTACTS

EU

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Thomas Voland
Partner
Düsseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Dieter Paemen
Partner
Brussels
T: +32 2 533 5012
E: dieter.paemen@cliffordchance.com

Josep Montefusco
Partner
Barcelona
T: +34 93 344 2225
E: josep.montefusco@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Gail Orton
Head of EU Public Policy
Paris
T: +33 1 4405 2429
E: gail.orton@cliffordchance.com

Milena Robotham
Counsel
Brussels
T: +32 2 533 5074
E: milena.robotham@cliffordchance.com

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Susanne Werry
Counsel
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

Rita Flakoll
Senior Associate Knowledge Lawyer
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

Ketevan Zukakishvili
Lawyer
Brussels
T: +32 2 533 5918
E: ketevan.zukakishvili@cliffordchance.com

Carmen Puscas
Senior Associate
Brussels
T: +32 2 533 5094
E: carmen.puscas@cliffordchance.com

Preslava Eneva
Avocat
Paris
T: +33 1 4405 5379
E: preslava.eneva@cliffordchance.com

Sophie Wijdeveld
Associate
Amsterdam
T: +31 20 711 9214
E: sophie.wijdeveld@cliffordchance.com

US

Soniya Ambadkar
Trainee Solicitor
Paris
T: +33 1 4405 8382
E: soniya.ambadkar@cliffordchance.com

Megan Gordon
Partner
Washington
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

APAC

Brian Harley
Consultant
Hong Kong
T: +85228262412
E: brian.harley@cliffordchance.com

Sharon Zhang
Registered Foreign Lawyer
Hong Kong
T:+85228258888
E: sharon.zhang@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

J2016 2203-000040