DIGITALEUROPE

16 JUNE 2023

Safeguarding Europe's economic competitiveness in the Data Act's final stretch

Executive summary

Barely a year after the Commission issued a proposal for a Data Act,[1] both European Parliament and Council adopted their positions on the legislative proposal and started interinstitutional negotiations at a quick pace.[2]

We welcome some of the solutions put forward in the negotiation mandates, for instance in clarifying key concepts and better protecting intellectual property rights. However, many issues still permeate the text, and merit more than quick fixes.

DIGITALEUROPE has warned against a speedy process, including in joint statements gathering 30 European associations from various sectors and major European business leaders.[3] The Data Act sets horizontal rules that will deeply affect data-sharing partnerships, bring unprecedented interference to contractual freedom, and risk exposing companies to unfair competition, cybersecurity and safety risks.

This paper and its annex compare the Parliament and Council mandates for trilogue negotiations, and make recommendations to improve the text.[4] We urge policymakers to take sufficient time to make sure the Data Act does not imperil Europe's economic attractiveness and competitiveness.

At a minimum, the final Data Act must:

- Better circumscribe central definitions, such as 'data' and 'products,' so that the proposal's exact nature and impact can be properly understood;

[1] COM/2022/68 final.

[2] Throughout this paper, we refer to the latest Council four-column document available to us at the time of writing, doc. 10530/23.

[3] Available at https://www.digitaleurope.org/news/joint-statement-the-data-act-is-a-leap-into-the-unknown/ and https://www.digitaleurope.org/news/ceos-call-for-urgent-rethink-on-data-act/, respectively.

[4] For our full position on the proposal, see DIGITALEUROPE, *Rebalancing the Data Act*, available at https://www.digitaleurope.org/resources/rebalancing-the-data-act/.

- Introduce stronger ex-ante safeguards against data misuse, to protect trade secrets but also cybersecurity, health, safety and privacy;
- Allow for appropriate compensation to reflect the investments and costs of making data accessible easily and securely, and of building the infrastructure and internal processes to respond to access requests;
- Restrict mandatory business-to-government (B2G) sharing to non-personal data and to emergency situations, whilst better specifying the categories of public bodies that can request data along with the necessary conditions and protective measures;
- Give users the freedom to choose from a wide range of cost-efficient and tailored cloud solutions, and safeguard their contractual freedom as to how and when to switch, including fixed-term contracts;
- Remove uncertainty as to Art. 27's applicability to international data transfers by deleting the word 'transfer' throughout the text; and
- Allow for a longer transition period, of at least 36 months, to give companies from all sectors time to prepare.

Table of contents

Scope and definitions

Central definitions, for instance that of 'data' or 'products,' must better circumscribe the proposal's nature and impact.

Both the Parliament and Council negotiation mandates dissect and multiply the definitions under Art. 2, at times going beyond the proposal's impact assessment. By contrast, as in the original proposal, the definition of 'product' should be limited to items whose primary function is not the storing and processing of data, and which are not designed to display, play, record and transmit content.

One example of the unhelpful changes brought about by the negotiating mandates is the fundamental definition of 'data.'

Although Council and Parliament correctly suggest that the notion of data should be circumscribed by excluding inferred and derived data, both also introduce several new definitions such as 'metadata,' 'data generated by the use of a product or related service,' 'readily available data,' 'personal data' and 'non-personal data.' Similarly, the definitions of 'user' and 'product' have been declined into 'data user,' 'data recipient,' 'user' not to be confused with 'data recipient' or 'data holder,' and 'product' and 'connected product.'

The scope and interplay of such definitions is often unclear, which does not bode well for a future-proof attribution of roles in the data economy. Our annex suggests a number of changes to clarify the definitions.

B2B and B2C data sharing

Safeguards against data misuse

Stronger ex-ante and ex-post safeguards are needed against data misuse, to protect trade secrets but also on the grounds of cybersecurity, health, safety and privacy.

The Council's and Parliament's positions can be complementary if trilogue negotiators successfully leverage the proposed security and safety safeguards (Arts 3 and 4) alongside protecting data linked to innovation.

Overall, we recommend refocusing on incentives for data sharing and data generation, which require widespread organisational, strategic and economic adaptation to make actual value out of various data sets.

Whilst DIGITALEUROPE welcomes the stronger ex-post liability rules the Parliament and Council introduced, for instance in Art. 11(2), ex-ante measures must be introduced. Such measures are needed to protect sensitive data before potential misuse takes place to prevent economic, commercial or even physical damage or harm, which could otherwise be irreversible once data has already been shared.

We therefore propose that, based on transparent justifications, the data holder should be able to demonstrate why a data sharing request is to be rejected. This could be to protect health, safety, security, privacy, trade secrets or intellectual property. The user could then challenge the decision, leveraging the role of dispute settlement bodies enshrined in Art. 10.

We believe such provisions would help start a conversation between the data holder and the user or third party making the request, and in many cases lead to an amicable solution to better protect the data, such as stronger technical and organisation measures.

To this end, the Council's provisions to protect trade secrets are welcome but are excessively restrictive. They limit the possibility of data access refusal to 'exceptional circumstances,' where the data holder must prove that it is 'highly likely to suffer serious damage.' These conditions present an unrealistically severe threshold and would not be usable in practice.

Even more worrisome is the recent trilogue proposal to restrict data holders' right to refuse data sharing to situations where data would be transferred to 'inadequate' third countries.

This potential compromise solution is problematic for several reasons. First, safeguards for trade secrets are needed inside the EU itself, as unfair competition through data misuse can arise from within Europe as well. It can also arise from countries that would likely be considered 'adequate,' as it's not merely a country's legal system that endangers trade secrets but data recipients' potential misuse of the shared data. This is also why the wording 'irrespective of their place of establishment' should be removed from Art. 1(2)(c).[5]

Second, this restriction would create a parallel adequacy system for data transfers in addition to the General Data Protection Regulation (GDPR) that would be detrimental to companies' ability to move data in global markets.[6] Companies should be free to reach such determinations themselves based on their own assessments as to the possible risks to trade secrets, security, etc.

Companies must be able to justify their refusal to share data on a case-by-case basis taking into account several reasons such as risks to security, health and

[5] Art. 1(2)(c) considers data recipients irrespective of their place of establishment. Entities not established in the EU may then be able to exploit the Data Act's provisions, creating large volumes of data access requests for data holders and increasing the risks we identified towards protection of trade secrets, IP, safety, security, etc. We suggest reverting to the Commission's original proposal, so that the Data Act only applies to data recipients in the EU.

[6] Regulation (EU) 2016/679. For more on this, see DIGITALEUROPE, *Data transfers in the data strategy: Understanding myth and reality*, available at https://www.digitaleurope.org/resources/data-transfers-in-the-data-strategy-understanding-myth-and-reality/.

safety, in addition to trade secrets. Otherwise, we risk not only harming companies' reasonable economic interests but also jeopardising citizens' protections.

The Parliament's position does propose some necessary and proportionate protections under Arts 3 and 4, notably by allowing data holders and users to agree on restricting or prohibiting access, use or further sharing when security, health and safety are at risk. We strongly welcome such provision as well as the possibility to involve the expertise of sectoral authorities.

Overall, although certain proposals for Arts 4 and 5 are promising, notably on trade secret protections, **the final provisions must provide more effective and practical ex-ante safeguards.**

Compensation

Compensation should reflect the investments and costs of making data accessible easily and securely, in respect of data protection legislation, or of building the infrastructure and internal processes to respond to requests.

Certain proposals in Chapter II require products and related services to be expressly designed to make data (and metadata) not only directly accessible, but also free of charge. This does not account for the fact that each recipient will have a different use for the data and different needs around metadata, which would be difficult to predict for the data holder. A list of requirements and conditions are also set for enabling such data sharing. For example, access must be 'easy,' 'secure,' structured,' in a 'commonly used and machine-readable format' – all free charge. And the Parliament proposes adding further requirements to this list.

Instead of incentivising companies, the absence of any form of market-based compensation for the cost of collecting, curating and making data accessible easily and securely could deter them from building data-driven business models.[7] The task of properly securing data in itself requires sufficient resources, and even more resources when it comes to curating it or sharing it.

B2G data sharing

Businesses stand ready to provide data to public bodies to respond to public emergencies. However, 'public bodies,' 'specific tasks in the public interest' and the general framework for requests need to be defined and structured, especially in time-sensitive cases.

We strongly support Parliament's position, notably where it excludes personal data from the scope of Chapter V.

[7] The Parliament's position refers to 'minimal adaptations necessary to make [the data] useable.'

This chapter should not allow for exceptions to the cases of public emergencies, which is why Art. 15(c) must be deleted.

Categories of public bodies that can request data must also be expressly designated. Transparency for the conditions for access requests must be in the text of the Data Act, especially with regard to data use and protective measures.

We fully understand the importance for public bodies to receive data in specific emergency situations. However, the framework as proposed by Parliament and Council still fails to impose concrete limitations in time and scope, and will likely lead to legal challenges.

Chapter V does not specify which 'public sector bodies' would be able to request data from companies, and neither does the definition in Art. 2(9). Thus, the range of authorities able to send requests would be considerable, from local to regional or national authorities, including public undertakings and other mixed public-private entities, as well as public research institutes.

Art. 15 remains extremely problematic due to its broad scope, going much beyond the notion of 'public emergency' and 'exceptional need.' This is specifically the case with Art. 15(c), which enables any public body to request data to carry a 'specific task in the public interest,' a concept loosely defined and open to excessive discretion.

Additionally, the Council's proposed exemption from the obligation to demonstrate that data could not be obtained on the market for requests necessary for official statistics further increases the possibility of abusing the Chapter V framework.[8]

Though some clarifications have been brought to mitigate arbitrary data requests, conditions and processes framing such requests need to be further developed. For instance, details as to the demonstration supporting a request should not be left to recitals such as Recital 58.

Whilst we support the principle that data made available to respond to a public emergency should be provided free of charge, exceptions should be possible due to the broad scope of Chapter V's provisions. The costs and administrative burden for companies generated by data access should be taken into account under Art. 20(1).

Cloud switching

Cloud switching requirements should be proportionate with regard to the variety of cloud services and the volume and complexity of data stored. Provisions should give users the freedom to choose from a wide range of cost-efficient and tailored solutions.

[8] Council mandate, Art. 15, first paragraph, point (c)(2b).

We welcome the Parliament's understanding of the above and willingness to significantly improve the Commission's proposal by providing much-needed flexibility on key provisions. Similar changes proposed by Council are also positive, though more limited.

Trilogue negotiators still need to fully commit to safeguarding contractual freedom, notably how and when to switch. The recognition of the possibility for parties to agree on fixed-term contracts must be present and expanded in the final Regulation.

The variety of cloud services and the volume and complexity of the different types of data stored should be better reflected in the final text.

In this regard, we support the Parliament's recognition that equivalent services may have different and competing characteristics.

However, more flexibility compared to both institutions' positions is still necessary, especially for the provisions regulating contracts. This approach would allow for a better adaptation to market realities.

Regarding the notice period, the possibility to negotiate through contractual terms should be protected and reinforced. A mandatory notice period in Arts 23 and 24 will undermine parties' ability to negotiate contracts tailored to their needs, including by preventing them from setting a termination date of their choosing. Extending the notice period proposed by the Commission by only a month, as suggested by both Parliament and Council, is insufficient in this regard.

We recommend that the final text allow for flexibility in certain exceptions, to reflect the diversity in cloud services, and the possibility to maintain fixed-term contracts and price benefits for customers. We therefore strongly support the clarification made in the Council's position that fixed-term contracts remain a possibility.[9] The Council's position also helpfully attempts to clarify the link between the termination of a contract and the effective completion of the switching process.

Completing the switching may sometimes be a difficult process. Set transition periods for switching defined by law cannot, by essence, cover all cloud uses. This is why it is important for the Data Act to acknowledge that the source provider and the customer are best placed to determine the expected duration of the switching process. Thus, more flexibility is needed, including when it comes to defining the alternate transition period under Art. 24(2). We also caution against some trilogue proposals which would prevent customers from extending the switching period more than once. Customers should have the possibility to revisit their switching operations and extend the period as they wish.

[9] Recital 72b of the Council's position.

Furthermore, whilst we strongly support the clarification that platform (PaaS) and software as a service (SaaS) have no obligation to implement the notion of ‘functional equivalence,’ such notion remains vague and will be difficult – or even impossible – to implement. This concept should be either deleted or further amended to reflect market realities. Offerings between service providers will often differ and the destination service cannot be fully aware of all the functionalities, security and performance levels in place. Services, configurations and protocols may change over time. These parameters also depend on customers’ infrastructure choices, as they are a competitive differentiator between cloud platforms.

We recommend that the cooperation of both the source and the destination providers, with the support of the customer and relevant third parties, be reinforced. Separate responsibilities should be allocated to different parties. Provisions should, for example, clarify that the customer, the source provider and the destination provider shall cooperate in good faith, avoid delaying or abusing the switching process (also applicable to third-party entities that manage switching capacities or the switching process on the customer’s behalf). The destination provider will have better knowledge of its platform and how to adapt it to the customer’s needs. We support the inclusion of a ‘good faith obligation’ for all parties involved in the switching process in the Parliament’s proposal.[10]

In addition, cloud service providers may not have any visibility as to customer data traffic to verify the purpose of a data transfer. Relying on customer attestation could result in a significant amount of fraud, where it is impossible to distinguish between customers using a multi-cloud solution or other business uses.

The proposed obligation in the Council mandate to provide multi-cloud services free of charge risks not only impeding innovation but increasing costs for providers and in turn customers.[11] The impact assessment did not cover the consequences of such a provision. The focus should instead be placed on allowing customers to make informed choices when selecting cloud providers.

Lastly, more clarity and flexibility are needed regarding the categories of data and the types of workloads in scope. For instance, the notion of ‘co-generated’ data under Art. 26(4) is too vague and could lead to disproportionate export requests. Here, we would welcome the Parliament’s clearer inclusion of ‘exportable data in a structured, commonly used and machine-readable format.’

[10] Art. 24(b).

[11] Council mandate, Art. 28a(2).

Data transfers

The Data Act should not impose restrictions concerning international data transfers, which would only bring further uncertainty to companies' international operations already severely tested following the Schrems II ruling.

To this end, the final text of Art. 27 and related provisions should remove all mentions of the word 'transfer.'

Whilst Arts 27(2)-(5) stipulate rules applicable only in case of data access requests from third-country authorities, Art. 27(1) introduces a general requirement applicable to all data transfers, preventing them in theoretical scenarios where they could conflict with EU or Member State law.

Whilst we welcome the direction taken in the Council's proposal, with the addition of the word 'governmental' and move of the word 'transfer' after 'access,' we strongly believe that the provision's intention (protection from unlawful government access) would be better reflected by deleting the word 'transfer' throughout Art. 27. In line with those changes, the title of Art. 27 must also delete the mention of 'transfer.'

Without these changes, there is still a risk of misinterpretation of Art. 27(1) by competent authorities, which could result in blocking international data transfers where there is a belief (whether unfounded or not) that an unlawful third-country data access might happen. Additionally, the Data Act should not regulate data already covered by the GDPR, for instance in adequacy findings, standard contractual clauses and corresponding transfer impact assessments, which companies must already comply with.

Finally, legal certainty is needed as to the standards used by bodies or authorities to review third-country requests under Art. 27, as well as the length a review might take and whether the review might be overturned at a later stage.

Implementation timeline

Companies from all sectors will need at least 36 months to prepare.

The Data Act must allow for a longer transition period, of at least 36 months, to give companies from all sectors time to prepare.

When it comes to the entry into application, although the Council's proposed transition period is still insufficient for compliance, we note the progress made in Art. 42 for the applicability of Art. 3(1). We recommend that the same timeline be set to apply to the obligations in Arts 4(1) (sharing data with users) and 5(1) (sharing data with authorised third parties).

All three provisions are intrinsically connected, as they will require manufacturers and service providers to alter the design of their products and put in place processes for dealing with data requests.

Such changes would also prevent retroactive provisions – applying to products and related services already placed on the market – and help ensure sufficient predictability of current investments. To this end, we welcome the Council's proposal for a definition of 'placing on the market' under Art. 2(1ah), aligned with product legislation.[12]

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

[12] Regulation (EU) 2019/1020.

Annex: detailed amendments and justifications

Council position	European Parliament position	DIGITALEUROPE comments
Article 2		
Definitions	*Definitions*	
For the purposes of this Regulation, the following definitions apply: (1) ‘data’ means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording; **(1ae) ‘readily available data’ means data generated by the use of a product or related service that the data holder obtains or can obtain without disproportionate effort, going beyond a simple operation;** **(1af) ‘data generated by the use of a product or a related service’ means data recorded intentionally by the user or as a by-product of the user’s action, as well as data generated or recorded during the period of lawful use among**	For the purposes of this Regulation, the following definitions apply: **(1)** ‘data’ means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording; **content, or data obtained, generated or collected by the connected product or transmitted to it on behalf of others for the purpose of storage or processing, shall not be covered by this Regulation.** **(1c)** **(1e) ‘data user’ means a natural or legal person who has lawful access to certain personal or non-personal data and has a right to use that**	**Parliament’s position:** • DIGITALEUROPE welcomes the Parliament’s suggested amendment to Art. 1(1). The exclusion of data for storage or processing on behalf of third parties, such as servers or cloud infrastructure, should however be further inscribed in the provisions, rather than indicated in a recital. • We recommend that at the very least if data beyond raw data is shared, it should include compensation and resulting obligations should remain proportionate (see comments to Arts 3, 4 and 5). Indeed, without the possibility of monetisation schemes, data that has been pre-processed, cleaned, or prepared, would incur important costs for Europe’s digital industry. Pre-processed data is also often attached to Intellectual Property rights and is essential to developing AI-related technology. Sharing it could therefore quickly result in unfair

Council position	European Parliament position	DIGITALEUROPE comments
others in standby mode or whilst the product is switched off. This ~~does~~ shall not include the results of processing that substantially modifies the data, data recorded on the use of the product to access software applications other than related services and data generated on the recording, transmission, displaying or playing of content as well as such content; **(1ag) ‘making available on the market’ means any supply of a product ~~[or service]~~ for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;** **(1ah) ‘placing on the market’ means the first making available of a product ~~[or service]~~ on the Union market;**	**data for commercial or non-commercial purposes;**	competitive advantages for companies that have invested in research and innovation. • We recommend that the Council’s wording of ‘beyond a simple operation’ be kept, as a ‘disproportionate effort’ would leave the provision open to interpretation. **Council’s position:** • In Art. 2(1af) of the Council’s position, we recommend that the word ‘substantially’ be deleted, as it is imprecise. • In Art. 1(af), we welcome the clarification that excludes ‘*data recorded on the use of the product to access software applications other than related services*.’ Indeed, this avoids widely expanding the scope to any software application running in general purpose computing devices. • Recital 14(a) of the Council’s position is welcome where it ties data to ‘user’s actions,’ instead of covering for example Data on the hardware’s status, which will represent superfluous information for the user. We recommend deleting the reference to ‘data generated automatically by sensors,’ as it could result in technical obstacles for companies without real added value for users. Sensor data that is processed exclusively for functionality or

Council position	European Parliament position	DIGITALEUROPE comments
		condition monitoring of an IOT should be excluded from the scope. **General remarks:** The definition of 'data' is at the very core of the Data Act and should be clearly circumscribed. DIGITALEUROPE recommends that any data beyond raw data should involve compensation. On the other hand, volatile data must be explicitly excluded, as they are only temporarily stored and then deleted. Data from devices in standby mode or switched off should be clearly excluded from the Data Act's scope.
(2) 'product' means a tangible~~, movable~~ item~~, including where incorporated in an immovable item,~~ that obtains, generates or collects~~,~~ data concerning its use or environment, and that is able to communicate data **directly or indirectly** via a publicly available electronic communications service **within the meaning of Article 2(4) of Directive (EU) 2018/1972** ~~and whose primary function is not~~ ~~**neither**~~ ~~the storing and processing of data~~ ~~**nor is it primarily designed to display or play content, or to record and transmit content**~~;	(2) '**connected** product' means an item, that obtains, generates or collects, **accessible** data concerning its use or environment, and that is able to communicate data via **an electronic communications service, a physical, connection or on-device access** and whose primary function is not the storing**, processing or transmission** of data **on behalf of others**;	• The Council's proposed wording for Art. 2(2) considerably broadens the Data Act's scope to cover *all* connected products sold in Europe. This is further combined with the partial deletion of Recital 15, which in the Commission's proposal helpfully provided examples of the products intended to be outside of the scope. • In Parliament's position, it is unclear which parties will be considered to be 'others.' All content developed by manufacturers for their proprietary hardware could therefore be covered, which widely expands the scope.

Council position	European Parliament position	DIGITALEUROPE comments
		• Changes of this magnitude were not analysed in the impact assessment and would widely expand the amount of devices in scope, whilst increase uncertainty as to which companies qualify as data holders, how to comply with product design requirements and which types of data they must share. The Data Act already covers important amounts of data, generated by devices without user actions. Expanding the scope further to connected devices would go beyond and destabilise the industry rather than incite innovation and creating value from the data. • We recommend that Art. 2(2) defines 'product' as an item whose primary function is not the storing and processing of data, and which is not primarily designed to display, play, record and transmit content. Indeed, solely relying on a definition of data to determine the Act's scope would bring considerable legal uncertainty. • Additionally, in line with our position on the Cyber Resilience Act, we urge that the final Regulation refers more precisely to 'connected products.' We note that the expression 'connected product' is already

Council position	European Parliament position	DIGITALEUROPE comments
		found, but not defined, in the proposal (see Recitals 16 and 18). Our proposed definition is also compatible with the widely acknowledged ISO definitions (see ISO/IEC 20924). Although we welcome the clear exemption of 'prototypes' in recital (14) of the Parliament's proposal, products that are not being used, or in standby mode or switched off should be excluded, notably in recital 14a.
(3) 'related service' means a digital service, **other than an electronic communications service,** including software **and its updates**, which is **at the time of the purchase, rent or lease agreement** ~~**incorporated** in or~~ inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions;	(3) 'related service' means a digital service, including software **, but excluding electronic communication services which is** inter-connected with a product in such a way that its absence would prevent the product from performing one **or more** of its functions**, and which involves accessing data from the connected product by the provider or the service**;	• It should be clarified that related services are limited to those essential to the product's functioning. • In the Parliament's positions, whilst we welcome the exclusion of 'electronic communication services,' we further recommend that the definition of 'related services' only covers those necessary for the product to perform one of its essential functions and not those services primarily used to display, play or protect content. • We also welcome the Council's proposal to clarify that the related services in scope are those that are inter-connected with a product at the time of purchase, rent or lease agreement.

Council position	European Parliament position	DIGITALEUROPE comments
(4) virtual assistants' means **a** software that can process demands, tasks or questions including **those** based on audio, written input, gestures or motions, and **that,** based on those demands, tasks or questions**,** provides access **to other** ~~their own and third party~~ services or control**s connected physical** ~~their own and third party~~ devices;	(4) 'virtual assistants' means software that can process demands, tasks or questions including **those** based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access **to other** services or control **the functions of products**;	- Recital 22 indicates that the intention is to capture assistants that act as a 'gateway' to third-party devices in the home/consumer environment. DIGITALEUROPE therefore welcomes clarifications that it is assistants that have control that are under the scope. We would further recommend that it is *connected* devices or products that are referred to.
(5) 'user' means a natural or legal person**, including a data subject,** that owns, rents or leases a product or receives a **related** service~~s~~;	(5) 'user' means a natural or legal person that owns **a connected product or receives a related service or to whom the owner of a connected product has transferred, on the basis of a rental or leasing agreement, temporary rights to use a connected** product or **receive related** services **and, where the connected product or related service involves the processing of personal data, the data subject**;	- The **'data users'** and **'users'** definitions suggested by Council and Parliament remain vague. For instance, the definitions of 'user' refers to 'related services' that are in fact already defined in separate provisions and should not be confused. The definition of 'data users' remains very broad and is only referred to in one recital. For

Council position	European Parliament position	DIGITALEUROPE comments
		example, any access to data based on the Data Act could be considered 'lawful'[13] • DIGITALEUROPE recommends the definition of a 'user' or 'data user' excludes the mention of 'related services' to avoid uncertainty around the concept of receiving a service. A distinction should further be made between B2B and B2C scenarios. • There are cases where the owner might not want the data to go to the person to whom they have lent a product. For example if you are renting your flat, in which there is a connected camera or fridge. It may cause security and privacy risks. • Switching off a device that still collects data: included? Recital 14 of Plt proposal should be amended.
(6) 'data holder' means a legal or natural person who - has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, **to make available certain data** or - **can enable access to the data** ~~in the case of non-personal data and~~ through control of the technical design ~~of the product and related services, the ability, to make available certain~~	(6) 'data holder' means a legal or natural person**,** who has **accessed data from the connected product or has generated data during the provision of a related service and who has the contractually agreed right to use such data, and the obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law** to make	• To clarify which single entity in the value chain (whether manufacturers or providers or related services) can qualify as a 'data holder,' the definition of should build on the notions of *control* over the data and the *ability* to make it available. Focusing on control over the technical design would ignore lack of control over the data for

[13] Recital 29 of the Parliament position.

Council position	European Parliament position	DIGITALEUROPE comments
~~data~~ **or means of access, in the case of non-personal data**;	available certain data **to the user or a data recipient**;	example for security or privacy reasons, or data used for simple maintenance. ● We would partially support the Parliament’s proposal in that it states that only the person having accessed data from the connected product qualifies as a data holder.
(7) ‘	(7) ‘	
(8) ‘	(8) ‘	
(9) ‘public sector body’ means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies;	(9) ‘public sector body’ means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies;	● The definition of ‘public sector bodies’ in the Commission’s proposal encompasses all entities governed by public law and associations thereof. Private-public undertakings and other mixed public-private entities, as well as public research institutes are all included. 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.
(10) ‘public emergency’ means an exceptional situation **such as public health emergencies, emergencies resulting from natural disasters, as well as human-induced major disasters, such as major cybersecurity incidents,** negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting	(10) ‘public emergency’ means an exceptional situation**, limited in time such as public health emergencies, emergencies resulting from natural disasters, as well as human-induced major disasters, including major cybersecurity incidents,** negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting	● In the definition of ‘public emergency,’ we welcome clarifications of the types of emergencies covered and believe the Parliament’s mention that it is ‘limited in time’ should be kept. However, DIGITALEUROPE strongly recommend that more objective criteria be included in the

Council position	European Parliament position	DIGITALEUROPE comments
repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s) **and the existence or likely occurrence of which is determined ~~and~~ or officially declared according to the respective procedures under Union or national law**; **(10a) ‘official statistics’ means European statistics according to Regulation 223/2009 and statistics considered official according to national legislation~~.~~;**	repercussions on living conditions or economic stability, **financial stability,** or the substantial **and immediate** degradation of economic assets in the Union or the relevant Member State(s) **and which is determined and officially declared according to the relevant procedures under Union or national law**; **(10a) ‘official statistics’ means ‘European statistics’ within the meaning of Regulation (EC) No 223/2009;**	definition. For instance, a precise timeframe and magnitude of the actual or expected negative effects should be determined. We would welcome an exhaustive list under Art. 15. - The inclusion of ‘official statistics’ pertains to a separate objective from the Data Act’s. - The recently proposed exemption of requests for official statistics from the obligation to demonstrate that data could not be obtained on the market further increases the possibility of abusing the framework set in Chapter V.
(**12b**) **‘digital assets’ mean elements in digital format for which the customer has the right of use, independently from the contractual relationship of the data processing service it intends to switch away from, including data, applications, virtual machines and other manifestations of virtualisation technologies, such as containers~~.~~;**	(12) ‘	- We do not recommend the inclusion of a definition for ‘digital assets,’ in particular since they are to be included in contractual terms for cloud switching, yet refer to elements ‘independently from the contractual relationship.’
(13b) ‘switching charges’ mean charges, other than data egress charges and early termination penalties, imposed by a data processing provider on a customer for the switching to the systems of another provider, as mandated by this Regulation;		- The attractiveness and existence of multi-year contracts would be at risk if no penalties for early termination were possible. Thus, we welcome the definition of ‘switching charges’ proposed by the Council. For additional clarity, the possibility to set such penalties in contracts should be

Council position	European Parliament position	DIGITALEUROPE comments
		spelled-out through Arts 23 and 24, or within a recital.
(14) ‘functional equivalence’ means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract;	(14) ‘functional equivalence’ means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract;	• Whilst we strongly support the Council’s clarification that PaaS and SaaS service types have no obligation to implement the notion of ‘functional equivalence,’ we believe that such notion remains vague and will be difficult – or even impossible – to implement. This concept should be either deleted or further amended to reflect market realities. Indeed, offerings between service providers will often differ and the destination service cannot be fully aware of all the functionalities, security and performance levels in place. These parameters also depend on the infrastructure choices for customers, as they are a competitive differentiator between platforms.
	(19a) ‘portability’ means the ability of a customer to move imported or directly generated data that can be clearly assigned to the customer between their own system and cloud services, and between cloud services of different cloud service providers;	• We welcome the inclusion of data that can be clearly assigned to the customer, but would recommend clearly excluding anonymised and aggregated data.

Council position	European Parliament position	DIGITALEUROPE comments
	(20a) 'common European data spaces' means purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives; ***(20b) 'metadata' means a structured description of the contents of the use of data facilitating the discovery or use of that data;***	**Parliament**: • Whilst we welcome the inclusion of a definition of 'metadata,' the one proposed by Parliament needs further clarification. • 'metadata' risks covering business data or data that is necessary to keep in a cloud provider records for various purposes, including product improvement. • 'metadata' as defined will still 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.
CHAPTER II		
CHAPTER II RIGHT OF USERS TO USE DATA OF CONNECTED PRODUCTS	CHAPTER II	

Council position	European Parliament position	DIGITALEUROPE comments
AND RELATED SERVICES ~~BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING~~	BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING	
Article 3		
Obligation to make data generated by the use of products or related services accessible ***to the user***	*Obligation to make data* ***accessed from connected products or*** *generated* ***during the provision of*** *related services accessible* ***to the user.***	
(1) Products shall be designed and manufactured, and related services shall be **designed and** provided, in such a manner that data generated by their use **that are ~~accessible~~ readily available to the data holder, as well as metadata that is necessary to interpret and use that data,** are, by default **and free of charge**, easily, securely and, where relevant and appropriate, directly accessible to the user.**, in a structured, commonly used and machine-readable format.**	**(1) Connected** products shall be designed and manufactured **in such a manner that data they collect, generate or otherwise obtain, which are accessible to data holders or data recipients** are, by default **free of charge to the user, and** easily, securely and, where relevant and **technically feasible**, directly accessible to **it, in a comprehensive, structured, commonly used and machine-readable format. Data shall be available in the form in which they have been collected, obtained or generated by the connected product, along with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data. Information derived or inferred from this data by means of complex proprietary algorithms, in particular where it combines the output of multiple sensors in the connected product, shall not be considered within**	**General remarks:** - We strongly support the Parliament's safeguards against security and cybersecurity risks by making reference to inhibiting the functionality of the connected product. - However, in both positions, there is a considerable unbalance in requiring that data to be directly accessible to the user free of charge should also be easily, securely and directly accessible in a structured, commonly used and machine-readable format. This list of requirements will complicate data sharing and business models in the data economy. We recommend that this provision be clarified and simplified to ensure that only data that is readily available to the data holder should be shared, securely and easy to access.

Council position	European Parliament position	DIGITALEUROPE comments
	the scope of a data holder's obligation to share data with users or data recipients unless agreed differently between the user **and the data holder. In case that user is a data subject, connected products shall offer possibilities to directly exercise the data subjects' rights, where technically feasible. Connected products shall be designed and manufactured in such a way that a data subject, irrespective of their legal title over the connected product, is offered the possibility to use the products covered by this Regulation in the least privacy-invasive way possible. The requirements set out in the first subparagraph shall be met without inhibiting the functionality of the connected product and related services and in accordance with data security requirements as laid down by Union law**. **1a. Data holders may reject a request for data if access to the data is prohibited by Union or national law.**	**Council position:** ● We strongly welcome the Council's proposal to bring clarity to the provisions by for example replacing 'accessible' with 'readily available.' This provision should be combined with the Parliaments reference to safety and security requirements in Art 3(1) and the exclusion of inferred information. **Parliament position:** ● It introduces contradictory measures in Art.3(1). First, it mixes data collected, generated and otherwise obtained. Whilst data that is readily available or generated could quite naturally fall into the scope, collected or otherwise obtained data already imply an effort of regrouping data from different sources, including outside the product itself. Data from all these different sources would then have to be made accessible to the user without compensation but also 'easily' and 'securely.' The cost of collecting the data, obtaining it, making it accessible easily and securely risks disincentivising companies from building data-driven business models, or stop them from having enough resources to fully secure the data.

Council position	European Parliament position	DIGITALEUROPE comments
		● The provision even goes a step further and ‘where relevant and technically feasible,’ direct access should be given still free of charge, in a ‘comprehensive,’ ‘commonly used’ and ‘machine-readable’ format. The language is vague (e.g. ‘where relevant’), and does not recognise that it might not be economically or legally feasible for companies to design and manufacture connected products to realistically follow such instructions. ● The first paragraph on Art. 3(1) is in direct contradiction with the second part, which indicated that ‘only minimal adaptations’ shall be made to make data useable. A third party might prefer to decide how to make the data useable, according to their goals. ● We welcome the exclusion of inferred and derived data, in line with the objectives of the proposal for example outlined in Recitals 14 and 17. However, alignment is needed between recital 24(b) and Art 3(1), as the number of sensors is not of relevance but rather the investment made and proprietary technologies used by the company to process raw data and infer or derive additional insights.

Council position	European Parliament position	DIGITALEUROPE comments
		• Further, it is important that data specific to sensors should only be available upon request, rather than automatically. Otherwise the risk would be that the user is overflowed with data that would be expensive in terms of energy and storage space. • Data sharing should not be privacy-invasive, in accordance to the GDPR. We recommend deleting the reference to products being the ‘least privacy invasive’ possible. Art. 3(1) should further be drafted in respect with the data minimisation principle described in Recital 19. Indeed, the Data Act affects both personal and non-personal data, and companies cannot be held liable for seeking to comply with the Data Act. As it might not always be technically feasible to both share data and ensure the possibility to exercise data subject rights, the Parliament’s Art. 1a should prevail. • Sharing related metadata ‘necessary to interpret and use the data’ may also come at an additional cost, in particular since the type of metadata concerned was not defined. It should not by default be free of charge. • Last, in the Council’s proposal, we note progress made in Art. 42 for the applicability

Council position	European Parliament position	DIGITALEUROPE comments
		of Art. 3(1). However the same timeline should apply to the obligations in Art. 4(1) and 5(1), as all three provisions are intrinsically connected. They require manufacturers and service providers to alter the design of their products and put processes into place for dealing with data requests.
(2) Before concluding a contract for the purchase, rent or lease of a product or a related service, **the data holder shall at least provide** ~~at least~~ the following information ~~shall be~~ ~~provided~~ to the user, in a clear and comprehensible format: a. ~~the nature~~ **type of data** and the **estimated** volume of the data likely to be generated by the use of the product or related service; b. whether the data is ~~likely to be~~ generated continuously and in real-time; c. how the user may access those data **including in view of the data holder’s data storage and retention policy;** d. whether the **data holder** ~~manufacturer supplying the product or the service~~	**(2)** Before concluding a contract for the purchase **of a connected product, the manufacturer, or where relevant the vendor, shall provide** at least the following information to the user, in a **simple manner and in a** clear and comprehensible format: **a.** the **type of data, format, sampling frequency, the in-device storage capacity, and the estimated** volume of **accessible data which the connected product is capable of collecting, generating or otherwise obtaining;** **b.** whether the **connected product is capable of generating data** continuously and in real-time; **(ba) whether data will be stored on-device or on a remote server, including the period during which it shall be stored;**	• The Parliament’s proposed list of information to be provided about the data can become costly or difficult to gather, and discourage contracts for the sale of connected products. For example, in many cases the ‘volume’ of data is impossible to estimate upfront and of little value, particularly where the user is a data subject. This additional information would make it harder to make data generated by the use of products or related services accessible. Further, buyers of connected products might not necessarily always be interested in this amount of information about the data, which would be costly and time consuming to prepare. • A similar provision to Art. 15(4) GDPR should prevent sharing sensitive data, such as data that once accessed, may cause risks to a person’s safety, health, security or privacy.

Council position	European Parliament position	DIGITALEUROPE comments
~~provider providing the related service~~ intends to use the data itself or allow a third party to use the data and~~, if so,~~ **in either case** the purposes for which those data will be used; e. ~~whether the seller, renter or lessor is the data holder and, if not,~~ the identity of the data holder, such as its trading name and the geographical address at which it is established; f. the means of communication which **make it possible** ~~enable the user~~ to contact the data holder quickly and communicate with that data holder efficiently; g. how the user may request that the data are shared with a third-party; h. the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the competent authority referred to in Article 31	c. how the user may access **free of charge, and, where relevant, retrieve and request the deletion of** those data; **(ca) the technical means to access the data, such as Software Development Kits or application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable the development of such means of access;** **(cb) whether a data holder is the holder of trade secrets or other intellectual property rights contained in the data likely to be accessed from the connected product or generated during the provision of related service, and, if not, the identity of the trade secret holder, such as its trading name and the geographical address at which it is established.**	- Real-time data sharing should not be mandatory where it is not technically feasible, or where the confidentiality, integrity and availability of a device or service can be compromised. Just as the GDPR sets limits to real-time sharing, the Data Act should at the very least account for the risks and difficulties with sharing large volumes of diverse data. Real-time data sharing also exacerbates the risks to cybersecurity.
	(2a) Related services shall be provided in such a manner that data generated during their provision, which represent the digitalisation	

Council position	European Parliament position	DIGITALEUROPE comments
	of user actions or events, are free of charge to the user and, by default, easily, securely and, where relevant and technically feasible, directly accessible to the user in a structured, commonly used and machine-readable format, along with the relevant metadata necessary to interpret and use it.	
	(2b) Before the user concludes an agreement with a provider of related services, which involves the provider's access to data from the connected product during the provision of such services, in line with Article 4(6) of this Regulation, the agreement shall address: **a. the nature, volume, collection frequency and format of data accessed by the provider of related services from the connected product and, where relevant, the modalities for the user to access or retrieve such data, including the period during which it shall be stored;** **b. the nature and estimated volume of data generated during the provision of the related service, as well as modalities for the user to access or retrieve such data;** **c. granular, meaningful consent options for data processing, within**	• Trusted contractual relationships rely on a balance in rights of obligations, whereas the Parliament's proposal largely poses obligations on the data holders and service providers. • Sharing information of whether the data holder is the holder of trade secrets in precise agreements could pose a risk to those same trade secrets. They would make the data and device targets of reverse-engineering. • The possibility users to withdraw consent to data sharing combined with the obligation to state the minimal period for which the related service is guaranteed do not offer sufficient contractual stability and economic viability. Submitting data sharing to user consent would impinge on the legal basis for processing personal data set by the GDPR.

Council position	European Parliament position	DIGITALEUROPE comments
	the meaning of Article 4(11) of Regulation (EU) 2016/679; **d. whether the service provider providing the related service, in its role as data holder, intends to use the data accessed from the connected product itself or allow one or more third parties to use the data for purposes agreed upon with the user;** **e. the trading name of the provider of the related service, its legal entity identifier, contact details and the geographical address at which it is established; and where applicable, other data processing parties;** **f. where relevant, the means of communication which enable the user to contact the provider quickly and communicate with its staff efficiently;** **g. how the user may request that the data are shared with a data recipient, and, where relevant, withdraw the consent for data sharing;** **h. whether a data holder is the holder of trade secrets or other intellectual property rights contained in the data likely to be**	

Council position	European Parliament position	DIGITALEUROPE comments
	accessed from the connected product or generated during the provision of related service, and, if not, the identity of the trade secret holder, such as its trading name, legal identity identifier and the geographical address at which it is established; **i. how the user is able to manage permissions to allow the use of data, where possible with granular permission options, and including the option to withdraw permissions to a data holder for the use of the user's data, to the third parties nominated by a data holder, or to exclude geographical addresses;** **j. the duration of the agreement between the user and the provider of the related service, as well as the modalities to terminate such an agreement prematurely; as well as the minimal period for which the related service is guaranteed to receive security and functionality updates;** **k. the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with**	

Council position	European Parliament position	DIGITALEUROPE comments
	the data coordinator referred to in Article 31.	
	Article 3a – Data Literacy	
	(1) When implementing this Regulation, the Union and the Member States shall promote measures and tools for the development of data literacy, across sectors and taking into account the different needs of groups of users, consumers and businesses, including through education and training, skilling and reskilling programmes and whilst ensuring a proper gender and age balance, in view of allowing a fair data society and market.	• DIGITALEUROPE supports the connection between skills and data spaces at national and European level.[14] Greater focus should be given to making value out of the data, as opposed to forcing data sharing with a whole list of inflexible new obligations. Without the necessary skills, users, consumers, and businesses at the centre of the Data Act will simply not benefit from the data economy.
Article 4		
(1) Where data cannot be directly accessed by the user from the product **or related service**, the data holder shall make available to the user the data generated by its **the** use of a product or related service **that are accessible readily available to the data holder, as well as the relevant metadata that is necessary to interpret and use that data,** without undue delay, free of charge**, easily, securely, in a structured, commonly used and machine-readable format** and, where applicable, **of the same quality as is available to the data holder,** continuously and in real-time. This shall be done on	(1) Where data cannot be directly accessed by the user from the product, **data holders** shall make available to the user **any data accessed by them from a connected** product or **generated during the provision of a** related service without undue delay, **easily, securely, in a comprehensive, structured, commonly used and machine-readable format,** free of charge and, where **relevant and technically feasible**, continuously and in real-time**, including making any personal data derived from such data available to a data subject pursuant to Article**	

[14] https://www.digitaleurope.org/data-space-for-skills/

Council position	European Parliament position	DIGITALEUROPE comments
the basis of a simple request through electronic means where technically feasible.	**15 of Regulation (EU) 2016/679, accompanied with relevant metadata. Data shall be provided in the form in which they have been accessed from the connected product or generated by the related service, with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data. Information** **derived or inferred from this data by means of complex proprietary algorithms, in particular where it combines the output of multiple sensors in the connected product,** shall **not be considered within the scope of a data holder's obligation to share data with users or data recipients, unless agreed differently between the user and the data holder. Any data access request to a data holder should** be done on the basis of a simple request through electronic means where technically feasible **and, where appropriate, indicate the type, nature or scope of data requested**.	
(1a) Any agreement between the data holder and the user shall not be binding when it narrows the access rights pursuant to paragraph 1.		
	(1a) Data holders may reject a request for data if access to the data is prohibited by Union or national law;	We welcome the addition that requests may be rejected where access would be prohibited by Union or national law.

Council position	European Parliament position	DIGITALEUROPE comments
	(1b) Users and data holders may agree contractually on restricting or prohibiting the access, use of or further sharing of data, which could undermine security of the product as laid down by law. Each party may refer the case to the data coordinator, to assess whether such restriction is justified, in particular in light of serious adverse effect on the health, safety or security of human beings. Sectoral competent authorities will be given the possibility to provide technical expertise in this context.	Strengthening ex-post liability for the misuse of data. We welcome the Parliament's position which recognises the importance of the 'security of the product.' However, in most cases the data holder will have a greater awareness of the possible safety and security risks, they should therefore be given the option to restrict or prohibit access on such grounds.
	(1c) Where in compliance with all the provisions established within this Regulation, and the terms and conditions agreed in the contractual agreement between the parties, a data holder shall not be liable towards the user for any damage arising from data made available, provided that the data holder has processed the data lawfully in accordance with Union and national law and has complied with relevant cybersecurity requirements and where applicable, with the technical and organisational measures to preserve the confidentiality of the shared data. When complying with this Regulation, a user, who lawfully makes available data accessed from the connected product or received following a request under Article 4 paragraph 1 to a third party, or a data	

Council position	European Parliament position	DIGITALEUROPE comments
	recipient, who is lawfully sharing data made available to it by a data holder, to a third party, shall not be liable for damage arising from sharing such data, provided that the user or data recipient have processed the data in accordance with Union and national laws and have complied with relevant cybersecurity requirement and where applicable, with the technical and organisational measures to preserve the confidentiality of the shared data.	
	(1d) Data holders shall not make the exercise of the rights or choices of users unduly difficult, including by offering choices to the users in a non-neutral manner or by subverting or impair the autonomy, decision-making or free choices of the user via the structure, design, function or manner of operation of a user interface or a part thereof.	
(2) The data holder shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. The data holder shall not keep any information, **in particular log data,** on the user's access to the data requested beyond what is necessary for the sound execution of the **individual** user's access request and for the security and the maintenance of the data infrastructure.	***(2)*** **Data holders** shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. **Data holders** shall not keep any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure. **Where identification is legally requires, data holders shall enable the**	

Council position	European Parliament position	DIGITALEUROPE comments
	possibility for users to identify and authenticate through the European Digital Identity Wallets, pursuant to Regulation (EU) No 914/2014.	
(2a) **The data holder shall not coerce, deceive or manipulate in any way and at any time the user or the data subject where ~~the user is not a~~ the data subject is not the user, by subverting or impairing the autonomy, decision-making or choices of the user or the data subject, including by means of a digital interface with the user or the data subject, to hinder the exercise of the user's rights under this Article.**		
(3) Trade secrets shall only be disclosed provided that **the data holder and the user take** all ~~specific~~ necessary measures ~~are taken~~ ~~**in advance**~~ **prior to the disclosure** to preserve the confidentiality of trade secrets in particular with respect to third parties. **Where the data holder can show that such measures do not suffice, t**~~T~~he data holder and the user ~~**can**~~ **shall** agree **on necessary additional measures, such as technical and organisational** measures**,** to preserve the confidentiality of the shared data, in particular in relation to third parties. **The data holder shall identify the data which are protected as trade secrets, including in the relevant metadata**	**(3)** Trade secrets shall **be preserved and shall** only be disclosed provided that all specific necessary measures **pursuant to Directive (EU) 2016/943** are taken **in advance** to preserve **their** confidentiality**,** in particular with respect to third parties. The data holder **or the trade secret holder if it is not simultaneously the data holder, shall identify the data which are protected as trade secrets and** can agree **with the user any technical and organisational** measures to preserve the confidentiality of the shared data, in particular in relation to third parties**, as well as on liability provisions. Such technical and organisational measures include, as appropriate, model contractual terms, confidential agreements, strict access**	• We recommend that the final Regulation clarifies or defines the 'necessary measures' expected between data holders and users and the 'specific necessary measures' expected between data holders and third parties. • In the Council's proposal, the benefit of an additional layer of 'necessary' measures is also unclear. Indeed, it supposes that the data holder could 'show that such measures do not suffice,' meaning that in practice they would have to monitor and collect proof that the original measures taken were not respected. In practice those measures would often apply to a range of users, which means that the data holder might have to monitor a wide number of cases. It is

Council position	European Parliament position	DIGITALEUROPE comments
	protocols, technical standards and the application of codes of conduct. In cases where the user fails to implement those measures or undermines the confidentiality of trade secrets, the data holder shall be able to suspend the sharing of data identified as trade secrets. In such cases, the data holder must immediately notify the data coordinator of the Member State in which the data holder is established, pursuant to Article 31 of this Regulation, that it has suspended the sharing of data and identify which measures have not been implemented or which trade secrets have had their confidentiality undermined. Where the user wishes to challenge the data holder's decision to suspend the sharing of data, the data coordinator shall decide, within a reasonable period of time, whether the data sharing shall be resumed or not and if yes, indicate under which conditions.	therefore unlikely that the data holder could have the bandwidth to put additional measures into place before damage is done. • The Parliament's proposal should specify that the 'specific necessary measures' refer to Art. 2 of the Trade Secrets Directive and the minimum standard of measures required for trade secret protection. • The data holder may receive a number of data access requests, which would result in a number of contractual arrangements. We would welcome the introduction of safeguards and objective criteria in case an agreement cannot be reached. • Protections against data misuse for health and safety reasons must be in place, in conformity with Art. 114(3) TFEU. One example of a threat to human health and safety would be where medical devices could be hacked because of data shared under the Data Act. • Contractual ex-post safeguards to trade secrets may not always allow a swift identification of the person responsible for a data misuse. Non-disclosure agreements and Terms and Conditions will for instance hardly prevent misuse. • Neither proposal's address the issue of liability in depth. We strongly recommend that it specifies that any Intellectual Property rights attached to the shared data shall remain the property of the data holder. The user would not have the right to

Council position	European Parliament position	DIGITALEUROPE comments
		file for Intellectual Property over the data obtained.
(3a) **In exceptional circumstances, when the data holder can demonstrate that it is highly likely to suffer serious damage from ~~an acquisition, disclosure or use~~ the disclosure of trade secrets ~~unlawful under Article 4 of Directive (EU) 2016/943, or of an unlawful use of intellectual property protected material~~, despite the technical and organisational measures taken by the user, the data holder may refuse the request for access. Such demonstration shall be duly substantiated, provided in writing and without undue delay. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.**		• We welcome Council's much needed introduction of an Art.4(3a) and the introduction of recitals 28(a) and 1(4c), which sets grounds for refusal. However, the grounds for refusal are highly restrictive and limited to trade secrets. The proposal risks ignoring the risks of misuse of data for health, safety, security and privacy. • We recommend that instead of 'exceptional circumstances' the wording 'by exception' should be used. Indeed, the grounds for refusal are limited not only to 'exceptional circumstances,' but also where the data holder can prove that it is 'highly likely to suffer serious damage.' Art. 4(3a) therefore places a high burden of proof by setting an obligation to demonstrate that a data holder is 'highly likely to suffer serious damage.' Indeed, the data holder would have to both predict or foresee both the likelihood of the damage occurring *as well as* the level of seriousness of that damage. • Having to demonstrate *a high likeliness* of suffering a *serious* damage on a case-by-case basis would further be costly, and resource-intensive.

Council position	European Parliament position	DIGITALEUROPE comments
		- Last, grounds for refusal should be available to third parties, as they may also suffer serious damages. Similarly, the criteria to determine that 'necessary measures' do not suffice is not clear in the proposal. The practical modalities to use Art. 4(3a) should be clarified.
(4) The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate**, nor share the data with another third party for that purpose.**	***(4)*** The user shall not use data obtained pursuant to a request referred to in paragraph 1 to develop a product that **directly** competes with the product**,** from which the data originate **and shall not use such data to derive insights about the economic situation, assets and production methods of the manufacturer**.	- We welcome the inclusion of third parties in the Council's proposal. - In the Parliament's proposal, whilst clarity around 'insights about the economic situation, assets and production methods' is welcome, we recommend that it concern the data holder rather than the manufacturer. - In the Parliament position, to avoid condoning unfair competition, we strongly recommend that the word 'directly' is removed. The Data Act should encourage trusted relationships and not start data-access wars.
(4a) The user shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.	**(4a) The user shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.**	The provision is intended to prevent access to data through coercive means. The word 'evident' should be therefore be deleted, abusing any gaps should be unlawful.

Council position	European Parliament position	DIGITALEUROPE comments
	(4b) Users have the right to either directly share, through a data holder or through providers of data intermediation services as set in the Regulation (EU) 2022/868, non-personal data accessed from the connected product or obtained pursuant to a request referred in paragraph 1 to any data recipient for commercial or non-commercial purposes. The data sharing between a user and a data recipient shall be carried out by means of contractual agreements; the provisions of Chapter IV on fair, reasonable and non-discriminatory terms shall apply mutatis mutandis to the contractual agreements between users and data recipients.	
(5) Where the user is not ~~a~~ **the** data subject **whose personal data is requested**, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6~~(1)~~ of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 **and Article 5(3) of** ~~**Regulation**~~ **Directive (EU) 2002/58** are fulfilled.	(5) Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where ***all conditions and rules provided by the applicable data protection law are complied with, in particular where*** there is a valid legal basis under Article ***6*** of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 ***and Article 5(3) of Directive 2002/58/EC*** are fulfilled.	
(6) The data holder shall only use any non-personal data generated by the use of a product or related service	(6) **Data holders** shall only use any non-personal data **accessed from a connected product or**	

Council position	European Parliament position	DIGITALEUROPE comments
on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active.	generated **during the provision of a** related service on the basis of a contractual agreement with the user. The data holder shall not **make the use of the product or related service dependent on the user allowing it to process data not required for the functionality of the product or provision of the related service. The data holder shall delete the data when they are no longer necessary for the purpose contractually agreed. Data holders and the users shall not** use such data **obtained, collected or** generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use **of the product or related service** by the **other party** that could undermine the commercial position of the **other party** in the markets in which the user is active.	
	(6a) Data holders shall not make available non-personal data accessed by them from the connected product, referred to in point (a) of Article 3(2), to third parties for commercial or non-commercial purposes other than the fulfilment of their contractual obligations to the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them.	The reference to data 'referred to in point (a) of Article 3(2)' is unclear. If it includes information such as type of data, format, estimated volume, the provision would disproportionately limit the data holder's right to share data about their own product and contractual freedom to share information with suppliers or other relevant parties. This would disproportionally affect smaller companies which may not be able to analyse data in-house and would need to share with select third parties (including to improve products and services, for instance by sharing diagnostics data).

Council position	European Parliament position	DIGITALEUROPE comments
	(6b) Where the contractual agreement between the user and a data holder allows for the use of non personal data accessed by them from the connected product, referred to in point (a) of Article 3(2a), the data holder shall be able to use that data for any of the following purposes: (a) **improving the functioning of the connected product or related services;** (b) **developing new products or services;** (c) **enriching or manipulating it or aggregating it with other data, including with the aim of making available the resulting data set to third parties, as long as such derived data set does not allow the identification of the specific data items transmitted to the data holder from the connected product, or allow a third party to derive those data items from the data set.**	The data holder should fully be able to improve, design and develop better and new products. Instead, the Parliament's proposal impedes on contractual freedom and sets a short list of options. This precludes innovation based on making value out of data. At the very least this provision should clearly state that the list of purposed is non-exhaustive.
	(6c) Users, in business-to- business relations, have the right to make data available to data recipients or data holders under any lawful contractual condition, including by agreeing to limit or restrict further sharing of such data, and to be compensated proportionately in exchange for foregoing their right to use or share such data lawfully. Data recipients or data holders shall not make the offer of a related service, or its commercial terms,	Here, Parliament's position recognised the right to contractual freedom for businesses. Indeed, we welcome the recognition that contracts can be mutually beneficial to the user and to the data holder.

Council position	European Parliament position	DIGITALEUROPE comments
	including pricing, contingent on such agreement by the user, or coerce, deceive or manipulate in any other way the user to make available data under such contractual conditions.	
	Article 5	
*Right **of the user** to share data with third parties*	*Right **of the user** to share data with third parties*	
(1) Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service **that are ~~accessible~~ readily available to the data holder** to a third party**, as well as the ~~relevant~~ metadata that is necessary to interpret and use that data,** without undue delay, free of charge to the user, of the same quality as is available to the data holder**, easily, securely, in a structured, commonly used and machine-readable format** and, where applicable, continuously and in real-time. **The making available of the data by the data holder to the third party ~~This~~ shall be done in accordance with the conditions and compensation rules set in Articles 8 and 9.**	(1) Upon request by a user, or by a party acting on behalf of a user, **such as an authorised data intermediation service in the meaning of the Regulation (EU) 2022/868, data holders** shall make available the data **accessed by them from a connected** product or **generated during the provision of a** related service to a third party, without undue delay, **easily, securely, in a comprehensive, structured, commonly used and machine-readable format,** free of charge to the user, of the same quality as is available to the data holder and, where **relevant and technically feasible** continuously and in real-time. **Where the user is a data subject, personal data shall be processed for purposes specified by the data subject, such as the following:** **(a) the provision of after-market services, such as the maintenance and repair of the product, including after-market services in competition with a**	- Real-time data sharing included in Art. 4 and 5 should not be mandatory where it is not technically feasible, or where the confidentiality, integrity and availability of a device or service can be compromised. Just as the GDPR sets limits to real-time sharing, the Data Act should at the very least account for the risks and difficulties with sharing large volumes of diverse data.

Council position	European Parliament position	DIGITALEUROPE comments
	connected product or service provided by a data holder; **(b) enabling the user to update the software of the connected product or related services in particular to fix security and usability problems;** **(c) specific data intermediation services recognised in the Union or specific services provided by data altruism organisations recognised in the Union under the conditions and requirements of Chapters III and IV of Regulation (EU) 2022/868.** **Data shall be provided in the form in which they have accessed from the product, with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data. Information derived or inferred from this data by means of complex proprietary algorithms, in particular where it combines the output of multiple sensors in the connected product, shall not be considered within the scope of a data holder's obligation to share data with users or data recipients, unless agreed differently between the user and the data holder.**	

Council position	European Parliament position	DIGITALEUROPE comments
	(1a) The right under paragraph 1 shall not apply to data resulting from the use of a product or related service in the context of testing of other new products, substances or processes that are not yet placed on the market unless use by a third party is permitted by the agreement with the enterprise with whom the user agreed to use one of its products for testing of other new products, substances or processes.	
(2) Any undertaking ~~providing core platform services for which one or more of such services have been~~ designated as a gatekeeper, pursuant to Article **3** ~~[…]~~ of ~~[~~Regulation ~~XXX~~ **(EU) 2022/1925**~~]~~ on contestable and fair markets in the digital sector (Digital Markets Act), shall not be an eligible third party under this Article and therefore shall not: (a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1); (b) solicit or commercially incentivise a user to request the data holder to make data	**(2)** Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper, pursuant to Article […] of Regulation **(EU) 2022/1925**, shall not be an eligible **data recipient** under this Article and therefore shall not: **a.** solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1); **b.** solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;	The definition of a 'product' having been substantially expanded, the scope of Art 5(2) should be aligned to that of the DMA, so that it applies to core platform services.

Council position	European Parliament position	DIGITALEUROPE comments
available to one of its services pursuant to paragraph 1 of this Article; (c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).	**c.** receive data from a user that the user has obtained pursuant to a request under Article 4(1).	
(3) The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1. The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.	(3) The user or **the data recipient** shall not be required to provide any information beyond what is necessary to verify the quality as user or as **data recipient** pursuant to paragraph 1. **Data holders** shall not keep any information on the **data recipient**'s access to the data requested beyond what is necessary for the sound execution of the **data recipient**'s access request and for the security and the maintenance of the data infrastructure.	
(4) The third party shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.	(4) The **data recipient** shall not deploy coercive means or abuse gaps in the technical infrastructure of **a** data holder designed to protect the data in order to obtain access to data.	
(5) The data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the	(5) The data holder shall not use any non-personal data **obtained, collected or** generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party	

Council position	European Parliament position	DIGITALEUROPE comments
commercial position of the third party on the markets in which the third party is active, unless the third party has ~~consented~~ **given permission** to such use and has the technical possibility to withdraw that consent at any time.	that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has **expressly** consented to such use and has the technical possibility to **easily** withdraw that consent at any time	
(6) Where the user is not ~~a~~ **the** data subject **whose personal data is requested**, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6~~(1)~~ of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 **and Article 5(3) of ~~Regulation~~ Directive (EU) 2002/58** are fulfilled.	(6) **In the case of** a data subject **who is not the user requesting access**, any personal data **obtained, collected, or** generated by **their** use of a product or related service**, and data derived and inferred from that use,** shall only be made available **by the data holder to the third party** where there is a valid legal basis under Article **6** of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 **and Article 5(3) of Directive 2002/58/EC** are fulfilled.	
(7) Any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation.	(7) Any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation.	
(8) 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	(8) Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose **of the request**	See comments to Art.4(3a).

Council position	European Parliament position	DIGITALEUROPE comments
party and all specific necessary measures **including technical and organisational measures** agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. **Where the data holder can show that such measures do not suffice, the data holder and the third party shall agree on necessary additional measures.** ~~In such a case, the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party.~~ **The data holder shall identify the data which are protected as trade secrets, including in the relevant metadata.**	agreed between the user and the third party and all specific necessary measures agreed between the data holder**, or between the trade secrets holder if it is not simultaneously the data holder,** and the third party are taken **prior to the disclosure** by the third party to preserve the confidentiality of the trade secret. In such a case, the **data holder or the trade secret holder, shall identify** the data **which are protected** as trade secrets and the **technical and organisational** measures for preserving **their** confidentiality**, as well as on liability provisions. Such technical and organisational measures** shall be specified in the agreement between the data **or trade secret** holder and the third party**, including, as appropriate through model contractual terms, strict access protocols, confidential agreements, technical standards and the application of codes of conduct. In cases where the third party fails to implement those measures or undermines the confidentiality of trade secrets, the data holder shall be able to suspend the sharing of data identified as trade secrets. In such cases, the data holder must immediately notify the data coordinator of the Member State in which the data holder is established, pursuant to Article 31, that it has suspended the sharing of data and identify which measures have not been implemented or which trade secrets**	• We also recommend that the final Regulation clarifies or defines the ‘necessary measures’ expected between data holders and users and the ‘specific necessary measures’ expected between data holders and third parties, as well as ‘additional’ ones.

Council position	European Parliament position	DIGITALEUROPE comments
	have had their confidentiality undermined. Where the third party wishes to challenge the data holder's decision to suspend the sharing of data, the data coordinator shall decide, within a reasonable period of time, whether the data sharing shall be resumed or not and if yes, indicate under which conditions.	
(8a) In exceptional circumstances, when the data holder can demonstrate that it is highly likely to suffer serious damage from ~~an acquisition, disclosure or use~~ the disclosure of trade secrets ~~unlawful under Article 4 of Directive (EU) 2016/943, or of an unlawful~~ ~~use of intellectual property protected material~~, despite the technical and organisational measures taken by the third party, the data holder may refuse the request for access. Such demonstration shall be duly substantiated, provided in writing and without undue delay. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.		• We welcome Council's much needed introduction of an Art.5(8a) and the introduction of recitals 28(a) and 1(4c), which sets grounds for refusal. • However, the grounds for refusal are highly restrictive and limited to trade secrets. The proposal risks ignoring the risks of misuse of data for health, safety, security and privacy. • It is also limited not only to 'exceptional circumstances,' but also where the data holder can prove that it is 'highly likely to suffer serious damage.' Art. 4(3a) therefore places a high burden of proof by setting an obligation to demonstrate that a data holder is 'highly likely to suffer serious damage.' Indeed, the data holder would have to both predict or foresee both the likelihood of the damage occurring *as well as* the level of seriousness of that damage. • Having to demonstrate *a high likeliness* of suffering a *serious* damage on a case-by-case basis would further be costly, and

Council position	European Parliament position	DIGITALEUROPE comments
		resource-intensive. Similarly, the obligation to 'duly substantiate' grounds for refusal in a short timeframe, as well as notify it could be interpreted differently by national courts. - Last, grounds for refusal should be available to third parties, as they may also suffer serious damages. Similarly, the criteria to determine that 'necessary measures' do not suffice is not clear in the proposal. The practical modalities to use Art. 5(8a) should be clarified.
(9) ~~The right referred to in paragraph 1 shall not adversely affect data protection rights of others~~.	(9) The right referred to in paragraph 1 shall not adversely affect ***the*** rights of ***data subjects of*** others ***pursuant to the applicable data protection law***.	
Article 6		
Obligations of third parties receiving data at the request of the user	*Obligations of* ***data recipients*** *receiving data at the request of the user*	
(1) A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the	(1) A **data recipient** shall process data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and **where all conditions and rules provided by the applicable data protection law are complied with, notably where there is a valid legal basis under Article 6(1) of**	

Council position	European Parliament position	DIGITALEUROPE comments
data when they are no longer necessary for the agreed purpose	**Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 and Article 5(3) of Directive 2002/58/EC are fulfilled, and** subject to the rights of the data subject insofar as personal data are concerned**. The data recipient** shall delete the data when they are no longer necessary for the agreed purpose**, unless otherwise agreed with the user.**	
(2) The third party shall not: a. coerce, deceive or manipulate **in any way and at any time** the user **or the data subject where** ~~**the user is not a**~~ **the data subject is not the user,** ~~in any way~~, by subverting or impairing the autonomy, decision-making or choices of the user **or the data subject**, including by means of a digital interface with the user **or the data subject**; b. use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of Regulation (EU) 2016/679, unless it is **objectively** necessary ~~to provide~~ **for a purpose that is integral to the delivery of** the service requested by the user; c. make the data **it receives** available ~~it receives~~ to ~~another~~ **other** third ~~party~~ **parties**, in raw, aggregated or derived form, unless this is necessary to provide the	(2) The ***data recipient*** shall not: a. ***make the exercise of the rights or choices of users unduly difficult including by offering choices to the users in a non-neutral manner, or*** coerce, deceive or manipulate the user in any way, ***or*** by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user ***or a part thereof, including its structure, design, function or manner of operation***; b. use the data it receives for the profiling of natural persons within the meaning of Article ***4, point (4),*** of Regulation (EU) 2016/679, ***other than in accordance with that Regulation***;	

Council position	European Parliament position	DIGITALEUROPE comments
service requested by the user **and provided that the other third parties take all necessary measures agreed between the data holder and the third party to preserve the confidentiality of trade secrets**; d. make the data **it receives** available ~~it receives~~ to an undertaking ~~providing core platform services for which one or more of such services have been~~ designated as a gatekeeper pursuant to Article **3** ~~[…]~~ of ~~[~~Regulation **(EU) 2022/1925** ~~on contestable and fair markets in the digital sector (Digital Markets Act)]~~; e. use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose; f. prevent the user, including through contractual commitments, from making the data it receives available to other parties.	c. make the data it receives ***available*** to another third party ***without making the user aware in a clear and easily accessible way and seeking its the explicit contractual permission*** by the user; d. make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article ***3 of [Regulation (EU) 2022/1925*** (Digital Markets Act)]; e. use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose; ***data recipients shall also not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the data holder that could undermine the commercial position of the data holder on the markets in which the data holder is active;***	

Council position	European Parliament position	DIGITALEUROPE comments
	(ea) use the data it receives in a manner that adversely impacts the security of the product or related service(s); **(eb) where relevant, disregard the specific measures agreed with a data holder or with the trade secrets holder pursuant to article 5 (8) of this Regulation and break the confidentiality of trade secrets;** **(ec) use the data to disrupt sensitive critical infrastructure protection information within the meaning of Article 2(d) of Directive 2008/114/EC.**	
	(2a) The third party shall bear the responsibility to ensure the security and protection of the data it receives from a data holder.	
CHAPTER III		
Article 9		
Compensation for making data available.	Compensation for making data available.	
(1) Any compensation agreed **upon** between a data holder and a data recipient for making data available **in business-to-business relations** shall	(1) Any compensation agreed between a data holder and a data recipient for making data available ***in business- to- business relations*** shall be ***non -***	- We welcome the Council's proposal to take into account the investment required for making the data available and a margin in

Council position	European Parliament position	DIGITALEUROPE comments
be reasonable~~,~~ **and may include a margin.**~~.~~ ~~**Such reasonable compensation may include the costs incurred and investment required for making the data available as well as a margin, which may vary for objectively justified reasons relating to the data.**~~	***discriminatory and*** reasonable. ***A data holder, a data recipient or a third party shall not directly or indirectly charge consumers or data subjects a fee, compensation or costs for sharing data or accessing it.***	calculating reasonable compensation. To help the data economy continue to grow, companies should be incentivised and able to obtain remuneration for sharing data. • The cost of putting in place the right infrastructure and internal processes to adequately respond to data requests should however be recognised and remunerated in B2B and B2C relations. We therefore recommend that the last sentence of Parliament's proposal be deleted.
(1a) The data holder and the data recipient shall take into account ~~reflect~~ in particular: **(1) the costs incurred and investments required for making the data available, including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage;** **(2) the investments in data collection and production, taking into account whether other parties contributed to the obtaining, generating or collecting the data in question.** **Such compensation may also depend on the volume, format and nature of the data.**		• We welcome the Council's proposal that the data recipient and the data holder together shall take into account specific costs and investments, such as the cost of making data available. Data holders and recipients should be given the possibility to agree, without one party having to demonstrate that compensation is reasonable as stated in (4) of this provision. • We also welcome the inclusion of volume, format and nature of the data in the calculation.

Council position	European Parliament position	DIGITALEUROPE comments
(2) Where the data recipient is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, **provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro, small or medium enterprise**, any compensation agreed shall not exceed the costs **set out in paragraph 1a(a).** ~~directly related to making the data available to the data recipient and which are attributable to the request.~~ ~~**These costs include the costs necessary for data reproduction, dissemination via electronic means and storage, but not of data collection or production.**~~ ~~Article 8(3) shall apply accordingly.~~	**(2)** Where the data recipient is a ***non- profit research organisation or a SME***, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, ***provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC and do not qualify as an SME,*** any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly. ***In case of an SME, the data holder shall actively inform of the obligation to provide the data preferably on the basis of a cost-based model.***	
	(2a) The Commission shall develop guidelines to determine criteria for categories of costs related to making data available, which shall be the basis for awarding compensation pursuant to paragraph 1.	• When it comes to drafting guidelines, stakeholder consultation will be crucial to leverage concrete industry experience and best practices in determining compensation schemes.
(3) This Article shall not preclude other Union law or national legislation ~~implementing~~ **adopted in accordance with Union law** from excluding compensation for making data available or providing for lower compensation.	**(3)** This Article shall not preclude other Union law or national legislation implementing Union law from excluding compensation for making data available or providing for lower compensation.	• In both proposals, Art. 9(3) still leaves room for fragmentation but very little legal certainty in relation to other legislative frameworks. • We recommend that the exclusion be limited to strict conditions where Member State law might derogate from the Regulation's

Council position	European Parliament position	DIGITALEUROPE comments
		provisions, such as on ‘an exceptional basis and when duly justified.’
(4) The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can ~~verify that~~ **assess whether** the requirements of paragraph 1 and, where applicable, paragraph 2 are met.	**(4)** The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can verify that the requirements of paragraph 1 and, where applicable, paragraph 2 are met.	• By obliging the data holder to demonstrate that compensation is ‘reasonable,’ the fairness test holds a de facto presumption against data holders. • Art. 9(4) requires that the data holder provide ‘information setting out the basis for the calculation of the compensation in sufficient detail,’ which may contain sensitive financial information. • This additional obstacle, besides the possibility that EU or Member State law can in any event provide for lower or no compensation, risks in fact discouraging data sharing. • Instead, parties should be given the opportunity to negotiate data sharing contracts as best allows trusted commercial relations.
(4a) The Commission shall adopt guidelines on the calculation of reasonable compensation, taking into account the opinion of the European Data Innovation Board established under Regulation (EU) 2022/868.		• When it comes to drafting guidelines as per the new Art. 9(4a), stakeholder consultation will be crucial to leverage concrete industry experience and best practices in determining compensation schemes.

Council position	European Parliament position	DIGITALEUROPE comments
CHAPTER V		
~~[~~**MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES,** ~~AND~~ ~~**UNION INSTITUTIONS, AGENCIES**~~ **THE COMMISSION, THE EUROPEAN CENTRAL BANK OR UNION BODIES BASED ON EXCEPTIONAL NEED**~~]~~	MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES AND UNION INSTITUTIONS, AGENCIES OR BODIES BASED ON EXCEPTIONAL NEED	
Article 14		
Obligation to make data available based on exceptional need	Obligation to make data available based on exceptional need	
(1) Upon request, a data holder shall make data**, which could include**~~**ing**~~ ~~**relevant**~~ **metadata that is necessary to interpret and use that data,** available to a public sector body or to ~~a Union institution, agency or body~~ **the Commission, the European Central Bank or Union bodies** demonstrating an exceptional need**, as laid out in Article 15,** to use the data requested **in order to carry out their** ~~**legal competencies**~~ **statutory duties in the public interest.**	(1) Upon **a specified duly justified** request **limited in time and scope**, a data holder **that is a legal person** shall make **non-personal data which are available at the time of the request, including metadata** available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.	- We welcome and support the Parliament's clarification that a request must be 'duly justified' and 'limited in time and scope.' - The exclusion of personal data is also fundamental in Chapter V, as here the Data Act goes beyond the GDPR in giving public bodies access to personal data. Indeed, the relevant tasks of public interest, the public sector bodies, Union institutions, agencies or bodies involved have not been identified. The EDPB and EDPS Joint Opinion on the Data Act should still apply to the Parliament and Council positions: 'Instead, the Proposal sets out a number of conditions that would give

Council position	European Parliament position	DIGITALEUROPE comments
		rise to a legal obligation for the data holder to provide personal data.'[15] • Whilst we welcome the Parliament's mention that the request should be 'limited in time and scope,' we believe such limits should be clarified in the Proposal itself. The proposal would thus mitigate the risk of fragmentation and allow companies to prepare for emergency response.
(2) ~~This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.~~	(2) This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.	
	(2a) This Chapter shall not preclude voluntary arrangements between businesses and public sector bodies and union institutions, agencies or bodies for the sharing of data for purpose of delivering public services, including for exceptional needs if stipulated in their contracts.	
Article 15		
Exceptional need to use data	*Exceptional need to use data*	
(1) ~~e~~**E**xceptional need to use data within the meaning of this Chapter shall be **limited in time and scope and** deemed to exist **only** in ~~any of~~ the following circumstances: a. where the data requested is necessary to respond to a public emergency **and the**	(1) An exceptional need to use ***non-personal*** data within the meaning of this Chapter shall be ***limited in time and scope and shall be*** deemed to exist in the following circumstances:	• **<u>Council</u>**: Additionally, in the Council position, the recently proposed exemption of requests for official statistics – from the obligation to

[15] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

Council position	European Parliament position	DIGITALEUROPE comments
public sector body, the Commission, the European Central Bank or Union body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions; b. where the data request is ~~limited in time and scope and~~ necessary to ~~prevent~~ **mitigate** a public emergency or to assist the recovery from a public emergency **and the public sector body, the Commission, the European Central Bank or Union body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions**; **or** c. where the lack of available data prevents the public sector body**,** ~~or Union institution, agency or body~~ **the Commission, the European Central Bank or Union bodies** from fulfilling a specific task in the public interest**, such as official statistics,** that has been explicitly provided by law; and the public sector body ~~or Union institution, agency or body~~ **the Commission, the European Central Bank or Union body has exhausted all other means at its disposal** ~~has been unable~~ to obtain such data ~~by alternative means~~, including**, but not limited to,** ~~by~~ **purchase**~~ing~~ **of** the data on the market ~~at~~ **by offering** market rates or ~~by~~ relying on existing obligations to	(a) where the data requested is necessary to respond to public emergency; (b) ***in non-emergency situations,*** where the ***public sector body or Union institution, agency or body is acting on the basis of Union or national law and has identified specific data, which is unavailable to it and which is*** necessary to ***fulfil, a specific task in the*** public ***interest that has been explicitly provided by law such as the prevention or*** recovery from a public emergency ***and which the public sector body or Union institution, agency or body has been unable to obtain by any of the following means: voluntary agreement***; ***by purchasing the data on the market or by relying on existing obligations to make data available.***	demonstrate that data could not be obtained on the market – further increases the possibility of abusing the framework set in Chapter V. • **General remarks:** Overall, in both Parliament and Council positions, although some clarifications have been brought to mitigate arbitrary data requests, conditions and processes framing such requests need to be further developed and offer enough foresight to users and data holders. For instance, details as to the demonstration supporting a request should not be left to recitals, for example Recital 58. • We welcome Parliament's exclusion of personal data, although the cost of separating and identifying personal or non-personal data should be recognised. • As specified by the EDPB Opinion, to ensure lawfulness, necessity and proportionality, the **scope** and **manner** of the exercise of their powers by the competent authorities must be defined, and users and data holders protected from arbitrary interference. • Article 15 in both the Council and the Parliament's proposals remains extremely problematic due to its broad scope going far beyond the notion of 'public emergency' and 'exceptional need.' This is specifically the

Council position	European Parliament position	DIGITALEUROPE comments
make data available, ~~and~~ **or** the adoption of new legislative measures **which could guarantee** ~~cannot ensure~~ the timely availability of the data**.**~~; or~~ ~~obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises.~~		case with Article 15(c), which enables any public body to request data to carry a 'specific task in the public interest,' a concept loosely defined and open to excessive discretion.
(2) Letters (b) and (c) of paragraph 1 shall not apply to small and micro enterprises as defined in article 2 of the Annex to Recommendation 2003/351/EC 2003/361/EC.		
(3) The obligation to demonstrate that the public sector body was unable to obtain data by purchasing of the data on the market shall not apply in case the specific task in the public interest is the production of official statistics and where the purchase of data is <u>prohibited</u> <u>not allowed</u> by national law		
	Article 15a	
	Single point to handle public sector bodies' request	
	(1) **The data coordinator designated pursuant to Article 31 shall be responsible for coordinating the requests pursuant Article 14(1) from the sector bodies of the Member**	

Council position	European Parliament position	DIGITALEUROPE comments
	State concerned, in order to ensure that the requests meet the requirement laid down in this Chapter and shall transmit them to the data holder. It shall avoid multiple requests by different public sector bodies within their territory to the same data holder. (2) **Member States shall regularly inform the Commission about requests pursuant to Article 14(1).** (3) **Where public sector bodies or Union institutions, agencies or bodies requires data from the same data holder in more than one Member State on the basis of an exceptional need pursuant Article 14(1), the competent authorities of the Member States shall cooperate in accordance with Article 22 to coordinate their requests where it is necessary to minimise the administrative burden on the data holders.** (4) **The Commission shall develop a model template for requests pursuant to Article 17**	
Article 17		
Requests for data to be made available	*Requests for data to be made available*	
(1) Where requesting data pursuant to Article 14(1), a public sector body or ~~a Union institution, agency or~~	**(1) In a request for** data pursuant to Article 14(1), a public sector body or a Union institution, agency or body shall:	- We support Parliament's proposal to specify the datasets covered by B2G data requests. Indeed, the Data Act should allow

Council position	European Parliament position	DIGITALEUROPE comments
~~body~~ **the Commission, the European Central Bank or Union body** shall: (a) specify what data are required**, including ~~relevant~~ metadata that is necessary to interpret and use that data**; (b) demonstrate **that** the **conditions necessary for the existence of the** exceptional need **as described in Article 15** for which the data are requested **are met**; (c) explain the purpose of the request, the intended use of the data requested**, including when applicable by a third party in accordance with paragraph 4,** and the duration of that use; (d) state the legal ~~basis~~ **provision allocating to the requesting public sector body or to ~~Union institutions, agencies or~~ the Commission, the European Central Bank or Union bodies the specific public interest task relevant** for requesting the data **~~as well as the specific legal basis for the processing of personal data in Union or Member State law~~**; (e) specify the deadline **referred to in Article 18 and** by which the data are to be made available or within which the data holder may request the public sector body, ~~Union institution, agency~~ **the Commission, the**	(a) **request data within their remit and** specify what **datasets** are required; (b) demonstrate the exceptional need for which the data are requested **and compliance with the conditions mentioned in Article 15**; (c) explain the purpose of the request, the intended use of the data requested, and the duration of that use; **(ca) specify, if possible, when the data is expected to be deleted by all parties that have access to it;** **(cb) justify the choice of data holder to which the request is addressed;** **(cc) specify any other public sector bodies, Union institutions, agencies or bodies and the third parties with which the data requested is expected to be shared with;** **(cd) disclose the identity of the third party referred to in paragraph 4 of this Article, and in Article 21 of this Regulation;** **(ce) apply all relevant ICT security measures concerning the transfer and storage of data;** (d) state the legal basis for requesting the data;	foreseeability and preparedness for companies in public emergencies, which are by nature time-sensitive.

Council position	European Parliament position	DIGITALEUROPE comments
European Central Bank or **Union** body to modify or withdraw the request	**(da) specify the geographical limits that apply to the request for data;** (e) specify the deadline by which the data are to be made available **and** within which the data holder may request the public sector body, Union institution, agency or body to modify or withdraw the request**;** **(ea) submit a declaration on the lawful and secure handling of the data requested, including the confidentiality of trade secrets;** **(eb) ensure that making the data available does not put the data holder in a situation that violates Union or national law or confer liability on the data holder for any infringement or damage resulting from the data access that a public sector body or a Union institution, agency or body has requested**	
(2) A request for data made pursuant to paragraph 1 of this Article shall: (a) be expressed in clear, concise and plain language understandable to the data holder; (b) be proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested;	(2) A request for data made pursuant to paragraph 1 of this Article shall: (a) **be made in writing and** be expressed in clear, concise and plain language understandable to the data holder; **(aa) be submitted through the competent authority;**	

Council position	European Parliament position	DIGITALEUROPE comments
(c) respect the legitimate aims of the data holder, taking into account the protection of trade secrets and the cost and effort required to make the data available; (d) **in case of requests made pursuant to Article 15, points (a) and (b)** concern, insofar as possible, non-personal data; **in case personal data are requested, the request should justify the need for including personal data and set out the technical and organisational measures that will be taken to protect the data;** **(da) in case of requests made pursuant to Article, 15 point (c), concern personal data only in case the data processing has a specific basis in Union or Member State law;** (e) inform the data holder of the penalties that shall be imposed pursuant to Article 33 by a competent authority referred to in Article 31 in the event of non-compliance with the request; (f) be made publicly available online without undue delay**, unless this would create a risk for public security, and the requesting public sector body shall inform notify the competent authority referred to in Article 31, of the Member State where the requesting public sector body is established. The Commission,**	**(ab) be specific with regards to the type of data is requested and correspond to data which the data holder has available at the time of the request;** (b) be **justified and** proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested; (c) respect the legitimate aims of the data holder, taking into account the protection of trade secrets and the cost and effort required to make the data available**. Where applicable, specify the measures to be taken pursuant to Article 19(2) to preserve the confidentiality of trade secrets, including, as appropriate, through the use of model contractual terms, technical standards and codes of conduct**; (d) concern **only** non-personal data; (e) inform the data holder of the penalties that shall be imposed pursuant to Article 33 by a **data coordinator** referred to in Article 31 in the event of non-compliance with the request; (f) **be transmitted to the data coordinator referred to in Article 31, who shall**	

Council position	European Parliament position	DIGITALEUROPE comments
the European Central Bank and Union bodies shall make their requests available online without undue delay and inform the Commission thereof;. **(fa) in case personal data are requested, be notified without undue delay notify to the independent supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 in the member state where the data holder is established.**	**make the request** publicly available online without undue delay; **the data coordinator may inform the public sector body or Union institution, agency or body if the data holder already provided the requested data in response to previously submitted request for the same purpose by another public sector body or Union institution agency or body.**	
(3) A public sector body or ~~a Union institution, agency~~ **the Commission, the European Central Bank** or **Union** body shall not make data obtained pursuant to this Chapter available for reuse within the meaning of Directive (EU) 2019/1024 **or Regulation (EU) 2022/868**. Directive (EU) 2019/1024 **and Regulation (EU) 2022/868** shall not apply to the data held by public sector bodies obtained pursuant to this Chapter.	(3) A public sector body or a Union institution, agency or body shall not make data obtained pursuant to this Chapter available for reuse within the meaning of Directive (EU) 2019/1024 **and Regulation (EU) 2022/868**. Directive (EU) 2019/1024 **and Regulation (EU) 2022/868** shall not apply to the data held by public sector bodies obtained pursuant to this Chapter.	
(4) Paragraph 3 does not preclude a public sector body or a Union institution, agency or **the Commission, the European Central Bank or Union** body to exchange data obtained pursuant to this Chapter with another public sector body, Union institution, agency or **the Commission, the European Central Bank or Union** body, in view of completing the tasks in Article 15 or to make the data available to a third party in cases where it has outsourced, by	(4) Paragraph 3 does not preclude a public sector body or a Union institution, agency or body to exchange data obtained pursuant to this Chapter with another public sector body, Union institution, agency or body, **for the purpose** of completing the tasks in Article 15 **which was included the request in accordance with paragraph 1(cc),** or to make the data available to a third party in cases where it has outsourced, by means of a	

Council position	European Parliament position	DIGITALEUROPE comments
means of a publicly available agreement, technical inspections or other functions to this third party. The obligations on public sector bodies, Union institutions, agencies or **the Commission, the European Central Bank or Union** bodies pursuant to Article 19 apply **also to such third parties.** Where a public sector body or a Union institution, agency or **the Commission, the European Central Bank or Union** body transmits or makes data available under this paragraph, it shall notify **without undue delay** the data holder from whom the data was received	publicly available agreement, technical inspections or other functions to this third party. **It shall bind the third party contractually not to use the data for any other purposes and not to share is with any other third parties, Where a public sector body or a Union institution, agency or body transmits or makes data available under this paragraph, it shall notify the data holder from whom the data was received without undue delay. Within five working days of that notification, the data holder shall have the right to submit a reasoned objection to such transmission or making available of data. In the case of a rejection of the reasoned objection by the public sector body or a Union institution, agency or body, the data holder may bring the matter to the data coordinator referred to in Article 31. The receiving** public sector bodies, Union institutions, agencies or bodies **and third parties shall be bound by the obligations laid down in** Article 19. **Data obtained pursuant this chapter shall be used only for the purpose specified in the request. Public sector bodies, Union institutions, agencies or bodies shall bind contractually third parties with whom they agreed to share data pursuant paragraph 4**	

Council position	European Parliament position	DIGITALEUROPE comments
	not to use the data for any other purpose and not to share it with other parties	
Article 18		
Compliance with requests for data	*Compliance with requests for data*	
(1) A data holder receiving a request for access to data under this Chapter shall make the data available to the requesting public sector body or a Union institution, agency or **the Commission, the European Central Bank or Union** body without undue delay.	(1) A data holder receiving a request for access to data under this Chapter shall make the data available to the requesting public sector body or a Union institution, agency or body without undue delay**, taking into account provision of time and necessary technical, organisational and legal measures.**	
(2) Without prejudice to specific needs regarding the availability of data defined in sectoral legislation, the data holder may decline or seek the modification of the request **without undue delay and not later than** within 5 working days following the receipt of a request for the data necessary to respond to a public emergency and **without undue delay and not later than** within 15 working days in other cases of exceptional need, on either of the following grounds: (a) ~~the data is unavailable~~ **the data holder does not have control over the data requested;** (b) the request does not meet the conditions laid down in Article 17(1) and (2)	(2) Without prejudice to specific needs regarding the availability of data defined in sectoral legislation, the data holder may decline or seek the modification of the request within **five** working days following the receipt of a request for the data necessary to respond to a public emergency and within **30** working days in other cases of exceptional need, on either of the following grounds: (a) the data is **not available to the data holder at the time of the request**;**(aa) provided security measures concerning transfer, storing and maintaining confidentiality are insufficient;**	

Council position	European Parliament position	DIGITALEUROPE comments
	(ab) a similar request for the same purpose has been previously submitted by another public sector body or Union institution, agency or body and the data holder has not been notified of the destruction of the data pursuant to Article 19(1) point (c); (b) the request does not meet the conditions laid down in Article 17(1) and (2).	
(3) In case of a request for data necessary to respond to a public emergency, the data holder may also decline or seek modification of the request if the data holder already provided the requested data in response to previously submitted request for the same purpose by another public sector body or ~~Union institution agency or~~ **the Commission, the European Central Bank or Union** body and the data holder has not been notified of the ~~destruction~~ **erasure** of the data pursuant to Article 19(1), point (c).		
(4) If the data holder decides to decline the request or to seek its modification in accordance with paragraph 3, it shall indicate the identity of the public sector body or ~~Union institution agency or~~ **the Commission, the European Central Bank or Union** body that previously submitted a request for the same purpose.	(4) If the data holder decides to decline the request or to seek its modification in accordance with paragraph 3, it shall indicate the identity of the public sector body or Union institution agency or body that previously submitted a request for the same purpose.	

Council position	European Parliament position	DIGITALEUROPE comments
(5) **Where the dataset requested includes personal data, the data holder shall properly anonymise the data, unless** ~~Where~~ **the** compliance with the request to make data available to a public sector body or ~~a Union institution, agency or~~ **the Commission, the European Central Bank or Union** body requires the disclosure of personal data~~,~~**. In that case** the data holder shall ~~take reasonable efforts to~~ pseudonymise the data, insofar as the request can be fulfilled with pseudonymised data	(5) Where compliance with the request to make data available to a public sector body or a Union institution, agency or body requires the disclosure of personal data, the data holder shall pseudonymise the **personal** data **to be made available.**	
(6) Where the public sector body or the ~~Union institution, agency or~~ **Commission, the European Central Bank or Union** body wishes to challenge a data holder's refusal to provide the data requested~~, or to seek modification of the request~~, or where the data holder wishes to challenge the request, **and the matter cannot be solved by an appropriate modification of the request,** the matter shall be brought to the competent authority referred to in Article 31 **of the Member State where the data holder is established.**	(6) Where the public sector body or the Union institution, agency or body wishes to challenge a data holder's refusal to provide the data requested, or to seek modification of the request, or where the data holder wishes to challenge the request, the matter shall be brought to the **data coordinator** referred to in Article 31**, without prejudice to the right to submit a dispute to a civil or administrative court, in accordance with Union or national law.**	
Article 19		
Obligations of public sector bodies and ~~*Union institutions, agencies*~~ ***the Commission, the European Central Bank and Union*** *bodies*	*Obligations of public sector bodies and Union institutions, agencies and bodies.*	
(1) A public sector body or ~~a Union institution, agency or~~ **the Commission, the European**	(1) A public sector body or a Union institution, agency or body having received data pursuant to a request made under Article 14 **and statistical**	

Council position	European Parliament position	DIGITALEUROPE comments
Central Bank or Union body ~~having received~~ **receiving** data pursuant to a request made under Article 14 shall: a. not use the data in a manner incompatible with the purpose for which they were requested; b. **have** implement**ed**~~, insofar as the processing of personal data is necessary,~~ technical and organisational measures that **preserve the confidentiality and integrity of the requested data,** ~~**including**~~ **in particular** personal **data, as well as** safeguard the rights and freedoms of data subjects;	**or research organisations receiving data pursuant to a request made under Article 21(1)** shall: (a) implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects **and guarantee a high level of security and prevent the unauthorised disclosure of data**; **(ba) implement the necessary technical and organisational measures to manage cyber risk that could affect the confidentiality, integrity or availability of the requested data;** **(bb) notify the data holder from whom has received the data of any cybersecurity incident affecting the confidentiality, integrity, or availability of the received data as soon as possible but not later than 72 hours after having determined that the incident has occurred without prejudice to the reporting obligations under Regulation(EU) XXX/XXXX (EUIBAL) and Directive (EU) 2022/2555. Those entities shall be liable by damages due to a cybersecurity breach if they have not had the measures in place pursuant to paragraph 1, point (ba);**	

Council position	European Parliament position	DIGITALEUROPE comments
c. **erase** ~~destroy~~ the data as soon as they are no longer necessary for the stated purpose and inform the data holder **and individuals or organisations that received the data pursuant to paragraph 1 of Article 21 without undue delay** that the data have been **erased** ~~destroyed~~ **unless archiving of the data is required for transparency purposes in accordance with national law.**	**(2)** **erase** the data as soon as they are no longer necessary for the stated purpose and inform **without undue delay** the data holder that the data have been **erased.**	
	(1a) A public sector body, Union institution, agency, body, or a third party receiving data under this Chapter shall not: **(3) use the data to develop a product or a service that competes with the product or service or enhance an existing product or service from which the accessed data originates;** **(4) derive insights about the economic situation, assets and production or operation methods of the data holder, or share the data with another third party for that purpose; or** **(5) share the data with another third party for any of those purposes.**	

Council position	European Parliament position	DIGITALEUROPE comments
(2) Disclosure of trade secrets ~~or alleged trade secrets~~ to a public sector body or to ~~a Union institution, agency or~~ **the Commission, the European Central Bank or Union** body shall only be required to the extent that it is strictly necessary to achieve the purpose of the request. In such a case, the public sector body or the ~~Union institution, agency or~~ **Commission, the European Central Bank or Union** body shall take**, prior to the disclosure,** appropriate **measures, such as technical and organisational** measures**,** to preserve the confidentiality of those trade secrets. **The data holder shall identify the data which are protected as trade secrets, including in the relevant metadata.**	**(2)** Disclosure of trade secrets to a public sector body or to a Union institution, agency or body shall only be required to the extent that it is strictly necessary to achieve the purpose of **a** request **under Article 15**. In such a case, the **data holder shall identify the data which are protected as trade secrets. The** public sector body or the Union institution, agency or body shall take **in advance all the necessary and** appropriate **technical and organisational** measures **agreed with the data holder or with the trade secrets holder if it is not simultaneously the same legal person,** to preserve the confidentiality of those trade secrets **including as appropriate through the use of model contractual terms, technical standards and the application of codes of conduct.**	
	(2a) Where a public sector body or a Union institution, agency or body transmits or makes data available to third parties to perform the tasks that have been outsourced to it as a result of the outsourcing of technical inspections or other functions pursuant to Article 17(4), trade secrets as identified by the data holder, shall only be disclosed to the extent that they are strictly necessary for the third party to perform the tasks that have been outsourced and provided that all specific necessary measures agreed between the data holder	

Council position	European Parliament position	DIGITALEUROPE comments
	and the third party are taken in advance, including technical and organisational measures to preserve the confidentiality of those trade secrets, including as appropriate through the use of model contractual terms, technical standards and the application of codes of conduct.	
	(2b) In cases where the public sector body or a Union institution, agency or body that submitted the request for data or the third party to which data were made available pursuant to Article 17(4) fails to implement those measures or undermines the confidentiality of trade secrets, the data holder shall be able to suspend the sharing of data identified as trade secrets. In such cases, the data holder shall immediately notify the data coordinator of the Member State in which the data holder is established, pursuant to Article 31, that it has suspended the sharing of data and identify which measures have not been implemented or which trade secrets have had their confidentiality undermined. Where the public sector body or Union institution, agency or body or the third party wishes to challenge the data holder's decision to suspend the sharing of data, the data coordinator shall decide within a reasonable period of time, whether the data sharing shall be resumed or	

Council position	European Parliament position	DIGITALEUROPE comments
	not and if yes, indicate under which conditions.	
	(2c) A public sector body or a Union institution, agency or body shall be responsible for the security of the data that they receive.	
	(2d) A public sector body or a Union institution, agency or body shall notify the data holder in the event of a security breach as soon as possible, but within 48 hours at the latest.	
	Article 20	
Compensation in cases of exceptional need	*Compensation in cases of exceptional need*	
(1) Data **holders other than small and micro enterprise as defined in article 2 of the Annex to Recommendation ~~2003/351/EC~~ 2003/361/EC shall make** ~~made~~ available **data necessary** to respond to a public emergency pursuant to Article 15**(1)**, point (a), ~~shall be provided~~ free of charge.	(1) **Unless specified otherwise in Union or national law,** data made available to respond to a public emergency pursuant to Article 15, point (a), shall be provided free of charge. **The public sector body or the Union institution, agency or body that has received data shall provide public recognition to the data holder if requested by the data holder.**	• Whilst we support the principle that data made available to respond to a public emergency should be provided free of charge, exceptions should be possible due to the broad scope of Chapter V's provisions. The costs and administrative burden for companies generated by data access should be taken into account under Art. 20(1). • We recognise Parliament's inclusion of public recognition and the possibility of a fair remuneration, although it only covers 'the technical and organisational costs incurred to comply.'
(2) Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15**(1)**, points (b) or (c),	(2) The data holder **shall be entitled to fair remuneration** for making data available in compliance with a request made pursuant to	

Council position	European Parliament position	DIGITALEUROPE comments
such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation**, pseudonymisation** and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the ~~Union institution, agency or~~ **Commission, the European Central Bank or Union** body requesting the data, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.	Article 15, **point (b)**, such compensation shall **at least cover** the technical and organisational costs incurred to comply with the request including, where **applicable**, the costs of anonymisation and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the Union institution, agency or body requesting the data, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.	
(2a) Paragraph 2 shall also apply where a small and micro enterprise as defined in article 2 of the Annex to Recommendation ~~2003/351/EC~~ 2003/361/EC claims compensation for making data available.		
(2b) Data holders shall not be able to request compensation for making data available in compliance with a request made pursuant to Article 15, points (b) or (c) in case the specific task in the public interest is the production of official statistics and where the purchase of data is ~~prohibited~~ not allowed by national law.		
(3) **Where the public sector body or the ~~Union institution, agency or~~ Commission, the European Central Bank or Union body ~~wishes to challenge~~ disagrees with the level of compensation requested by the data holder, ~~the matter shall be brought~~ they may submit a**	**(2a) Where the public-sector body or the Union institution, agency or body wishes to challenge the level of remuneration requested by the data holder, the matter shall be brought to the attention of the data coordinator referred to in Article 31 of the**	

Council position	European Parliament position	DIGITALEUROPE comments
complaint to the competent authority referred to in Article 31 of the Member State where the data holder is established.	**Member State where the data holder is established.**	
Article 22		
Mutual assistance and cross-border cooperation	*Mutual assistance and cross-border cooperation*	
(1) Public sector bodies and ~~Union institutions, agencies and~~ **the Commission, the European Central Bank and Union** bodies shall cooperate and assist one another, to implement this Chapter in a consistent manner	(1) Public sector bodies and Union institutions, agencies and bodies shall cooperate and assist one another, to implement this Chapter in a consistent manner.	
(2) Any data exchanged in the context of assistance requested and provided pursuant to paragraph 1 shall not be used in a manner incompatible with the purpose for which they were requested.	(2) Any data exchanged in the context of assistance requested and provided pursuant to paragraph 1 shall not be used in a manner incompatible with the purpose for which they were requested**.**	
(3) Where a public sector body intends to request data from a data holder established in another Member State, it shall first notify the competent authority of that Member State as referred to in Article 31, of that intention **and transmit** ~~to it~~ **the request to that competent authority for examination**. **This requirement shall also apply to requests by** ~~Union institutions, agencies and~~ **the Commission, the European Central Bank and Union bodies.**	(3) Where a public sector body intends to request data from a data holder established in another Member State, it shall first notify the **data coordinator** of that Member State as referred to in Article 31, of that intention. This requirement shall also apply to requests by Union institutions, agencies and bodies. **The request shall be evaluated by the competent authority of the Member State where the data holder is established.**	
(4) After **having examined the request in the light of the requirements under Article 17,** ~~having been~~	(4) After having been notified in accordance with paragraph 3, the **data coordinator** shall advise	

Council position	European Parliament position	DIGITALEUROPE comments
~~notified in accordance with paragraph 3~~, the relevant competent authority shall **~~may~~ take one of the following actions:** a. transmit the request to the data holder~~;~~ **and, if applicable,** b. advise the requesting public sector body**, the Commission, the European Central Bank or Union body** of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request. The requesting public sector body**, the Commission, the European Central Bank or Union body** shall take the advice of the relevant competent authority into account~~.~~**;** **(eb) ~~return~~ reject the request ~~with duly justified reservations to~~ of the public sector body requesting the data for duly substantiated reasons ~~and notify it of the need to consult the competent authority of its Member State with the aim of ensuring compliance with the requirements of Article 17~~. The requesting public sector body shall take the advice of the relevant competent authority into account before possibly resubmitting the request~~.~~;**	the requesting public sector body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request. The requesting public sector body shall take the advice of the **data coordinator** into account.	

Council position	European Parliament position	DIGITALEUROPE comments
(dc) ~~return~~ reject the request ~~with duly justified reservations to~~ of the Commission, the European Central Bank or the requesting Union body for duly substantiated reasons. The Commission, the European Central Bank or the requesting Union body shall take the reservations into account before possibly resubmitting the request. **The competent authority shall act without undue delay.**		
CHAPTER VI		
SWITCHING BETWEEN DATA PROCESSING SERCIVES	SWITCHING BETWEEN DATA PROCESSING SERCIVES	
	Article 22a - Definitions	
	For the purposes of this Chapter, the following definitions apply:	
	(1) 'data processing service' means a digital service enabling ubiquitous, and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature, provided to a customer, that can be rapidly provisioned and released with minimal management effort or service provider interaction;	
	(2) 'on-premise' means an ICT infrastructure and computing resources leased or owned by the	

Council position	European Parliament position	DIGITALEUROPE comments
	customer, located in its own data centre and operated by the customer or by a third-party;	
	(3) ‘equivalent service’ means a set of data processing services that share the same primary objective and data processing service model;	
	(4) ‘data processing service data portability’ means the ability of the cloud service to move and adapt its exportable data between the customer’s data processing services, including in different deployment models;	
	(5) ‘switching’ means the process where a data processing service customer changes from using one data processing service to using a second equivalent or other service offered by a different provider of data processing services, including through extracting, transforming and uploading the data, involving the source provider of data processing services, the customer and the destination provider of data processing services;	
	(6) ‘exportable data’ means the input and output data, including metadata, directly or indirectly generated, or cogenerated, by the customer’s use of the data processing service, excluding any data processing service provider’s or third party’s assets or data protected by	• We strongly support the definition of ‘exportable data’ where it excludes data related to assets, intellectual property rights, trade secrets of confidential information.

Council position	European Parliament position	DIGITALEUROPE comments
	intellectual property rights or constituting a trade secret or confidential information;	
	(7) ‘functional equivalence’ means the possibility to re-establish on the basis of the customer’s data a minimum level of functionality in the environment of a new data processing service after the switching process, where the destination service delivers comparable outcome in response to the same input for shared functionality supplied to the customer under the contractual agreement;	
	(8) ‘egress fees’ refers to data transfer fees charged to the customers of a provider of data processing services for extracting their data through the network from the ICT infrastructure of a provider of data processing services.	
Article 23		
Removing obstacles to effective switching between providers of data processing services	*Removing obstacles to effective switching between providers of data processing services*	
(1) Providers of a data processing service shall take the measures provided for in Articles 24, 25 and 26 to ensure that **all** customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider. In particular, providers of data processing service**s** shall ~~remove~~ **not pose** ~~commercial, technical, contractual and~~	(1) Providers of a data processing service shall**, within their capacity,** take the measures provided for in Articles 24, **24a, 24b,** 25 and 26 to **enable** customers **to** switch to another data processing service, covering the **equivalent** service, which is provided by a different **provider of data processing services or, where relevant, to use several providers of data**	- We welcome the Parliament’s position where it ads the word ‘enable’ instead of ‘ensure.’ Indeed, the providers of data processing services are likely not to have control over the switching process, notably when it comes to the destination services for instance.

Council position	European Parliament position	DIGITALEUROPE comments
~~organisational~~ obstacles, **which can be, but not exclusively, of pre-commercial, commercial, technical, contractual and organisational nature, and** which inhibit customers from: (a) terminating, after ~~a~~ **the** maximum notice period **and the successful finalisation of the switching process,** ~~of 30 calendar days specified in the contract~~ **in accordance with Article 24**, the contractual agreement of the service; (b) concluding new contractual agreements with a different provider of data processing services covering the same service type; (c) porting its data **and metadata created by the customer and by the use of the originating service**~~,~~ **and/or the customer's** applications and**/or** other digital assets to another provider of data processing services **or to an on-premise system**~~;~~**, including if the customer benefited from a free-tier offering;** (d) **in accordance with** ~~paragraph 2~~ **Article 23a,** maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type, ~~in accordance with Article 26~~.	**processing services at the same time**. In particular, providers of **a** data processing service **shall not impose and** shall remove commercial, technical, contractual and organisational obstacles, which inhibit customers from: (a) terminating, after a maximum notice period of ***60*** calendar days, the contractual agreement of the service***, unless an alternative notice period is mutually and explicitly agreed between the customer and the provider where both parties are able equally to influence the content of the contractual agreement***; (b) concluding new contractual agreements with a different provider of data processing services covering the ***equivalent*** service; (c) porting ***the customer's exportable*** data, applications and other digital assets to another provider of data processing services ***or to an on-premise ICT infrastructure, including after having benefited from a free-tier offering***; (d) ***achieving*** functional equivalence ***in the use*** of the ***new*** service in the IT-environment of the different provider or providers of data processing services covering the ***equivalent*** service, in accordance with Article 26.	• Extending the notice period by a month (compared to the Commission's proposal) is insufficient as providers will be disincentivised, and in some cases prohibited, from offering fixed-term contracts, whose price and features have been tailored to a specific duration, and which customers often use 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. • The attractiveness and existence of multi-year contracts would be at risk if no penalties for early termination were possible. Thus, we welcome the amendment to the definition of 'switching charges' in the Council's proposal, which clarifies that early termination penalties would not be affected by the provisions of Article 25. We also welcome the last line of the Council's proposed Recital 72(b), which clarifies that fixed-term contracts remain possible. For added clarity, the possibility to set such penalties in contracts should be spelled out through articles 23 and 24, or within a recital. • A mandatory notice period in Articles 23 and 24 would also weaken consent and the reliability of the date of termination in the

Council position	European Parliament position	DIGITALEUROPE comments
		formation of a contract. We recommend that the final text allow for flexibility to agree on the contract's duration (such as with the notice, termination and transition periods) and also reflect the diversity in cloud services.s. • Whilst the concept of 'functional equivalence' remains vague, we welcome the Parliament's proposal that it does not apply to PaaS and SaaS services. • The Council's new concept of 'pre-commercial obstacles,' introduced in recent compromise texts, should be either removed or clarified. Additionally, the notion of 'technical obstacles' may vary based on each customer's needs and the specificities of their migration programmes. Art. 23 should therefore refer to obstacles that significantly impact switching processes and have an element of intent.
Article 23a – Scope of the technical switching obligations		**(3)** A mandatory notice period in Articles 23 and 24 would also weaken consent and the reliability of the date of termination in the formation of a contract. We recommend that the final text allow for flexibility in certain exceptions, to reflect the diversity in cloud services, and the possibility to maintain fixed-term contracts and price benefits for customers.

Council position	European Parliament position	DIGITALEUROPE comments
~~Paragraph 1~~ **The responsibilities of data processing service providers as defined in Articles 23 and 26** shall only apply to ~~obstacles that are related to~~ the services, contractual agreements or commercial practices provided by the original provider.	(1) Paragraph 1 shall only apply to obstacles that are related to the services, contractual agreements or commercial practices provided by the ***source*** provider ***of data processing services***.	
Article 24		
Contractual terms concerning switching between providers of data processing services	*Contractual terms concerning switching between providers of data processing services*	
(1) The rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services **or to an on-premise system** shall be clearly set out in a written contract. Without prejudice to Directive (EU) 2019/770, that contract shall include at least the following: (a) clauses allowing the customer, upon request, to switch to a data processing service offered by another provider of data processing service or to port all data**, including metadata,** applications and **other** digital assets generated directly or indirectly by the customer **and/or relating to the customer** to an on-premise system, in particular the establishment of a mandatory maximum transition period of 30 calendar days, **to be initiated after the maximum notice period referred to in ~~Article 23~~ point (aa),** during which **the service contract remains**	(1) The rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services **or, where applicable, to an on-premise ICT infrastructure** shall be clearly set out in a written contract **which is made available to the customer in a user-friendly manner prior to signing the contract**. Without prejudice to Directive (EU) 2019/770, **the provider of a data processing service** shall **ensure that that contract includes** at least the following: (a) clauses allowing the customer, upon request, to switch to a data processing service offered by another provider of data processing **services** or to port all **exportable** data ▌ applications and digital assets **to an on-premise ICT infrastructure, without undue delay and in any event no longer than** mandatory maximum transition period of **90**	**<u>General remarks</u>**: • The revisions proposed to Art. 24 do not allow sufficient contractual freedom nor a clear balance between the parties. • The proposed ‘exhaustive specification’ of ‘all data and application categories exportable’ may evolve depending on the use of the service. For instance where new applications are used, or if data or metadata is generated in new ways. Ultimately, setting detailed or exhaustive lists at an early stage in the contract might complicate the switching process that follows. It removes flexibility for providers and customers to jointly agree at a later stage on the scope of the data to be ported. • In Art. 24 (1b), we recommend encouraging the possibility of a registry hosted by the data processing service, where practical.

Council position	European Parliament position	DIGITALEUROPE comments
applicable and the data processing service provider shall: 1. assist **the customer and third parties authorised by the customer in** ~~and~~, where technically feasible, ~~complete~~ **completing** the ~~switching~~ **porting** process; 2. ensure full continuity in the provision of the respective functions or services **under the contract;** 3. **ensure that a high level of security is maintained throughout the porting process, notably the security of the data during their transfer and the continued security of the data during the retention period specified in ~~paragraph 1~~ point (c)~~ of this article.~~;** **(aa) a maximum notice period for initiation of the switching process ~~termination of the contract by the user~~, which shall not exceed 2 months;** **(ab) a clause specifying that the contract shall be deemed terminated and the customer shall be notified of the termination, in one of the following cases:** • **upon the successful completion of the switching process to another provider of data processing services or an on-premise system;**	calendar days, during which the **provider of** data processing **services** shall: i **reasonably assist through and facilitate** the switching process; ii **act with due care to maintain business continuity and a high level of security of the service and, taking into account the advancement in the switching process,** ensure**, to the greatest extent possible,** continuity in the provision of the **relevant** functions or services **within the capacity of the source provider of data processing services and in accordance with contractual obligations.** **iia. provide clear information concerning known risks to continuity in the provision of the respective functions or services on the part of the provider of source data processing services.** **(aa) a list of additional services that customers can obtain facilitating the switching process, such as the test of the switching process;** **(ab) an obligation on the provider of data processing services to support the**	**Council**: • Imposing multiple lists for the ‘exhaustive specification’ of data, application categories and metadata on top of a number of other obligations impedes on contractual freedom for all parties, as explained above, and removes flexibility in the commercial relationship between the service provide and the customer. For more legal certainty, we further recommend that Art. 24 refers to ‘exportable data’ rather than ‘metadata,’ ‘data’ or ‘other digital assets,’ which would be extremely broad and would not ensure safeguards to trade secrets. **Parliament**: • The difference in cloud switching and on premise should be recognised. Art. 24(1)(b) fails to recognise that 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 services provided by device manufacturers who have developed infrastructure and diagnostic systems. Transfers of configuration parameters, security settings, access

Council position	European Parliament position	DIGITALEUROPE comments
- **at the end of the maximum notice period referred to in paragraph (aa), in the case that the customer does not wish to switch but to delete all its digital assets upon service termination.** (b) an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service~~, in accordance with point (ba)~~; **(ba) an exhaustive specification of categories of metadata specific to the internal functioning of provider's service that will be exempted from the exportable data under point (b), where a risk of breach of ~~business~~ trade secrets of the provider exists. These exemptions shall however never impede or delay the porting process as foreseen in Article 23;** (c) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the service provider, in	**development of the customer's exit strategy relevant to the contracted services, including through providing all relevant information;** (b) **a detailed** specification of all data and application categories **that can be ported** during the switching process, including, at **a** minimum, all **exportable data;** (c) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the **provider of data processing services**, in accordance with paragraph 1, point (a) and paragraph 2; (ca) **an obligation on the provider of data processing services to delete all of the former customer's exportable data after the expiration of the period set out in paragraph 1, point (c), of this Article;**	rights and access logs amount to conveying detailed information about the service provider's internal processes and know-how.

Council position	European Parliament position	DIGITALEUROPE comments
accordance with paragraph 1, point (a) and paragraph 2~~.~~**;** (d) **a clause guaranteeing full ~~deletion~~ erasure of all data, ~~and~~ including metadata, applications and other digital assets generated directly by the customer and/or relating to ~~created by~~ the customer directly after the expiration of the period set out in ~~paragraph 1~~ point (c) ~~of this Article~~ or after the expiration of an alternative agreed period later than the expiration of the period set out in ~~paragraph 1~~ point (c), provided that the porting process has been completed successfully~~.~~;** (e) **reference to an up-to-date online register hosted by the data processing service provider, with details of all the ~~standards and open interoperability specifications,~~ data structures and data formats as well as the standards and open interoperability specifications, in which the exportable data described according to ~~paragraph (1)~~ point (b~~a~~) will be available~~.~~;** (f) **information on any data egress charges and switching charges that may be imposed by providers of data processing services in accordance with Article 25.**		

Council position	European Parliament position	DIGITALEUROPE comments
(~~2~~1a) The contract as defined in paragraph 1 shall include provisions providing that the customer has the exclusive right to invoke the mandatory notification period as defined in paragraph 1 and shall notify the data processing service provider of its decision to perform one or more of the following actions upon termination of the notification period: **(a) switch to another provider of data processing services, in which case the customer shall provide the necessary details of that provider; (2) switch to an on-premise system; (3) delete its digital assets.**		
(2) **The contract as defined in paragraph 1 shall include provisions providing that w**~~W~~here the mandatory transition period as defined in paragraph 1, points (a) and (c) of this Article is technically unfeasible, the provider of data processing services shall notify the customer within 7 working days after the switching request has been made, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period, which may not exceed 6 months. In accordance with paragraph 1 of this Article, full service continuity shall be ensured throughout the alternative transition period**.** ~~against reduced charges referred to in Article 25(2).~~	(2) Where the mandatory transition period as defined in paragraph 1, points (a) and (c) of this Article is technically unfeasible, the provider of data processing services shall notify the customer within **14** working days after the switching request has been made, **and shall duly motivate** the technical unfeasibility **and indicate** an alternative transition period, which may not exceed **9** months. In accordance with paragraph 1 of this Article, service continuity shall be ensured throughout the alternative transition period against reduced charges, referred to in Article 25(2). **The customer shall retain the right to extend that period, if needed, prior to or during the switching process.**	Parliament's position introduces welcome contractual freedom for both parties to extend the maximum notice period. The maximum notice period of 2 months for the initiation of the switching process, we support the transition period of 90 days to 9 months.

Council position	European Parliament position	DIGITALEUROPE comments
(3) **Without prejudice to paragraph 2, the contract as defined in paragraph 1 shall include provisions providing the customer with the right to extend the transition period with a period that the customer deems more appropriate for its own ends.**		
Article 24a	**Article 24a**	
Contractual transparency obligations on international access and transfer	***Information obligation of providers of destination data processing services***	
(1) **Providers of data processing services shall make the following information available on their websites, and keep the information updated:** (a) **~~information regarding~~ the jurisdiction to which ~~physical location of all~~ the IT infrastructure deployed for data processing of their individual services is subject;** (b) **a general description of the technical, ~~legal and~~ organisational and contractual measures adopted by the data processing service provider in order to prevent governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State.**	**(1) The provider of destination data processing services shall provide the customer with information on available procedures for switching and porting to the data processing service when it is a porting destination, including information on available porting methods and formats as well as restrictions and technical limitations which are known to the provider of destination data processing services.**	

Council position	European Parliament position	DIGITALEUROPE comments
(2) The websites defined in paragraph 1 of this Article shall be referenced in contractual agreements of all data processing services offered by data processing service providers.		
	Article 24b	
	Good faith obligation	
	All parties involved, including providers of destination data processing services, shall collaborate in good faith to make the switching process effective, enable the timely transfer of necessary data and maintain the continuity of the service.	We support the Parliament's proposal to include a 'good faith' obligation for all parties involved, as the exporting data processing service provider does not alone have absolute control over the operation. Instead, effective, secure and timely switching requires full cooperation between the providers of destination services, the exporting service providers and customers. Expertise at both the exporting and importing levels are therefore key.
Article 25		
*Gradual withdrawal of **data egress charges and** switching charges*	*Gradual withdrawal of switching charges*	
(1) From [**date of entry into force** ~~date X~~+3yrs] onwards, providers of data processing services shall not impose any **data egress charges or switching** charges on the customer for the switching process.	**(1)** From [**the date of entry into force of this Regulation**] onwards, providers of data processing services shall not impose any charges on **customers who are consumers** for the switching process	- Cloud service providers presently do not distinguish between types of customers, which would make this provision open to fraud. - We recommend that the timeframe for implementation be extended.
(2) From [~~date X],~~ date of entry into force of the Data Act] until [~~date X~~ **date of entry into force**+3yrs], providers of data processing services may impose	(2) From [date X, the date of entry into force of **this Regulation**] until [date X+3yrs], providers of data processing services may impose reduced	- Once more, the timeframe for implementation would be to short for companies to fully comply.

Council position	European Parliament position	DIGITALEUROPE comments
reduced **data egress and~~/or~~ reduced switching** charges on the customer for the switching process.	charges on **customers in the context of business-to-business relations** for the switching process**, with particular reference to egress fees.**	• At present cloud service providers might not distinguish between customers, reduced charges for some could therefore lead to fraud. It would also be resource intensive and time consuming for both cloud service providers and the responsible authorities to assess and monitor the cost of each use case.
	(2a) From [3 years after the date of entry into force of this Regulation] onwards, providers of data processing services shall not impose any charges for the switching process.	• We recommend that all charges are not disallowed, as it would have a considerable impact on innovation, for instance in support to switching.
(3) The charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the **data transfer and~~/or~~ the** switching process concerned.	**(3)** The charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned **and shall be linked to the mandatory operations that providers of data processing services must perform as part of the switching process.**	
	(3a) **Standard subscription or service fees and charges for professional transition services work undertaken by the provider of data processing services at the customer's request for support in the switching process shall not be considered switching charges for the purposes of this Article.**	
	(3b) Before entering into a contractual agreement with a customer, the provider of data processing services shall provide the	

Council position	European Parliament position	DIGITALEUROPE comments
	customer with clear information describing the charges imposed on the customer for the switching process in accordance with paragraph 2, as well as the fees and charges referred to in paragraph 3a, and, where relevant, shall provide information on services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, application or service architecture. Where applicable, the provider of data processing services shall make this information publicly available to customers via a dedicated section of their website or in any other easily accessible way.	
(4) The Commission is empowered to adopt delegated acts in accordance with Article 38 to supplement this Regulation in order to introduce a monitoring mechanism for the Commission to monitor **data egress charges and** switching charges imposed by data processing service providers on the market to ensure that the withdrawal of ~~switching~~ **these** charges as described in paragraph 1 of this Article will be attained in accordance with the deadline provided in the same paragraph.	(4) The Commission is empowered to adopt delegated acts in accordance with Article 38 to supplement this Regulation in order to introduce a monitoring mechanism for the Commission to monitor switching charges imposed by **providers of** data processing **services** on the market to ensure that the withdrawal **and reduction** of switching charges as described in **paragraphs 1 and 2** of this Article will be attained in accordance with the deadline provided in **those paragraphs.**	
CHAPTER VII		

Council position	European Parliament position	DIGITALEUROPE comments
UNLAWFUL INTERNATIONAL GOVERNMENTAL ACCESS AND TRANSFER OF ~~CONTEXTS~~ NON-PERSONAL DATA ~~SAFEGAURDS~~	INTERNATIONAL CONTEXTS NON-PERSONAL DATA SAFEGUARDS	
Article 27		
*International **governmental** access and transfer*	*International access and transfer*	
(1) Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international ~~transfer or~~ governmental access **and transfer of** ~~to~~ non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.	(1) Providers of data processing services shall take all technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer **and third-country** governmental access to **such** non-personal data held in the Union where such transfer or access would **be in contravention of** Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.	• Whilst Articles 27(2)-(5) stipulate rules applicable only in case of data access requests from third-country authorities, Art. 27(1) introduces a general requirement applicable to data transfers tout court, requiring transfers to be prevented in theoretical scenarios where they could conflict with EU or Member State law. • Whilst we welcome some of the direction of changes made in the Council position, which add the word ‘governmental’ and move the word ‘transfer’ after ‘access,’ we believe that the provision’s intention would be better reflected by simply deleting the word ‘transfer’ throughout Art. 27. In line with those changes, the title of Art. 27 must also delete the mention of ‘transfer.’ Without those changes, there is still a risk of misinterpretation of Art. 27(1) by competent authorities, which could result in blocking international data transfers where there is a belief (whether unfounded or not) that third-country data access might

Council position	European Parliament position	DIGITALEUROPE comments
		happen. Additionally, the Data Act should not regulate data already covered by the GDPR,5 for instance in adequacy findings, standard contractual clauses and corresponding transfer impact assessments, to which companies must already comply with.
Article 42		
This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from [~~12 18~~ **24** months after the date of entry into force of this Regulation]. **The obligation resulting from Article 3(1) shall apply to products and related services placed on the market after [12 months] after the date of application of this Regulation.** **The provisions of Chapter IV shall apply to contracts concluded after [date of application of this Regulation].**	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from ***18*** months after the date of entry into force of this Regulation. ***The obligations resulting from Article 4(1) shall apply to related services placed on the market within five years prior to the entry into force of this Regulation and only where the provider of a related service is able to remotely deploy mechanisms to ensure the fulfilment of the requirements pursuant to Article 4(1) and where the deployment of such mechanisms would not place a disproportionate burden on the manufacturer or provider of related services.***	• We note progress made in Council's position on extending the transition period, although it remains realistically insufficient for compliance. • In the Council's position, we also note the progress made in Art. 42 for the applicability of Art.3(1). We recommend that the same timeline be set to apply to the obligations in articles 4(1) (sharing data with users) and 5(1) (sharing data with authorised 3rd parties). All three provisions are intrinsically connected, as they will require manufacturers and service providers to alter the design of their products and put in place processes for dealing with data requests. • Such changes would also prevent retroactive provisions – applying to products and related services already placed on the market – and help ensure sufficient predictability of current investments.

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 is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, 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