DIGITALEUROPE

1 SEPTEMBER 2022

Rebalancing the Data Act

Executive summary

With the data economy estimated to account for only 3 per cent of Europe's GDP,[1] the Data Act must unlock European companies' full potential to develop new digital solutions. Whilst all the right ambitions have been outlined in the European Commission's proposal,[2] numerous changes will be necessary to ensure the final text can be an enabler of Europe's data aspirations – rather than stifling them.

The proposal would impose across-the-board horizontal rules obliging data sharing, as opposed to more flexible enabling measures to spur voluntary sharing. However, there is little, largely circumstantial evidence to justify radical measures, which can on the contrary directly impact companies' entrepreneurial freedom and economic opportunities without any tested macroeconomic benefits.

The final Data Act should allow companies much more predictability about what it covers, what obligations apply, and how the rules will be enforced.

In particular:

- Central definitions must better delimit the proposal's nature and impact. The final Regulation should apply to **finished connected products**, clarify its applicability only to **raw data**, and identify data holders based on the notions of **control and ability** to make data available.
- Proper limits to data availability must be incorporated in order to avert incentives for data misuse and anticompetitive behaviour. This must include: a clear **exemption of trade secrets** and an acknowledgement of the risk of 'reverse-engineering' for **confidential business data**; protections against the development of **competing products and services**; clearer **obligations and penalties against data misuse** by data recipients; and a recognition of the need for data holders and data recipients to **agree suitable contractual and compensation terms**.

[1] European Data Market study, SMART 2013/0063, IDC, 2016.

[2] COM(2022) 68 final.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- Much more **stringent conditions** must be set out to **prevent the risk of public bodies' misuse** of data supplied to them, and to ensure the key criteria of **lawfulness, necessity and proportionality** under Union law are fulfilled.
- The final switching rules for cloud service providers must better reflect the **variety of cloud services**, the **volume and complexity** of data stored and processed on them, and the **shared responsibilities** between cloud providers and customers.
- The proposed **restrictions concerning international access and transfer must be removed**. Although they are aimed at non-personal data, these rules address laws (such as the US CLOUD Act and e-evidence) that will tend to involve personal data and are already covered by the General Data Protection Regulation (GDPR).[3] They would only bring further uncertainty to companies' international operations, which have already been severely tested by the *Schrems II* ruling.[4]
- A **formal coordination and consistency mechanism** must be established, allowing for the identification of one single lead competent authority and an EU-level body able to make binding decisions. This is vital to prevent what would otherwise be an inevitable multiplication of both interpretation and enforcement by a disparate set of authorities.
- **Clearer rules on the relationship with the EU data protection and privacy frameworks** must be stipulated. Importantly, the Data Act should require authorities to assess what elements of cases before them might involve personal data or mixed datasets, and should therefore be yielded to the competent data protection authority (DPA) instead.
- A **longer transition period** of 36 months to allow for the development of relevant interoperability standards and for companies to prepare for compliance.

[3] Regulation (EU) 2016/679.

[4] C-311/18. For more on this point, see DIGITALEUROPE, *Data transfers in the Data Strategy: Understanding myth and reality*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-data-strategy_Understanding-myth-and-reality.pdf.

Table of contents

Main definitions

Several definitions, all of which are crucial in delimiting the precise nature and impact of the proposal, must be clarified.

Data

The proposal uses the term 'data' too broadly. Under this broad definition, it not only equally covers personal and non-personal data, but also fails to distinguish between further types of data.

Indications as to the scope of the 'data' definition are provided only in Recitals 14 and 17. Recital 14 states that the definition should include 'user actions and events,' but exclude 'information derived or inferred from this data.' Similarly, Recital 17 excludes 'data resulting from any software process that calculates derivative data.'

Both recitals appear, correctly, to want to limit the definition to 'raw' data, that is, to data that has not undergone any processing beyond mere collection. This is welcome, as the inclusion of derived, inferred or otherwise further processed data would inherently impinge on proprietary information, commercially confidential data, trade secrets and intellectual property rights.

For this reason, **the definition of 'data' in Art. 2(1) should be replaced with a new definition clarifying its applicability only to raw data, and explicitly excluding derived, inferred or further processed data.**

Sectoral considerations

The Data Act's horizontal definition of data should not conflict with existing and in-development sectoral legislation. In healthcare, the European health data space proposal contains additional provisions for electronic health data in its scope, overlapping with, but also going beyond the Data Act.[5] For the financial sector, recitals should specify that data related to payments is not in scope, as such data is covered specifically by the Payment Services Directive (PSD2),[6] as noted by the Commission in its recent consultation on an Open Finance Framework.[7]

In line with our recommendations regarding the 'data holder' definition below, the final Regulation should clarify that data that is not under the data holder's

[5] COM/2022/197 final.

[6] Directive (EU) 2015/2366.

[7] The consultation document (p. 3) states that the Data Act 'does not introduce any new data access rights in the financial sector.' European Commission, *Targeted consultation on open finance framework and data sharing in the financial sector*, available at https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/2022-open-finance-consultation-document_en.pdf.

control – for example, data that is encrypted or processed locally on a device and is therefore not accessible by the data holder – is excluded. The text should also clarify that it does not oblige data holders to store data for longer than necessary for the purposes of complying with the Data Act.

Further exclusions must be provided in Recital 17. This recital states that the definition should include 'also data generated as a by-product of the user's action,' including diagnostics and other technical data. At a minimum, the recital should exclude 'volatile' data, that is, data that is only temporarily stored and then deleted, for instance when a device is switched off.

Finally, it must be considered that even raw technical data can expose trade secrets and other proprietary information. Likewise, direct access to raw technical data, such as device logs, could make devices vulnerable to security risks. Appropriate safeguards and exclusions should therefore be mentioned under this recital.

Product

The proposal's definition of 'product' in Art. 2(2) must be circumscribed to ensure a proper scope.

In line with our position on the upcoming Cyber Resilience Act,[8] we urge that **the final Regulation should refer more precisely to 'connected products,'** with the following definitions:

- Connected product: A finished product that is intended to communicate directly or indirectly over the internet. Products that are primarily designed to store and process data, or to display, play, record and transmit content, are excluded.[9]
- Finished product: A product usable for its intended purpose without being embedded or integrated into any other product. Components of a device, such as a processor or a sensor, are excluded.

We welcome the proposal's clarification under Recital 15 that products that are primarily designed to display, play, record and transmit content should be excluded, along with related services. We believe this should be mirrored in the definition of 'connected product.' We also suggest that the list of examples contained in Recital 15 should be expanded to include TVs, printers, IP phones, video game consoles, video surveillance cameras, videoconferencing endpoints, ATMs, point-of-sale terminals, bank cards and digital wallets.

[8] See DIGITALEUROPE, *Building blocks for a scalable Cyber Resilience Act*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf.

[9] We note that the expression 'connected product' is already found, but not defined, in the proposal (see Recitals 16 and 18).

Data holder

The proposed definition of ‘data holder’ at Art. 2(6) is purely circular and therefore ineffectual. All it does is state that a data holder is someone who is obliged by the Regulation, or other EU or Member State law, to make data available.

The goal of this definition should be to allow **clearer identification of what single entity in the value chain will qualify as ‘data holder’ in a given scenario**.

From this perspective, the final text should build on the proposed definition specifying the central concurrent criteria of:

- *Control* over the data; and
- The *ability* to make it available.

This may be the connected product’s manufacturer or the provider of a related service. This will ensure that the right actor in the value chain, having control over the relevant data, is responsible for ensuring access to data generated by the use of its own offerings.

The definition of ‘data holder’ must recognise that **manufacturers may themselves not be in control of the data generated by a device**, and should therefore not be singled out.

For example, devices may run third-party applications (including from data recipients pursuant to the Data Act) that are not under the manufacturer’s control. Likewise, data may be encrypted or processed locally on a device, and therefore not accessible by the manufacturer. Similarly, the diversity and complexity of contractual agreements behind the provision of related services might prohibit one of the parties, including manufacturers, from accessing data.

If an entity has no access to data itself, i.e. if it does not ‘hold’ data, it cannot qualify as a data holder. As suggested, this should be reflected by centring the final definition around the notion of control *of the data* (as opposed to the mere ‘technical design of the product and related services’ in the current version as well as in Recital 19).

These changes to the definition would also clarify that obligations fall on the data holder as the ‘data controller’ as opposed to entities acting as ‘data processors,’ both terms being well understood from the GDPR. Recital 21 should be modified to this end to reflect that, in case the remote server to which the data is communicated ‘belongs to a third party acting as data processor on behalf of the data holder, the obligations pursuant to this Regulation shall be incumbent on the data holder as data controller under Regulation (EU) 2016/679.’

Related services

The proposal's definition of 'related service' could capture *any* service or piece of software that interacts with a connected product.

Instead of requiring merely that the absence of a service 'would prevent the product from performing one of its functions,' Art. 2(3) should refer more strictly to a **product's 'intended purpose,'** in line with EU product legislation.[10]

User

Art. 2(5) qualifies a user indistinctly as any 'natural or legal person that owns, rents or leases a product or receives [related] services.'

In particular due to the latter part of this definition – which relies on the vague notion of 'receiving' a service – this might generate uncertainty as to whether both legal entities, e.g. a company, and individuals, e.g. that company's employees, might be able to access and use the same data.

The final Regulation should draw a firmer distinction between business-to-consumer (B2C) and business-to-business (B2B) scenarios in order to ensure that data holders have clarity as to whom data should be provided to pursuant to the Data Act.

To this end, **the final 'user' definition should only refer to the 'natural or legal person that owns, rents or leases a connected product.'** This will help ensure that contractual relationships involving connected products, and the related data sharing obligations, can be more clearly identified as either B2C or B2B.

The reference to 'receiving' related services in the proposed definition is unhelpful. In any event, it is unnecessary given the 'related service' definition, which should clearly link services to a product's intended purpose, as we have suggested.

Other definitions

Other definitions would benefit from further specification:

- The definitions of 'data processing service,' 'service type' and 'functional equivalence' ignore certain specificities of B2B software.[11] In the cloud sector, different services can offer a number of features that may be comparable or overlapping with competing offers but are not delivered the same way – often at the customer's request –

[10] The notion of 'intended purpose' is used, among others, in Regulation 2019/1020 (market surveillance), Directive 2014/53/EU (radio equipment) and Regulation 2017/745 (medical devices).

[11] Arts 2(12)–(14).

making the proposal's portability and interoperability requirements difficult or impossible;[12]

- 'Virtual assistants' are in scope alongside products and related services. Recital 22 indicates that the intention is to capture assistants that act as a 'gateway' to third-party devices in the home/consumer environment, but the definition in Art. 2(4) neither distinguishes between B2B and B2C nor fully reflects that such assistants are expected to control third-party devices. Such distinctions should be made in the text to ensure hardware that embeds virtual assistants but is not otherwise in scope is not captured;
- Relevant definitions stemming from the GDPR, including at a minimum 'data controller,' 'data processor' and 'data subject,' should be introduced with full reference to the GDPR; and
- A definition of 'main establishment' as 'the place of the data holder's central administration in the Union' should be introduced in line with our recommendation in the 'Enforcement' section below.

Data sharing obligations

The Commission has opted for across-the-board horizontal rules obliging data sharing, as opposed to more flexible enabling measures to spur voluntary data sharing. This choice is regrettable given the little, and largely circumstantial, evidence backing the proposal.

One central study referenced in the impact assessment has expressly recognised profound limits to its findings:

> *The data economy is in the 'emergence phase' of a new market. The vast majority of European businesses are still considering how they will integrate these technologies into their business models. Consequently, the results of the study inevitably come from a relatively small group of proactive users of [third-party] data, IoT, robots and autonomous systems.*
>
> *… The small number of cases and the difficulty for the companies themselves of knowing the true scale or cost of barriers that are still emerging put limits on meaningful quantification.*[13]

Absent stronger evidence showing widespread market failure, mandatory horizontal measures should be carefully weighed, as they will directly impact

[12] See 'Switching rules for cloud service providers' section below.

[13] Pp. 14–15, *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*, prepared by Deloitte for the European Commission, available at https://op.europa.eu/o/opportal-service/download-handler?identifier=74cca30c-4833-11e8-be1d-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=.

data holders' entrepreneurial freedom and economic opportunities without any tested macroeconomic benefits.

Transparency

We support the **inclusion of mandatory information that must be made available to users under Art. 3(2)**. Such information will help users understand what data they have access to and exercise their rights under the Regulation.

In practice, these requirements may overlap with the GDPR's transparency requirements – certainly in cases where users are data subjects.[14] We therefore believe that the final Regulation should allow data holders to present the relevant information along with the GDPR-required information, and that the European Data Protection Board (EDPB) should be tasked with developing Guidelines to this end.

We believe that information about the 'volume' of data at Art. 3(2)(a) is unnecessary, and in many cases impossible to estimate upfront. It is also of little value, particularly where the user is a data subject. We therefore urge that its provision should be required only 'where appropriate.'

Necessary limits to data availability

Art. 3(1) sets out a general requirement to design products and services in a manner that makes data available to the user by default, with a preference for direct access. Art. 4 grants users access rights when data cannot be accessed directly, whilst Art. 5 establishes users' right to share data with third parties.

We support these general principles. At the same time, their practical realisation will be far from straightforward. The final Regulation should therefore not only remain general, but also better acknowledge limits and exceptions to the general rules in subsequent provisions.

Competing products and services

Arts 4(4) and 6(2)(e) state that the user and any third party cannot use data to develop a product that competes with the product the data originates from. These provisions are particularly important, including due to their link with the protection of confidential business data, trade secrets and intellectual property rights.[15]

Although in principle commendable, these clauses are not sufficiently specific to provide any appreciable guarantees.

---

[14] Chapter III GDPR, notably Sections 1–3.

[15] See section below.

For all practical purposes, they shift the burden onto the data holder to demonstrate not only that a trade secret has been used, but that its use specifically breaches an obligation not to compete with the original product. In case of misuse, the proposal even states that competing offerings may not have to be terminated if they have 'not caused significant harm' or 'would be disproportionate.'[16] This generates very significant incentives for misuse. Additionally, the proposal does not foresee the possibility that a third party could be accessing various competitors' trade secrets to develop its own products against several original products.

Provisions against anticompetitive behaviour should be strengthened thus:

- They should apply not only to directly competing products, but also to components of a product, to related services including software, and to existing competing products already on the market. In particular, the significance of services for manufacturers' value propositions cannot be overestimated, and goes well beyond aftermarket activities;
- Arts 4(6) and 5(5) – stipulating the data holder should not 'derive insights about the economic situation, assets and production methods of or use by' the user or third parties that could 'undermine' their 'commercial position' – should be mutually applicable to both the user and third parties vis-à-vis the data holder;
- Art. 11(3) allowing competing offerings by data recipients in case of data misuse should be deleted; and
- The competent authorities' tasks under Art. 31(3) should explicitly include market surveillance and investigation of non-compete violations.

Trade secrets, confidential business data and databases

We are particularly concerned by the superficial treatment given to trade secrets in the proposal. At present, the text effectively forces disclosure of trade secrets to users, third parties and public bodies if necessary for the purposes pursued by them, and only loosely refers to 'necessary' or 'appropriate' measures to preserve confidentiality.[17]

These very loose safeguards, combined with the proposal's timid non-compete provisions and requirements to share data 'continuously or in real-time,'[18] make it exceedingly easy for both users and third parties to misuse trade secrets. Among other things, the proposal does not specify the consequences of a user or third party disagreeing with the non-disclosure

[16] Art. 11(3) of the proposal.

[17] See to this effect Arts 4(3), 5(8) and 19(2) of the proposal.

[18] See, in particular, Arts 4(1) and 5(1) of the proposal.

agreement provided by the data holder – a presumption against the data holder might on the contrary be inferred in this case, similar to the non-compete clauses.

Access to data by current or future competitors should not jeopardise the acquired know-how of data holders.

Rather than focusing on confidentiality as a mitigation, the final Regulation should **clearly exempt trade secrets from its scope, with a full reference to Directive (EU) 2016/943, which should take precedence**.

Presently, the proposal's reference to the Directive at Art. 8(6) is effectively null and void, as full precedence is given instead to the Data Act provisions as well as to any other EU or Member State law to the contrary. This directly contradicts the claim in the explanatory memorandum that the proposal does not affect the legal protection of trade secrets.[19]

The final Regulation should explicitly provide in Art. 6 that data recipients shall not use data to 'derive insights about the economic situation of the data holder or its assets or production methods or the use in any other way that could undermine the commercial position of the data holder on the markets it is active on.'[20] It should acknowledge the risk of 'reverse-engineering' – whereby trade secrets or the data holder's know-how may be obtained from data which in and of itself may not appear to contain protected information – and explicitly state that there is no obligation to share trade secrets or information considered to be confidential, and that the disclosure of trade secrets should only be voluntary and subject to appropriate safeguards to be agreed contractually between the data holder and the user or third parties.

Another key concern stems from the proposed exclusion of data to be shared pursuant to the Data Act from the Database Directive's *sui generis* right.[21]

Whilst the objective to avoid an artificial use of this right to evade data holders' sharing obligations is meritorious, the current formulation of Art. 35 goes beyond this goal and would exclude from the *sui generis* right not only the relevant data but also any mixed or aggregated databases containing such data.

Databases merit protection, in particular because substantial investments can go into presenting or verifying their contents. These conditions can still be met by databases containing product- and service-generated data.

To remedy any unintended consequences, **rather than revoking the *sui generis* right altogether, the final Regulation should clarify that it**

[19] P. 5 of the explanatory memorandum accompanying the proposal. We note that this might also contravene the EU's and Member States' obligations under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). See Council Decision 94/800/EC.

[20] This provision would mirror Arts 4(6) and 5(5) equally protecting users and third parties vis-à-vis the data holder.

[21] Directive 96/9/EC.

'cannot be invoked to hinder the effective exercise of rights provided for' in the Data Act.[22]

Penalties and remedies for data misuse by data recipients

Art. 33 of the proposal refers generically to 'penalties applicable to infringements,' and allows Member States full flexibility to determine the relevant rules and measures.[23]

The final Regulation should clarify that infringements can stem not only from data holders but also from data recipients. Appropriate dissuasive financial penalties should therefore explicitly be envisaged for violations under Art. 6.

Beyond penalties, competent authorities, dispute settlement bodies pursuant to Art. 10 or courts should mandate generally applied remedies in case of data misuse. This means referring to the remedies mentioned in Arts 11(2)(a) and (b) but also extending them to cover economic losses and moral prejudice.

Cybersecurity

The confidentiality, integrity and availability of a device or service can directly be compromised when data (e.g. device logs) is shared. This is particularly the case for obligations to share data 'continuously or in real-time.'

The proposal's Art. 11 allows data holders to apply appropriate technical protection measures to prevent unauthorised access and ensure compliance with the Regulation's provisions as well as with agreed contractual terms.

This article should, however, refer more broadly to **technical and contractual measures to ensure that third-party data access does not endanger the integrity of products and related services**. In line with the current language, these measures should be possible so long as they are not abused with the aim to evade the rights provided for in the Regulation.

Contractual terms and fairness

Arts 8 and 13 of the proposal both place the burden of proof on the party supplying the terms to demonstrate that they are fair or not unilaterally imposed. Art. 13, whilst purportedly applying only to SMEs, describes terms that are presumed to be unfair also under Art. 8.

The lists contained in Arts 13(3) and (4) are vague and therefore inconclusive, relying on terms such as 'inappropriately,' 'significantly detrimental,'

[22] For more on this and IPR-related issues in the context of the proposal, see Toby Bond and Katharine Stephens, 'Why IP lawyers need to pay attention to the EU's draft Data Act,' Bird & Bird Insights, available at https://www.twobirds.com/en/insights/2022/uk/why-ip-lawyers-need-to-pay-attention-to-the-eus-draft-data-act.

[23] Arts 33(3)–(4) merely repeat that DPAs are in any event competent for data protection penalties based on data protection rules, in addition to any penalties under the Data Act.

'proportionate' or 'unreasonable.' Considering this – and given that the general principle of 'fair, reasonable and non-discriminatory terms' is already established by Art. 8, and that the necessary rights for users and third parties are already outlined in Arts 4 and 5 – **Art. 13 should be deleted**.

Dispute settlement bodies pursuant to Art. 10, as well as courts, will be able to determine fairness in light of Arts 4, 5 and 8. It is unclear under Art. 10 which Member State authorities would be in charge of certifying dispute settlement bodies and overseeing their work. In order to ensure that dispute resolutions do not differ too greatly across Europe, Art. 10 should task the Commission to adopt guidelines for Member States and dispute bodies.

Fairness determinations should place the burden of proof on data recipients. A presumption against the data holder is very difficult to overturn, as it is harder to prove something has not happened than the contrary. In addition, it will be close to impossible for the data holder to search forensic data in a separate, external service. Data recipients, by contrast, not only will have stronger proof of negative impacts, but will have strong incentives to provide such proof as they directly stand to benefit from data sharing.

Ultimately, we believe that raising awareness regarding contractual data sharing arrangements and providing support to companies, particularly smaller businesses, would have a much more positive impact on companies' capacity to find the right data partnerships. To this end, **we support the Commission's proposal in Art. 34 to draft non-binding model contractual terms** which companies could use as a basis for their negotiations.

Compensation

Collecting, curating and making data available implies significant costs for companies. Notably, setting and managing the infrastructure and internal processes to support access requests from data recipients will require major investments by data holders. To help the data economy continue to grow, companies should be incentivised and able to obtain a fair remuneration for sharing data.

Beyond contractual terms in general, proposed Art. 9 imposes a specific fairness test for compensation by stipulating it should be 'reasonable.' Such reasonableness must be literally proved by the data holder, who is required to provide 'information setting out the basis for the calculation of the compensation in sufficient detail.'[24] In addition, Art. 9(2) stipulates compensation should not exceed cost when data is provided to SMEs, whilst Art. 9(3) stipulates that other EU or Member State law can in any event provide for lower or no compensation.

[24] Art. 9(4) of the proposal.

Provisions on compensation are a direct restriction to companies' entrepreneurial freedom and economic opportunities, which are particularly unjustified in the absence of clear evidence of market failure.

As such – rather than stipulating a *de facto* presumption against data holders, which may in itself force them to disclose sensitive financial information – the final Regulation should **recognise the need for data holders and data recipients to agree suitable compensation terms**. It should include a non-exhaustive list of elements that the parties should consider in their agreement, which at a minimum should include fair remuneration for collecting and curating data. Dispute settlement bodies pursuant to Art. 10, as well as courts, will ultimately be able to settle issues related to compensation based on the non-exhaustive elements listed in Art. 9.

In some sectors, SMEs have become an essential part of the data value chain. As more and more SMEs are expected to develop data-driven business activities and collect data for selling and sharing in the coming years, the Art. 9(2) provisions could disincentivise the development of data-driven models on the part of SMEs. For instance, a medium-sized company could itself be obliged to share its data with other parties, including other SMEs, pursuant to the Data Act, but Art. 9(2) would prevent it from covering its data collection and curation costs. Art. 9(2) should therefore be deleted.

As with contractual terms more in general, guidance to market players regarding compensation will also result from the non-binding model contractual terms drafted by the Commission pursuant to Art. 34.

Finally, we find Art. 9(3) particularly unhelpful. The Data Act should attempt to set out solid general rules applicable to data sharing, with compensation being a particularly important economic component thereof. Rather than limiting itself to recognising that other laws can detract from it, the final Regulation should **stipulate strict conditions under which other EU or Member State law might derogate from its provisions**, including on compensation.

Legacy clause

Existing contracts governing data sharing should be clearly exempted from the final Regulation.

Retroactive provisions on data already generated or acquired under existing contracts would impose excessive burden on companies. For instance, products and services already placed on the market may not have been designed to handle the data management provisions stemming from the Regulation, and may no longer be supported by software updates.

Such **exemption should apply to all products that have been placed on the market before the entry into application of the Regulation, and related services contracted before that date**.

Gatekeeper exclusion

The proposal's Art. 5(2) excludes 'gatekeepers' subject to the Digital Markets Act (DMA) from being able to receive data as a third party.[25]

The DMA already contains specific provisions addressing gatekeeper behaviour, and the use of further legislation to address the same perceived issues would be disproportionate. This is particularly the case as the Data Act is based on explicit rights for users to share data. As such, **users should be able to share data with any third party of their choice**. The gatekeeper exclusion should therefore be deleted.

Sharing based on exceptional needs

The digital industry has been providing data to help tackle societal challenges as part of partnerships with public institutions across Europe. We fully understand the importance for public bodies to receive data in specific emergency situations, for instance where health and public safety may be at stake at a large scale.

DIGITALEUROPE believes that the proposal's Chapter V presents specific issues that require changes to ensure sufficient legal certainty. It must be considered that the use of data by public authorities must meet a particularly high test of lawfulness, necessity and proportionality under Union law, as has been stressed numerous times by the Court of Justice of the EU (CJEU).[26]

Any data request entails a risk of misusing, misreading or misinterpreting the data supplied by the private sector. The business-to-government (B2G) provisions should therefore **better define key concepts and provide more safeguards to prevent any abuse of the provisions or misuse of data** that is being shared. In particular:

- Art. 2(10)'s definition of 'public emergency' should be narrowed by providing more objective criteria for determining the type, the timeframe and the magnitude of the actual or expected negative effects. This should be done via an exhaustive list under Art. 15.

  Art. 15(b), which refers to prevention of and recovery from a public emergency in addition to letter (a)'s general provision, is open to excessive discretion and should be deleted.

  Recital 57 lists 'major cybersecurity incidents' as an example of a public emergency. However, entities are already subject to specific rules and obligations on cybersecurity information sharing under the recently reformed EU framework for the security of network and

[25] COM/2020/842 final.

[26] See cases C-293/12, C-203/15, C-698/15, C-623/17, C-511/18, C-512/18, C-520/18 and C-746/18, C-140/20.

information systems (NIS2) as well as sectoral frameworks such as the Regulation on digital operational resilience for the financial sector (DORA).[27] Moreover, a separate proposal concerning cybersecurity rules for digital products and ancillary services is expected.[28] The reference to 'major cybersecurity incidents' should therefore be deleted.

- The definition of 'public sector body' (Art. 2(9)) covers all entities governed by public law and associations thereof. This can include public undertakings and other mixed public-private entities, as well as public research institutes. The final Regulation should limit this definition to specifically identified bodies in relation to the 'specific task[s] in the public interest' that merit attention.
- The obligation for companies to provide data when it is necessary for public bodies to fulfil a 'specific task in the public interest' (Art. 15(c)) circumvents the requirement for the necessary conditions and safeguards for data processing by the public body to be themselves explicitly provided by law. This includes the types of data to be processed, the entities the data can be disclosed to and for what purposes, storage periods and more.[29]

  The conditions in Arts 15(c)(1) and (2) refer in essence to it being more convenient for public bodies (or for unspecified 'other enterprises') to directly request data pursuant to the Data Act rather than by other means. These provisions are baseless and excessive, and should be deleted.
- Art. 19 in its current, generic formulation, is insufficient to provide by law the necessary conditions and safeguards for data processing by public bodies. This article should focus not only on safeguards after data has been received, but also on safeguards pertaining to public bodies' data collection in the first place. The conditions around data requests under Art. 17(2) cannot serve this purpose.
- Similar to Arts 4(5) and 5(6) for users and third parties, any sharing of personal data with public authorities should only happen in full respect of the EU data protection and privacy frameworks. At present, Chapter V attempts to minimise its data protection implications by requiring data requests to 'concern, insofar as possible, non-personal data' and by forcing data holders to 'take reasonable efforts to pseudonymise the data.'[30] For public authorities, Chapter V should instead explicitly require the existence of an appropriate legal basis, with specific

[27] COM/2020/823 final and COM/2020/595 final, respectively.

[28] See DIGITALEUROPE, *Building blocks for a scalable Cyber Resilience Act*.

[29] See Art. 6(3) GDPR.

[30] Arts 17(2)(d) and 18(5), respectively.

reference to Art. 6(3) GDPR. As we argue above, the necessary conditions should be stipulated in a new version of Art. 19.

- Art. 18 should provide both data holders and data subjects (in cases where personal data may be involved) with more extensive rights to challenge data requests, as well as to seek judicial remedy. The final Regulation could, from this perspective, draw inspiration from the e-evidence proposal that is still being debated.[31]
- Penalties should be explicitly foreseen in case public bodies breach their obligations.

Compensation

We support the principle that data made available to respond to a public emergency should be provided free of charge.[32]

However, the final Regulation should recognise the right for data holders to exceptionally request compensation, even in case of public emergencies. This should be triggered by a request from the data holder that could be based on the same elements as proposed Art. 20(2). In addition to anonymisation, reference should also be made to pseudonymisation to reflect the additional costs data holders may incur pursuant to Art. 18(5).

In case of opposition from the public body, such requests could be adjudicated by the competent authority, by a dispute settlement body pursuant to Art. 10 or by courts.

Conditions for reuse

The risk of data shared by companies being further reused or reshared as public-sector data, for instance pursuant to the Open Data Directive or to Chapter II of the Data Governance Act,[33] should be adequately addressed.

Whilst Art. 17(3) provides reassurance pertaining to the Open Data Directive, further sharing with other public bodies and third parties is foreseen by Art. 17(4), with Art. 19 stipulating the only applicable conditions.

We urge that Art. 17(3) should specifically refer also to the Data Governance Act. In addition, Art. 17(4) should be narrowed by reference to the more limited definition of 'public sector body' and the 'specific task[s] in the public interest' that the sharing obligations are meant to support.

---

[31] COM/2018/225 final.

[32] Art. 20(1) of the proposal. However, our support is contingent on a more stringent definition of 'public emergency,' as we explain above. As we have argued, we urge that public emergencies should be the only basis for Chapter V requests, and that the other cases of exceptional need in Arts 15(b) and (c) should be removed.

[33] Directive (EU) 2019/1024 and Regulation (EU) 2022/868, respectively.

Additionally, Art. 21 should further specify the conditions under which research organisations or other bodies can have access to data received pursuant to this Chapter. Proper safeguards are needed to prevent any possibility that companies' data may be misused, including for anticompetitive behaviours.

Safeguards for data holders

Further safeguards compared to current Arts 17 and 19 are needed to ensure that data holders' data will be protected and not used against them.

For instance, outsourcing to third parties under Art. 17(4) should be subject to explicit protections against anticompetitive behaviour and to ensure that use of the data would be strictly confined to the outsourced activities.

To ensure compliance with Art. 19 and good governance practices, public bodies should be required to inform data holders about how they complied with their obligations pertaining to the requested data. Member States should be required to report annually to the Commission on the requests made by national public bodies. The Commission should in turn be tasked with compiling an annual EU-wide report which should also list EU institutions' requests and include recommendations and good practice for public bodies to follow.

Finally, data holders should not be held liable for data they share with public bodies pursuant to the Data Act. For this reason, the final Regulation should include a provision stipulating that **data holders should be immune from liability for their good-faith compliance** with Chapter V obligations.

EU harmonisation

Our suggested modifications to Chapter V should limit the risk of a fragmented interpretation and implementation of the B2G provisions, notably in the way they would restrain Member States' discretion around the definitions of public emergencies or public sector bodies.

In addition, it will also be important for Art. 22 of the final Regulation to set out more binding provisions to facilitate collaboration and avoid fragmentation.

Art. 22 should clarify that the Data Act sets **maximum harmonisation**, thereby preventing a multiplication of Member State derogations. The Commission should be tasked with developing guidelines and monitoring Member States' use of the provisions.

Coordination should include **pan-European requests**, in order to avoid the cumbersome process currently foreseen by Arts 22(3) and (4). To this end, clarifications to Art. 18(3) are needed to state that 'previously submitted request for the same purpose by another public sector body' includes other Member States' bodies as well.

Incentivising voluntary sharing

The proposal does not reference voluntary B2G data sharing, even though companies have increasingly been developing partnership programmes with public institutions to share data, either regularly or on a need basis. Examples of this include efforts aimed to support the fight against climate change and to contain the COVID-19 pandemic.

The final Regulation should acknowledge the existence of B2G partnerships and foster their expansion as an alternative to mandatory data requests. This would be beneficial for both public bodies and data holders, notably by reducing compliance burden (drafting data access requests, addressing potential challenges, defining compensation costs, etc.). Such partnerships should of course develop in full compliance of the EU's data protection and privacy frameworks.

Putting in place attractive compensation mechanisms or commercial data acquisition and licensing agreements with companies could be a more efficient way to achieve the objective of providing the public sector with data. Incentives – direct (e.g. monetary) or indirect (e.g. reputational) – would allow companies to overcome the various risks and barriers associated with data sharing, notably data preparation costs.

Finally, public bodies often possess a lot of data which often remains unused or underused. In some cases, such as when the requested data has already been provided in response to previous requests, B2G access requests would not be needed if data was made more available within the public sector. B2G partnerships can help governments identify, categorise and curate their data to make it usable.

Switching rules for cloud service providers

DIGITALEUROPE supports easier and cost-effective switching between cloud services to foster competition and user choice.

The proposal, however, should be amended to better reflect the variety of cloud services, the volume and complexity of data stored and processed on them, and the shared responsibilities between cloud providers and customers.

Additionally, specific characteristics of a given cloud project, such as its architecture complexity, project timeline and pricing model, can also impact the switching process.

Differentiating types of services

The proposal does not consistently distinguish between infrastructure-level services – infrastructure-as-a-service (IaaS) – which are relatively standardised and easier to transfer, and software services higher up in the

application stack – platform-as-a-service (PaaS) and software-as-a-service (SaaS) – which are more complex, often tailor-made and not perfectly interchangeable.

Whilst the proposal recognises this difference in Art. 26, there remains uncertainty regarding whether the notion of 'functional equivalence' is expected to apply indistinctly.[34] The final Regulation should recognise that even if interoperability standards or specifications were to be defined,[35] **there remain operational and technical limits to switching because SaaS/PaaS services are not built onto identical architectures**.

Even cloud-native applications, which allow code to be run on different infrastructure stacks, may have dependencies in their operation. They may rely on backend public cloud services, e.g. to validate the code, and have written specific scripts for that purpose that will not work when the underlying infrastructure is changed. Relying on those backend services, or building the whole SaaS service to a single IaaS provider's technology stack, reduces development cost and complexity. If a SaaS service must remove existing dependencies, costs can become exorbitant. And if SaaS services need to be completely cloud agnostic in the future, it also means they need to avoid using any new, innovative backend services from the IaaS providers as they are not replicable on other platforms. The problem is even worse for switching between cloud and on premise,[36] which are architected in an entirely different manner and might involve a complete rewrite.

In setting the rules to negotiate contracts, the final Regulation should allow flexibility reflecting the great variety of services on the market. For instance, it could allow parties to agree *ex ante* on mandatory transition periods according to the expected complexity of the switching process.

Service types and interoperability

Beyond our considerations above, the proposed requirements can only be fulfilled if large-scale harmonisation of functionalities of data processing services is achieved on a cross-vendor basis, resulting in practice in all services being identical. Besides obvious competition concerns, this would ultimately limit the possibility for customers to use cloud and data services matching their unique needs and prevent the development of more innovative offerings.

[34] See, for instance, Recital 72.

[35] Art. 26(2) also requires PaaS and SaaS providers to make open interfaces publicly available free of charge, without defining what makes an interface 'open' or how the requirement is articulated around the functional equivalence requirement in Art. 26(1).

[36] Art. 24(1)(a) of the proposal.

In the context of interoperability standards and specifications for SaaS/PaaS services, difficulties are likely to emerge in defining what the 'same service type' means.[37]

There may be tens or hundreds of thousands of cloud service types in existence today. To serve as a useful construct for fostering switching opportunities, **'service types' need to be narrowly focused on competing services that offer the same *basic* functionality**.

Whilst this may be better addressed in sectoral standards development processes rather than legislation, one guardrail in the final Regulation could be the **need to demonstrate that two services actually compete for customers and offer the same basic functionality** before deciding they need to be interoperable for switching purposes.

To give an example of why this is necessary, take SaaS services that only make sense within the environment of the vendor's own offerings – such as aggregating data from the vendor's various SaaS services into a single platform for ease of operational orchestration by the customer. Whilst other vendors may produce similar services that relate to their own offers, they are simply not relevant outside their own ecosystem, so whilst the service type is similar at face value, requiring such services to be switchable is meaningless.

Functional equivalence

The proposal's notion of 'functional equivalence,' and the requirement for providers to 'ensure full continuity in the provision of the respective functions of services,'[38] should reflect that offerings between providers will often not be identical, and that data processing services cannot be fully aware of all the functionalities, security or performance levels of data processing services offered by other providers.

Some workloads and features may be provider specific, that is, part of the data processing service itself. They cannot be ported to another provider or may only be ported with limited functionality. Workloads may even be hardware specific, for instance with trial and evaluation of cloud-based services for potential customers. Requiring full equivalence and continuity would prevent providers from offering any applications and services which their competitors are not proposing to customers, thus reducing competition, incentives to innovate and customer choice.

The final Regulation should instead **ask customers to engage in due diligence and provide sufficient information regarding their technical needs and expectations and, on that basis, require providers to ensure their best efforts to make the data and workloads available**, based on

[37] Art. 29, ibid.

[38] Arts 26(1) and 24(1)(a)(2), ibid., respectively.

customers' demands and the capabilities of the cloud service upon which the data is to be ported.

Additionally, clarification is needed on the notion of 'obstacle' referred to in Art. 23(2). Whilst 'commercial, technical, contractual and organisational obstacles' may exist and complicate switching, some of these obstacles, particularly technical ones, may not be surmountable in some cases. It should also be noted that only customers have a complete overview of the technical and organisational requirements needed for their migration programme, whereas providers (incumbent or new) may only guess certain obstacles that could complicate switching in a given case. Thus, this paragraph should clarify that it only addresses obstacles that are directly influenced by providers and significantly impact switching processes.

Cooperation between providers

The proposal envisions cloud and data switching as a relatively straightforward transfer of stored data, which is getting more common in a B2C context. For the B2B landscape, however, switching complex service offerings requires the cooperation of both the former provider (transferring data) and the new provider (receiving it). The proposal disregards this reality and largely places switching obligations on the former provider.

By comparison, telecoms regulation places switching and portability obligations on both the transferring provider and the receiving provider, as well as Member States.[39] Such scenarios are arguably far more straightforward than cloud and data processing, yet they have taken many years and significant investments to be fully implemented.

Only collaboration between the customer,[40] the former and the new provider can help achieve effective switching. This should be reflected in the allocation of roles and responsibilities for the different parties, ensuring that **relevant obligations apply so long as all parties cooperate and offer sufficient support** to the switching process.

Switching timeframe

Setting a general notice period of 30 days,[41] whatever the type of contract, is likely to be highly disruptive, especially for existing fixed-term contracts whose price and features have been tailored to a specific duration – for instance because a company only needs the service for a limited period, or to secure a service over a longer period at a reduced price. Such contracts benefit both providers and customers, notably by helping plan costs over a set duration.

[39] Art. 106, Directive (EU) 2018/1972.

[40] As well as, if applicable, the third party engaged by the customer.

[41] Art. 24(1)(a) of the proposal.

Providers would no longer be able to propose attractive multi-year contracts if no penalties for early termination were allowed. As a result of such limitation to contractual freedom, contract prices will tend to increase. The **final Regulation should therefore explicitly allow parties to agree on minimum contractual terms with customers**.

The proposal also sets forth a 30-day deadline (extendable to maximum six months) for switching, regardless of the volume and specifications of the cloud workloads at hand.

This timeline will be unrealistic for moving large workloads, which may comprise many cloud-based applications and services sitting across multiple hosting servers. These can easily be multi-year projects for larger contracts. The more data is exported, the longer the switching period.

These obligations do not take into account the possibility for both parties to simply negotiate the right type of data switching for each customer. Cloud users may have specific needs, for instance wanting to port only part of the data and keep some data and services hosted within their current cloud solution, or to plan a transition over a period longer than six months.

For these reasons, the final Regulation should explicitly **allow providers and customers to agree on alternative transition periods longer than six months**. Such alternative transition periods would be suited to the level of complexity of the architecture, the array of services provided and the volume of data processed.

Exportable data and applications

More flexibility – reflecting, in particular, risks to trade secrets – is also needed on the categories of data and the types of workloads (applications, services, etc.) that are included.

Art. 24(1)(b) refers to ‘all data and metadata created … by the use of the service.’ In some cases, data derived from usage may have been aggregated or mixed with third-party sources, and its communication could infringe their rights.

Disclosure of such data also poses a risk to PaaS/SaaS services provided by device manufacturers who have developed infrastructure and diagnostic systems. Transfers of configuration parameters, security settings, access rights and access logs amount to conveying detailed information about the service provider’s internal processes and know-how.

Further, the term ‘metadata’ is particularly vague, and may vary in nature from service to service but also depending on the industry field. For instance, in the medical sector, the notion of ‘metadata’ may include digital imaging and communications in medicine (DICOM) metadata, which contains trade secrets. The transfer of DICOM metadata to competitors would enable them to train AI models in a similar quality but without the underlying investment

into R&D and innovation. Similar side effects could emerge with other sector-specific uses of cloud services.

Existing frameworks

The final Regulation should refer to and promote existing cloud and data initiatives to further enable switching. Importantly, these include SWIPO,[42] which successfully developed industry codes of conduct on cloud switching and porting pursuant to the Free Flow of Non-Personal Data Regulation.[43]

Additionally, a considerable amount of work is taking place in international fora to develop global standards and norms enabling interoperability for cloud and data processing.[44] These existing efforts should be leveraged and considered when setting a framework for European harmonised standards and specifications under the Data Act, and as part of other initiatives such as Gaia-X.

Building on existing initiatives will help promote transparency-based standards and specifications – thus also helping cloud users in their due diligence when comparing offerings and choosing a service.

International access and transfer

DIGITALEUROPE is particularly concerned by the introduction of new restrictions to data transfers in the proposal.

Proposed Art. 27 introduces what amounts to a framework for data transfers parallel to the GDPR that would only bring further uncertainty to companies' international operations, which have already been severely tested in light of the CJEU's *Schrems II* ruling.

In particular, we note that whilst Arts 27(2)-(5) stipulate rules applicable only in case of data access requests from third-country authorities, Art. 27(1) does not appear limited to such situations and instead introduces a general requirement applicable to data transfers *tout court*, requiring transfers to be prevented where they could conflict with EU or Member State law.

As we demonstrate at length in a separate report,[45] although it aims to regulate transfers of non-personal data, the proposal actually addresses laws that will tend to involve personal data and are already covered by the GDPR (particularly when it comes to rules meant to address the US CLOUD Act and e-evidence).

---

[42] https://swipo.eu

[43] Regulation (EU) 2018/1807.

[44] Such as ISO/IEC 19941:2017 on cloud interoperability and portability.

[45] DIGITALEUROPE, *Data transfers in the Data Strategy: Understanding myth and reality*.

We note that the Deloitte study supporting the proposal's impact assessment recognises itself that, although it is *theoretically* possible for non-personal data to be involved in cases of conflict of law at international level, 'in the typical scenario personal data will be involved.'[46] We note that the state of play in the study always makes a theoretical point about non-personal data, but never provides actual examples, particularly with respect to the US laws mentioned therein.

In addition to these substantive issues, uncertainty for companies would be exacerbated by the possibility that these rules might be interpreted and enforced by disparate authorities, with little or no consistency mechanism, as we highlight in the following section.

We urge that **Art. 27 should be deleted** in full.

Enforcement

Of great concern to DIGITALEUROPE is also the considerable potential for fragmentation, in both interpretation and enforcement, that would result from the proposal and from the broader Data Strategy.

Proposed Art. 31 envisages the possibility for Member States to designate one or more competent authorities. As an additional stipulation, Arts 31(2)(a)–(c) explicitly protect the competence of DPAs for anything related to personal data, that of any sectoral authorities for the sectors under their jurisdiction,[47] and – in what appears to be an indirect reference – that of national telecoms authorities. What is more, the proposal does not envisage any rule ensuring that data holders and providers of data processing services are only subject to enforcement by one lead competent authority – meaning that they are concurrently exposed to enforcement by competent authorities in each Member State. This is in addition to the one or more authorities Member States can designate under the Data Governance Act as competent bodies assisting public sector bodies, competent authorities for 'data intermediation services,' and competent authorities for 'data altruism organisations.'[48]

We estimate that potentially, this would allow up to a dozen authorities to interpret and enforce the Data Act, along with other applicable law, in any given situation and in each Member State. This presents an inherent, extensive risk to legal certainty for companies that must be remedied.

The Data Governance Act has created a new European Data Innovation Board, in the form of a European Commission expert group, to assist in

[46] P. 201, *Study to support an Impact Assessment on enhancing the use of data in Europe*, study carried out for DG CONNECT by Deloitte, The Lisbon Council, The Joint Institute for Innovation Policy, The GovLab, Timelex and The Open Data Institute.

[47] Notably, those Member States will designate pursuant to the European Health Data Space proposal, COM(2022) 197 final.

[48] Regulation (EU) 2022/868.

implementation.[49] This will be a composite group gathering representatives of the competent authorities under the Data Governance Act (but, oddly, not the Data Act), the EDPB and the European Data Protection Supervisor (EDPS), the European Union Agency for Cybersecurity (ENISA), the European Commission, the EU SME Envoy or a representative of the network of SME envoys, and 'other representatives of relevant bodies in specific sectors as well as bodies with specific expertise.' As an expert group, this Board will have a purely advisory role. Unlike the GDPR's EDPB, the Board will have no formal cooperation and consistency mechanism, and no possibility to adopt binding decisions. Similarly, the Data Act merely stipulates a duty of cooperation between the competent authorities (both of other Member States and within the same Member State) and 'as appropriate' between such authorities and the DPA of their own Member State.[50]

By generating such multiplication of competent authorities without any formal coordination and consistency mechanisms, the Data Strategy acts as a deterrent to, rather than a facilitator of, the EU's single market.

The final Regulation should:

- Oblige Member States to designate **one single competent authority**, setting out **clearer tasks, powers and independence** requirements;
- Subject data holders and providers of data processing services to enforcement by the **lead competent authority of their main establishment**;
- Establish a **formal cooperation and consistency mechanism**, ensuring collaboration between the lead competent authority and the other competent authorities concerned. It should establish an independent EU-level body with legal personality to ensure the Data Act's consistent application, leading to legally binding decisions in case of disputes between competent authorities; and
- Require competent authorities, including in the context of the cooperation and consistency mechanism, to perform a **mandatory assessment of what elements of cases before them might involve personal data or mixed datasets, and should therefore be yielded to the competent DPA** instead.[51]

The GDPR and ePrivacy

The tension with personal data – including mixed datasets, which are subject to the same treatment – and terminal equipment data will be intrinsic to the Data Act's data sharing obligations. The proposal's relationship with the EU

[49] Art. 29, ibid.

[50] Arts 30(3)–(4) of the proposal.

[51] See section below.

data protection and privacy frameworks, therefore, deserves more careful and explicit consideration.

At present, the proposal only includes general stipulations that aim to preserve the scope and safeguards contained under the GDPR and the ePrivacy Directive.[52] This will prove insufficient, and on the contrary will merely increase opportunities for inconsistent interpretations and enforcement by the various authorities at play. As we have argued in the previous section, this decreases legal certainty for companies and must be remedied.

By way of an example, a data holder may be required to transfer data to a third party following a decision from the competent authority under the Data Act, and later be found by a DPA to have illegally further processed data because the data subject had not given explicit consent to the processing of their biometric data pursuant to Art. 9(2)(a) GDPR for this specific data sharing scenario.

In addition, because the Data Act is based on the premise of sharing data from connected products, including core services related to such products, there appears to be a complete overlap with the concept of 'terminal equipment' under the ePrivacy Directive.[53] Importantly for this complete overlap, it must be stressed that ePrivacy at present covers both personal and non-personal data when it comes to terminal equipment.[54] In light of existing uncertainty around the interpretation of Art. 5(3) of the Directive and its relationship with the GDPR, as well as protracted negotiations pertaining to the proposed Regulation replacing it,[55] failure to appropriately consider ePrivacy now will impact the applicability of the entire proposal.

In order to minimise inconsistencies and the risk of conflictual interpretations, the final Regulation should:

- In line with our recommendation in the section above, require competent authorities, including in the context of the cooperation and consistency mechanism, to **assess what elements of cases before them might involve personal data or mixed datasets, and should therefore be yielded to the competent DPA** instead;
- Create a **specific legal basis** for the 'storing of information, or the gaining of access to information already stored, in the terminal

[52] See, in particular, Arts 1(3) and 31(2)(a), the latter concerning the competent authorities.

[53] Directive 2002/58/EC, as modified by Directives 2006/24/EC and 2009/136/EC.

[54] See *DIGITALEUROPE's consolidated position on ePrivacy Regulation*, available at https://www.digitaleurope.org/resources/digitaleuropes-consolidated-position-on-eprivacy-regulation/. See also, specifically on this point, the 'Relationship with ePrivacy and legal grounds for processing' section in our *Response to EDPB draft Guidelines on connected vehicles and mobility-related applications*, available at https://www.digitaleurope.org/resources/response-to-edpb-draft-guidelines-on-connected-vehicles-and-mobility-related-applications/.

[55] COM/2017/010 final.

equipment of a subscriber or user' by data holders for the purposes of complying with the Data Act. Data recipients should be required to process data under their own legal bases pursuant to both ePrivacy and the GDPR; and

- The EU-level body overseeing the Data Act's consistent application, which we propose, and the EDPB should be tasked with **developing joint guidance** to help data holders, users and data recipients comply with their obligations under the Data Act.

Implementation

Application timeline

Companies will need sufficient time to prepare for compliance with the various provisions of each chapter of the Data Act. Such preparatory work would notably include ensuring that manufactured devices and related services are designed to facilitate access to or share data pursuant to Chapter II, or to train employees to handle future data requests in the context of Chapter V.

According to proposed Art. 42, the requirements will enter into application 12 months after entry into force. This is a very short transition period, which should be **extended to 36 months** to give companies enough time to prepare.

Interoperability

Identifying and defining relevant interoperability standards will be essential for ensuring the implementation and enforcement of several chapters of the Data Act.

Numerous standards, good practices and norms already exist and should be further recognised.[56] Chapter VIII should be based on such **existing work and cooperation at the level of international and European standardisation organisations**.

By contrast, the ability for the Commission to write common specifications, bypassing standardisation, would disrupt current efforts to develop consensus-based, market-driven, fair, inclusive and transparent standards. Arts 28(5) and (6) should therefore be deleted.

[56] Examples include ETSI EN 303 645 (IoT consumer products) and IEC 62443 (industrial automation and control systems and products).

FOR MORE INFORMATION, PLEASE CONTACT:

Julien Chasserieau

Senior Manager for AI & Data Policy

julien.chasserieau@digitaleurope.org / +32 492 27 13 32

Béatrice Ericson

Officer for Privacy & Security Policy

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

Alberto Di Felice

Director for Infrastructure, Privacy & Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK