Council of the European Union

Brussels, 21 October 2022
(OR. en)

13342/22

Interinstitutional File:
2022/0047(COD)

LIMITE

TELECOM 399
COMPET 778
MI 727
DATAPROTECT 274
JAI 1287
JUSTCIV 126
PI 131
CODEC 1457

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	12169/22
No. Cion doc.:	6596/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) - Second Presidency compromise text (Chapters I-V)

I. INTRODUCTION

1. The Commission adopted the proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) on 23 February 2022[1].

2. Under the French Presidency, the WP TELECOM discussed the proposal at several meetings, during which the Commission presented in detail the entire text of the proposal, as well as the accompanying impact assessment. In addition to this, the French Presidency organised three workshops with the participation of the Commission and experts from the capitals, based on the questions and requests for clarifications submitted by the delegations in advance in writing.

[1] Doc. 6596/22.

3. On 25 May 2022 the French Presidency requested the Member States to provide their initial drafting suggestions and written comments on the entire text of the proposal by 15 June 2022.

4. Based on the input submitted by the Member States, the Czech Presidency drafted the first compromise text of the Data Act proposal, which were discussed in WP TELECOM on 19 July 2022 and on 5 and 15 September 2022.

5. The Czech Presidency has now drafted the first part of the second compromise text of the Data Act proposal, covering **Chapters I, II, III, IV and V and Article 42, together with the related recitals**, which is included in the Annex to this document.

6. **The Czech Presidency invites the delegations to discuss the changes in the above mentioned chapters and the related recitals, during the WP TELECOM meeting on 27 October 2022.**

7. The changes as compared with the previous document (st12169/22), containing the first two parts the compromise text, are underlined. The changes as compared with Commission's proposal are indicated as follows: additions are marked with **bold**, deletions with ~~strikethrough~~.

II. MAIN CHANGES

1. Chapter I

1.1 In **Article 1(2)**, **point (c)**, the wording has been aligned with points (a), (b) and (e) in relation with the geographical scope of application. Also, a **new point (f)** was added to cover also operators and vendors using smart contracts.

The new text in **Article 1(2a)** aims to clarify that virtual assistants are covered by this Regulation as far as they interact with a product or related service.

Additions in **Article 1(4)** exclude the voluntary agreements between private and public entities from the scope of application, while new **Article 1(4b)** addresses the interplay with Directive 93/13/EEC on Unfair Terms in Consumer Contracts, which was already referred to in **Recital 26**.

1.2 In **Article 2,** 2 new definitions have been added ('readily available data', 'official statistics' and 'Union bodies'), while the definitions of 'product', 'data holder' and 'public emergency' have been updated.

2. Chapter II

2.1 In **Article 3(1)**, the word 'accessible' has been replaced by 'readily available' to designate the data generated by products and related services.

2.2 In **Article 3(2)**, **point (c)** was updated to specify the data holder's obligation to inform the user before the conclusion of a contract also on the matter of data storage and retention policy. Points **(d)** and **(e)** were modified to be consistent with the rest of the paragraph.

2.3 The concept of 'readily available data' was introduced in **Article 4(1)**, together with its definition in **Article 2**. Furthermore, provision on maintaining, where applicable, the same quality of data for the user was added.

2.4 A **new Article 4(1a)** has been added to exclude the possibility to narrow the user's access rights through agreements between the data holder and the user.

2.5 Several changes have been introduced in **Article 4(3)** to better address the protection of the confidentiality of trade secrets. The added text now states that both data holder and user have to take unilaterally all necessary measures prior to sharing of data containing trade secrets to preserve their confidentiality. If those measures are not sufficient, data holder and user need to agree to additional measures of technical or organisational nature. Similar changes to protect trade secrets were added also in **Article 5(8) and Article 19**.

2.6 In **Article 5(1)**, an explicit link between the making available of data to third parties and the conditions and rules for compensation set in **Articles 8 and 9** has been introduced.

2.7 A **new Article 7(3)** explicitly excludes the application of contractual terms possibly in contrast with the user's rights as protected in Chapter II. In the same spirit, **Article 8(2)** in Chapter II was amended.

3. Chapter III

3.1 The scope of dispute settlement in **Article 10(1)** was extended to disputes involving micro, small or medium-sized enterprises in relation to the unfair contractual terms as referred to in **Article 13**.

3.2 Wording in **Article 10(2)** now includes a reference to non-discriminatory rules of procedures in **point (a)** and a link to compensation in **point (b)**.

3.3 **Articles 11(2a) and (3)** have been updated to also consider the interests of users when it comes to the application of point b) of Article 11(2) in situations where the rights of users under the Data Act have been violated.

4. Chapter IV

4.1 The modifications in **Article 13(7)** aim to clarify to which contractual terms the Article does not apply.

5. Chapter V

5.1 The title of **Chapter V** and, respectively, the scope of the chapter were modified to narrow down the Union institutions. In the new version of the text, only the Commission, the European Central Bank and Union bodies and agencies can request data under provisions of Article 14. A definition of Union bodies has been included under **Article 2(21)**. Relevant provisions throughout the chapter and relevant recitals were amended accordingly to the change of scope.

5.2 In **Article 14(1)** 'legal competencies' has been replaced by 'statutory duties', which is less vague and implies that more precise rules are needed to demonstrate an exceptional need.

5.3. **Article 15(c)** was amended to clarify conditions for scenarios where exceptional need is not based or connected to public emergency.

5.3 In **Article 16(1)** and **(2)**, text was added to emphasise that the Data Act does not affect the applicability of national or Union law in the case of requests for data for statistical purposes in non-exceptional situations and to reinforce the scope of the provision by including the right to access, share and use of data.

5.4 In **Article 17,** modifications aim at better clarifying the requirements and procedures for requesting data and the relevant deadlines, as referred to and clarified in **Article 18**.

5.5 **New Article 17(2) point (da)**, in particular, has been added to clarify that requests for personal data in situations other than those connected to a public emergency shall have a specific legal basis in Union or Member State law.

5.6 Wording in **Article 19(2)** has been aligned with that in **Article 14(3)**, with an additional reference to the protection of trade secrets.

5.7 In **Article 22(4), new points (c) and (d)** were introduced and existing provisions in paragraphs 3 and 4 were amended to address the procedures applying in case of cross-border requests by public sector bodies and at the EU level, respectively.

5.8 **Article 42** includes new text to clarify the applicability of different provisions, notably the application of design obligations resulting from Article 3(1) and the provisions of Chapter IV.

6. Recitals

6.1 **Recital 4** now includes text to clarify the scope of applicability of the Data Act with regard to international trade agreements concluded by the Union.

6.2 In **Recital 14**, non-medical wearables were added as one example of physical products covered by the Regulation.

6.3 Part of Recital 14 is now included in **new Recital 14a**, which clarifies what kind of data fall within the scope of the Regulation and also explanations of 'raw data' and 'prepared data' are provided.

6.4 **Recital 15** has been amended to provide a better explanation of which products are covered by or excluded from the scope of the Data Act.

6.5 The text of **Recital 17** was fully moved to new **Recital 14-a** because it introduces concepts that are explained further in **Recital 14a**.

6.6 New text in **Recital 18** explains how a product may be used, and its data generated, by multiple users with different forms of interest, while **Recital 20** addresses the possible separation of accounts (and decoupling of the relevant data) in case of multiple users.

6.7 In **Recital 23**, the obligations of the data holder with regard to the information provided to the user and the retention of data are further clarified. **Recital 24** further refers to situations where the purpose for which the data might be used during the lifetime of a product changes.

6.8 In **Recital 29** a thorough explanation of the role of data intermediation services acting on behalf of the user had been added.

6.9 Consistently with the provisions of the DMA, **Recital 36** clarifies that gatekeepers would not be excluded from the market.

6.10 **Recitals 41 to 46** have been reorganised and amended to reflect and explain previous changes in **Article 9** with regard to 'reasonable compensation'. **New Recital 42a**, in particular, includes text deleted from Recitals 42, 45 and 46 as well as new text concerning the possible

arrangements for reasonable compensations and the relevant costs. Part of **Recital 43** has been transferred to **new Recital 45a**, while the other part comes from old **Recital 46**, which is now deleted.

6.11 The information and provisions to be taken into account by dispute settlement bodies are referred to in a **new Recital 49a**.

6.12 The **new Recital 50a** was added to provide contextual information behind provisions of Article 11.

6.13 Slight amendments in **Recital 56** were included to make it clear that Chapter V covers B2G and not G2G relations.

6.14 New text in **Recital 58** aims to support the changes in Article 15 (c) in relation to the concept of 'other enterprises'.

6.15 **Recitals 61 and 64** help clarify the modifications included in **Article 17(2)** concerning the conditions for the use of personal data requested on the basis of exceptional need.

6.16 New **Recital 68a** complements the changes made in **Chapter V** and specifies in particular the different procedures relevant to cross boarder cases.

6.17 The tasks of competent authorities have been further clarified in **Recital 81**, where also the possible conflict of interest between different competent authorities is referred to, in relation to **Article 18(6)**.

6.18 In addition, clarifications were added in **Recitals 10, 19, 28a38, 55, 57, 59 and 67**.

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on harmonised rules on fair access to and use of data
(Data Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[2],

Having regard to the opinion of the Committee of the Regions[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

[2] OJ C , , p. .
[3] OJ C , , p. .

(1) In recent years, data-driven technologies have had transformative effects on all sectors of the economy. The proliferation in products connected to the Internet of Things in particular has increased the volume and potential value of data for consumers, businesses and society. High quality and interoperable data from different domains increase competitiveness and innovation and ensure sustainable economic growth. The same dataset may potentially be used and reused for a variety of purposes and to an unlimited degree, without any loss in its quality or quantity.

(2) Barriers to data sharing prevent an optimal allocation of data to the benefit of society. These barriers include a lack of incentives for data holders to enter voluntarily into data sharing agreements, uncertainty about rights and obligations in relation to data, costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, bottlenecks impeding data access, a lack of common data sharing practices and abuse of contractual imbalances with regards to data access and use.

(3) In sectors characterised by the presence of micro, small and medium-sized enterprises, there is often a lack of digital capacities and skills to collect, analyse and use data, and access is frequently restricted where one actor holds it in the system or due to a lack of interoperability between data, between data services or across borders.

(4) In order to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data, it is necessary to lay down a harmonised framework specifying who, other than the manufacturer or other data holder is entitled to access the data generated by products or related services, under which conditions and on what basis. Accordingly, Member States should not adopt or maintain additional national requirements on those matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of this Regulation. **Moreover, action at Union level should be without prejudice to obligations and commitments in the international trade agreements concluded by the Union.**

(5) This Regulation ensures that users of a product or related service in the Union can access, in a timely manner, the data generated by the use of that product or related service and that those users can use the data, including by sharing them with third parties of their choice. It imposes the obligation on the data holder to make data available to users and third parties nominated by the users in certain circumstances. It also ensures that data holders make data available to data recipients in the Union under fair, reasonable and non-discriminatory terms and in a transparent manner. Private law rules are key in the overall framework of data sharing. Therefore, this Regulation adapts rules of contract law and prevents the exploitation of contractual imbalances that hinder fair data access and use for micro, small or medium-sized enterprises within the meaning of Recommendation 2003/361/EC. This Regulation also ensures that data holders make available to public sector bodies of the Member States and to Union institutions, agencies or bodies, where there is an exceptional need, the data that are necessary for the performance of tasks carried out in the public interest. In addition, this Regulation seeks to facilitate switching between data processing services and to enhance the interoperability of data and data sharing mechanisms and services in the Union. This Regulation should not be interpreted as recognising or creating any legal basis for the data holder to hold, have access to or process data, or as conferring any new right on the data holder to use data generated by the use of a product or related service. Instead, it takes as its starting point the control that the data holder effectively enjoys, de facto or de jure, over data generated by products or related services.

(6) Data generation is the result of the actions of at least two actors, the designer or manufacturer of a product and the user of that product. It gives rise to questions of fairness in the digital economy, because the data recorded by such products or related services are an important input for aftermarket, ancillary and other services. In order to realise the important economic benefits of data as a non-rival good for the economy and society, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use.

(7) The fundamental right to the protection of personal data is safeguarded in particular under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725. Directive 2002/58/EC additionally protects private life and the confidentiality of communications, including providing conditions to any personal and non-personal data storing in and access from terminal equipment. These instruments provide the basis for sustainable and responsible data processing, including where datasets include a mix of personal and non-personal data. This Regulation complements and is without prejudice to Union law on data protection and privacy, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC. No provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications.

(8) The principles of data minimisation and data protection by design and by default are essential when processing involves significant risks to the fundamental rights of individuals. Taking into account the state of the art, all parties to data sharing, including where within scope of this Regulation, should implement technical and organisational measures to protect these rights. Such measures include not only pseudonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allow valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves.

(9) **In so far as not regulated in this Regulation, this Regulation should not affect national ~~general~~ contract laws such as rules on formation, the validity or effects of contracts, including the consequences of the termination of a contract.** This Regulation complements and is without prejudice to Union law aiming to promote the interests of consumers and to ensure a high level of consumer protection, to protect their health, safety and economic interests, in particular Directive 2005/29/EC of the European Parliament and of the Council[4], Directive 2011/83/EU of the European Parliament and of the Council[5] and Directive 93/13/EEC of the European Parliament and of the Council[6].

(10) This Regulation is without prejudice to Union legal acts providing for the sharing of, the access to and the use of data for the purpose of prevention, investigation, detection or

---

4 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 8 4/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

5 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

6 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

prosecution of criminal offences or the execution of criminal penalties, or for customs and taxation purposes, irrespective of the legal basis under the Treaty on the Functioning of the European Union on which basis they were adopted. Such acts include Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, the [e-evidence proposals [COM(2018) 225 and 226] once adopted], the [Proposal for] a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, as well as international cooperation in this context in particular on the basis of the Council of Europe 2001 Convention on Cybercrime ("Budapest Convention"). This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence and national security in accordance with Union law, and activities from customs on risk management and in general, verification of compliance with the Customs Code by economic operators.

(11) Union law setting physical design and data requirements for products to be placed on the Union market should not be affected by this Regulation.

(12) This Regulation complements and is without prejudice to Union law aiming at setting accessibility requirements on certain products and services, in particular Directive 2019/882[7].

(13) This Regulation is without prejudice to **Union and national legal acts providing for the protection of intellectual property, including 2001/29/EC, 2004/48/EC, and (EU) 2019/790 of the European Parliament and of the Council.**~~the competences of the Member States regarding activities concerning public security, defence and national security in accordance with Union law, and activities from customs on risk management and in general, verification of compliance with the Customs Code by economic operators.~~

(14) Physical products that obtain, generate or collect, by means of their components **or operating system**, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. Electronic communications services include **in particular** land-based telephone networks, television cable networks, satellite-based networks and near-field communication networks. Such products may include vehicles, home equipment and consumer goods, medical ~~and health devices~~ **equipment and wearables** or agricultural and industrial machinery.

(14-a) Data generated by the use of a product or related service include data recorded intentionally by the user. Such data include also data generated as a by-product of the user's action, such as diagnostics data, and without any action by the user, such as when the product is in 'standby mode', and data recorded during periods when the product is switched off. Such data should include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights.

(14a) The data represent the digitalisation of user actions and events and should accordingly be accessible to the user.~~, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation.~~ **In scope are data in raw form (also known as source or primary data, which refers to data points that are**

[7] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility equirements for products and services OJ L 151, 7.6.2019.

automatically generated without any form of processing) as well as prepared data (data cleaned and transformed for the purpose of making it useable prior to further processing and analysis). The term 'prepared data' should be interpreted broadly, without however reaching the stage of deriving or inferring insights. Prepared data may include data enriched with metadata, combined with other data (e.g. sorted and classified with other data points relating to it) or re-formatted into a commonly-used format. Such data are potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, in particular though facilitating the maintenance and repair of the products in question. **By contrast, Iinformation derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation. Such data is not generated by the use of the product, but is the outcome of a characterisation, assessment, recommendation, categorisation or similar systematic processes that assign values or insights to a user or product.**

(15) In contrast, certain products that are primarily designed to display or play content**, such as textual or audiovisual, often covered by intellectual property rights,** or to record and transmit **such** content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, ~~personal computers, servers, tablets and smart phones,~~ **smart televisions and speakers,** cameras, webcams, sound recording systems and text scanners. **Additionally, products primarily designed to process and store data, such as personal computers, servers, tablets and smart phones, should not fall in scope of this Regulation.** ~~They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.~~ **On the other hand, smart watches have a strong element of collection of data on human body indicators or movements and should thus be considered covered by this Regulation as far as they qualify as ~~the definition of~~ "product" in particular due to the ability to communicate data via a publicly available electronic communication service. Given the share of investment in providing data-related functions in relation to other functions of these categories of products, the oligation to allow access or the sharing of data would be disproportionate in the light of the objective of this Regulation.**

(16) It is necessary to lay down rules applying to connected products that **at the time of the purchase, rent or lease agreement** ~~incorporate or~~ are interconnected with a service in such a way that the absence of the service would prevent the product from performing **one of** its functions**, without being incorporated into the product**. Such related services can be part of the sale, rent or lease agreement, or such services are normally provided for products of the same type and the user could reasonably expect them to be provided given the nature of the product and taking into account any public statement made by or on behalf of the seller, renter, lessor or other persons in previous links of the chain of transactions, including the manufacturer. These related services may themselves generate data of value to the user independently of the data collection capabilities of the product with which they are interconnected. This Regulation should also apply to a related service that is not supplied by the seller, renter or lessor itself, but is supplied, under the sales, rental or lease contract, by a third party. In the event of doubt as to whether the supply of service forms part of the sale, rent or lease contract, this Regulation should apply.

~~(17) Data generated by the use of a product or related service include data recorded intentionally by the user. Such data include also data generated as a by-product of the user's action, such as diagnostics data, and without any action by the user, such as when the product is in 'standby mode', and data recorded during periods when the product is switched off. Such data should~~

~~include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights.~~

(18) The user of a product should be understood as the legal or natural person, such as a business or consumer, **but also a public sector body,** which has purchased, rented or leased the product **on other than short-term basis**. Depending on the legal title under which he uses it, such a user bears the risks and enjoys the benefits of using the connected product and should enjoy also the access to the data it generates. The user should therefore be entitled to derive benefit from data generated by that product and any related service. **An owner, renter or lessee should equally be considered as user, including when several entities can be considered as users. In the context of multiple users, each user may contribute in a different manner to the data generation and can have an interest in several forms of use, e.g. fleet management for a leasing company, or mobility solutions for individuals using a car sharing service.**

(19) In practice, not all data generated by products or related services are easily accessible to their users, and there are often limited possibilities for the portability of data generated by products connected to the Internet of Things. Users are unable to obtain data necessary to make use of providers of repair and other services, and businesses are unable to launch innovative, more efficient and convenient services. In many sectors, manufacturers are ~~often~~ able to determine, through their control of the technical design of the product or related services, what data are generated and how they can be accessed, even though they have no legal right to the data. It is therefore necessary to ensure that products are designed and manufactured and related services are provided in such a manner that **the** data **that are** generated by their use **and that are readily available ~~accessible~~ to the manufacturer or a party of his choice,** are always easily accessible **also** to the user**, including users with special needs. This excludes data generated by the use of a product where the design of the product does not foresee such data to be stored or transmitted outside the component in which they are generated or the product as a whole. This Regulation should thus not be understood as an obligation to store data additionally on the central computing unit of a product where this would be disproportionate in relation to the expected use. This should not prevent the manufacturer or data holder to voluntarily agree with the user on making such adaptations.**

(20) In case several persons or entities **are considered as user, e.g. in the case of co-ownership or when an owner and a renter or lessee exist** ~~own a product or are party to a lease or rent agreement and benefit from access to a related service~~, reasonable efforts should be made in the design of the product or related service or the relevant interface so that all persons can have access to data they generate. Users of products that generate data typically require a user account to be set up. This allows for identification of the user by the manufacturer as well as a means to communicate to exercise and process data access requests. Manufacturers or designers of a product that is typically used by several persons should put in place the necessary mechanism that allow separate user accounts for individual persons, where relevant, or the possibility for several persons to use the same user account. **Account solutions should allow a user to delete their account and the data related to it, in particular taking into account situations when the ownership or the usage of the product changes.** Access should be granted to the user upon simple request mechanisms granting automatic execution, not requiring examination or clearance by the manufacturer or data holder. This means that data should only be made available when the user actually wants this. Where automated execution of the data access request is not possible, for instance, via a user account or

accompanying mobile application provided with the product or service, the manufacturer should inform the user how the data may be accessed.

(21) Products may be designed to make certain data directly ~~available~~ **accessible** from an on-device data storage or from a remote server to which the data are communicated. Access to the on-device data storage may be enabled via cable-based or wireless local area networks connected to a publicly available electronic communications service or a mobile network. The server may be the manufacturer's own local server capacity or that of a third party or a cloud service provider who functions as data holder. ~~They~~ **Products** may be designed to permit the user or a third party to process the data on the product**,** ~~or~~ on a computing instance of the manufacturer **or within an IT environment chosen by the user or the third party**.

(22) Virtual assistants play an increasing role in digitising consumer environments and serve as an easy-to-use interface to play content, obtain information, or activate physical objects connected to the Internet of Things. Virtual assistants can act as a single gateway in, for example, a smart home environment and record significant amounts of relevant data on how users interact with products connected to the Internet of Things, including those manufactured by other parties and can replace the use of manufacturer-provided interfaces such as touchscreens or smart phone apps. The user may wish to make available such data with third party manufacturers and enable novel smart home services. Such virtual assistants should be covered by the data access right provided for in this Regulation also regarding data recorded before the virtual assistant's activation by the wake word and data generated when a user interacts with a product via a virtual assistant provided by an entity other than the manufacturer of the product. However, only the data stemming from the interaction between the user and product through the virtual assistant falls within the scope of this Regulation. Data produced by the virtual assistant unrelated to the use of a product is not the object of this Regulation.

(23) Before concluding a contract for the purchase, rent, or lease of a product or the provision of a related service, **the data holder should provide to the user** clear and sufficient information **relevant for the exercise of the user's rights with regard to data generated by the use of the product or related services** ~~should be provided to the user, on how the data generated may be accessed~~. **In case any information changes during the lifetime of the product, including when the purpose for which those data will be used changes from the originally specified purpose, this should also be provided to the user.** ~~to the user on how the data generated may be accessed.~~ This obligation provides transparency over the data generated and enhances the easy access for the user. **The information obligation should be on the data holder, independently whether the data holder concludes the contract for the purchase, rent or lease of a product or the provision of related service. If the data holder is not the seller, rentor or lessor, the data holder should ensure that the user receives the required information, for instance from the seller, rentor or lessor which acts as a messenger. In this regard, the data holder could agree in the contract with the seller, rentor or lessor to provide the information to the user. The transparency obligation could be fulfilled by the data holder for example by, maintaining a stable uniform resource locator (URL) on the web, which can be distributed as a web link or QR code, pointing to the relevant information. Such URL could be provided by the seller, rentor or lessor to the user before concluding the contract for the purchase, rent, or lease of a product or the provision of a related service. It is in any case necessary that the user is enabled to store the information in a way that is accessible for future reference and that allows the unchanged reproduction of the information stored. The data holder cannot be expected to store the data indefinitely in view of the needs of the user of the product, but should**

implement a reasonable data retention policy that allows for the effective application of the data access rights under this Regulation. This obligation to provide information does not affect the obligation for the controller to provide information to the data subject pursuant to Article 12, 13 and 14 of Regulation 2016/679.

(24) This Regulation imposes the obligation on data holders to make data available in certain circumstances. **The notion of data holder generally does not include public sector bodies. However, it may include public undertakings.** Insofar as personal data are processed, the data holder should be a controller under Regulation (EU) 2016/679. Where users are data subjects, data holders should be obliged to provide them access to their data and to make the data available to third parties of the user's choice in accordance with this Regulation. However, this Regulation does not create a legal basis under Regulation (EU) 2016/679 for the data holder to provide access to personal data or make it available to a third party when requested by a user that is not a data subject and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies in particular where the manufacturer is the data holder. In that case, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user. This agreement may be part of the sale, rent or lease agreement relating to the product. Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which the data holder intends to use the data. **Any change of the contract should depend on the informed agreement of the user.** This Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder. This Regulation should also not prevent sector-specific regulatory requirements under Union law, or national law compatible with Union law, which would exclude or limit the use of certain such data by the data holder on well-defined public policy grounds.

(25) In sectors characterised by the concentration of a small number of manufacturers supplying end users, there are only limited options available to users with regard to sharing data with those manufacturers. In such circumstances, contractual agreements may be insufficient to achieve the objective of user empowerment. The data tends to remain under the control of the manufacturers, making it difficult for users to obtain value from the data generated by the equipment they purchase or lease. Consequently, there is limited potential for innovative smaller businesses to offer data-based solutions in a competitive manner and for a diverse data economy in Europe. This Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement. Sectoral legislation may be brought forward to address sector-specific needs and objectives. Furthermore, the data holder should not use any data generated by the use of the product or related service in order to derive insights about the economic situation of the user or its assets or production methods or the use in any other way that could undermine the commercial position of the user on the markets it is active on. This would, for instance, involve using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on potential acquisition of the user's products or agricultural produce to the user's detriment, or for instance, using such information to feed in larger databases on certain markets in the aggregate (e.g. databases on crop yields for the upcoming harvesting season) as such use could affect the user negatively in an indirect manner. The user should be given the necessary technical interface to manage permissions, preferably with granular permission options (such as "allow once" or "allow while using this app or service"), including the option to withdraw permission.

(26) In contracts between a data holder and a consumer as a user of a product or related service generating data, Directive 93/13/EEC applies to the terms of the contract to ensure that a consumer is not subject to unfair contractual terms. For unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC[8], this Regulation provides that such unfair terms should not be binding on that enterprise.

(27) The data holder may require appropriate user identification to verify the user's entitlement to access the data. In the case of personal data processed by a processor on behalf of the controller, the data holder should ensure that the access request is received and handled by the processor.

(28) The user should be free to use the data for any lawful purpose. This includes providing the data the user has received exercising the right under this Regulation**,** to a third party offering an aftermarket service that may be in competition with a service provided by the data holder, or to instruct the data holder to do so. The data holder should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date as the data the data holder itself may be able or entitled to access from the use of the product or related service. Any ~~trade secrets or~~ intellectual property rights should be respected in handling the data. It is important to preserve incentives to invest in products with functionalities based on the use of data from sensors built into that product.

(28a) As regards the protection of trade secrets, this Regulation should be interpreted in a manner to preserve the protection awarded to trade secrets under Directive (EU) 2016/943. For this reason, data holders can require the user or third parties of the user's choice to preserve the secrecy of data considered as trade secrets, including through technical means. Also, the data holders can require that the confidentiality of a disclosure must be ensured by the user and any third party of the user's choice. Data holders, however, cannot refuse a data access request under this Regulation on the basis of certain data considered as trade secrets, as this would undo the intended effects of this Regulation. The aim of this Regulation should accordingly be understood as to foster the development of new, innovative products or related services, stimulate innovation on aftermarkets, but also stimulate the development of entirely novel services making use of the data, including based on data from a variety of products or related services. At the same time, it aims to avoid undermining the investment incentives for the type of product from which the data are obtained, for instance, by the use of data to develop a competing product. **This Regulation provides for no prohibition to develop a related service as this would have a chilling effect on innovation.**

(29) A third party to whom data is made available may be an enterprise, a research organisation ~~or~~ a not-for-profit organisation **or an entity acting in a professional capacity**. In making the data available to the third party, the data holder should not abuse its position to seek a competitive advantage in markets where the data holder and third party may be in direct competition. The data holder should not therefore use any data generated by the use of the product or related service in order to derive insights about the economic situation of the third party or its assets or production methods or the use in any other way that could undermine the commercial position of the third party on the markets it is active on. **Data intermediation services [as regulated by Regulation (EU) 2022/868] may support users or third parties in establishing a commercial relation for any lawful purpose on the basis of data of**

[8] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

products in scope of this Regulation e.g. by acting on behalf of a user. They could play an instrumental role in aggregating access to data from a large number of individual users so that big data analyses or machine learning can be facilitated, as long as such users remain in full control on whether to contribute their data to such aggregation and the commercial terms under which their data will be used.

(30) The use of a product or related service may, in particular when the user is a natural person, generate data that relates to an identified or identifiable natural person (the data subject). Processing of such data is subject to the rules established under Regulation (EU) 2016/679, including where personal and non-personal data in a data set are inextricably linked[9]. The data subject may be the user or another natural person. Personal data may only be requested by a controller or a data subject. A user who is the data subject is under certain circumstances entitled under Regulation (EU) 2016/679 to access personal data concerning them, and such rights are unaffected by this Regulation. Under this Regulation, the user who is a natural person is further entitled to access all data generated by the product, personal and non-personal. Where the user is not the data subject but an enterprise, including a sole trader, and not in cases of shared household use of the product, the user will be a controller within the meaning of Regulation (EU) 2016/679. Accordingly, such a user as controller intending to request personal data generated by the use of a product or related service is required to have a legal basis for processing the data under Article 6(1) of Regulation (EU) 2016/679, such as the consent of the data subject or legitimate interest. This user should ensure that the data subject is appropriately informed of the specified, explicit and legitimate purposes for processing those data, and how the data subject may effectively exercise their rights. Where the data holder and the user are joint controllers within the meaning of Article 26 of Regulation (EU) 2016/679, they are required to determine, in a transparent manner by means of an arrangement between them, their respective responsibilities for compliance with that Regulation. It should be understood that such a user, once data has been made available, may in turn become a data holder, if they meet the criteria under this Regulation and thus become subject to the obligations to make data available under this Regulation.

(31) Data generated by the use of a product or related service should only be made available to a third party at the request of the user. This Regulation accordingly complements the right provided under Article 20 of Regulation (EU) 2016/679. That Article provides for a right of data subjects to receive personal data concerning them in a structured, commonly used and machine-readable format, and to port those data to other controllers, where those data are processed **by automated means** on the basis of Article 6(1), point (a), or Article 9(2), point (a), or of a contract pursuant to Article 6(1), point (b). Data subjects also have the right to have the personal data transmitted directly from one controller to another, but only where technically feasible. Article 20 specifies that it pertains to data provided by the data subject but does not specify whether this necessitates active behaviour on the side of the data subject or whether it also applies to situations where a product or related service by its design observes the behaviour of a data subject or other information in relation to a data subject in a passive manner. The right under this Regulation complements the right to receive and port personal data under Article 20 of Regulation (EU) 2016/679 in several ways. It grants users the right to access and make available to a third party to any data generated by the use of a product or related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike ~~the technical obligations provided for in~~ Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of

[9] OJ L 303, 28.11.2018, p. 59–68.

data coming within its scope, whether personal or non-personal, **thereby making sure that technical obstacles no longer hinder or prevent access to such data**. It also allows the data holder to set reasonable compensation to be met by third parties, but not by the user, for any cost incurred in providing direct access to the data generated by the user's product. If a data holder and third party are unable to agree terms for such direct access, the data subject should be in no way prevented from exercising the rights contained in Regulation (EU) 2016/679, including the right to data portability, by seeking remedies in accordance with that Regulation. It is to be understood in this context that, in accordance with Regulation (EU) 2016/679, a contractual agreement does not allow for the processing of special categories of personal data by the data holder or the third party.

(32) Access to any data stored in and accessed from terminal equipment is subject to Directive 2002/58/EC and requires the consent of the subscriber or user within the meaning of that Directive unless it is strictly necessary for the provision of an information society service explicitly requested by the user or subscriber (or for the sole purpose of the transmission of a communication). Directive 2002/58/EC ('ePrivacy Directive') ~~(and the proposed ePrivacy Regulation)~~ protect the integrity of the user's terminal equipment as regards the use of processing and storage capabilities and the collection of information. Internet of Things equipment is considered terminal equipment if it is directly or indirectly connected to a public communications network.

(33) In order to prevent the exploitation of users, third parties to whom data has been made available upon request of the user should only process the data for the purposes agreed with the user and share it with another third party only if this is necessary to provide the service requested by the user.

(34) In line with the data minimisation principle, the third party should only access additional information that is necessary for the provision of the service requested by the user. Having received access to data, the third party should process it exclusively for the purposes agreed with the user, without interference from the data holder. It should be as easy for the user to refuse or discontinue access by the third party to the data as it is for the user to authorise access. The third party should not coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user. in this context, third parties should not rely on so-called dark patterns in designing their digital interfaces. Dark patterns are design techniques that push or deceive consumers into decisions that have negative consequences for them. These manipulative techniques can be used to persuade users, particularly vulnerable consumers, to engage in unwanted behaviours, and to deceive users by nudging them into decisions on data disclosure transactions or to unreasonably bias the decision-making of the users of the service, in a way that subverts and impairs their autonomy, decision-making and choice. Common and legitimate commercial practices that are in compliance with Union law should not in themselves be regarded as constituting dark patterns. Third parties should comply with their obligations under relevant Union law, in particular the requirements set out in Directive 2005/29/EC, Directive 2011/83/EU, Directive 2000/31/EC and Directive 98/6/EC.

(35) The third party should also refrain from using the data to profile individuals unless these processing activities are strictly necessary to provide the service requested by the user. The requirement to delete data when no longer required for the purpose agreed with the user complements the right to erasure of the data subject pursuant to Article 17 of Regulation 2016/679. Where the third party is a provider of a data intermediation service within the meaning of [Data Governance Act], the safeguards for the data subject provided for by that

Regulation apply. The third party may use the data to develop a new and innovative product or related service but not to develop a competing product.

(36) Start-ups, small and medium-sized enterprises and companies from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This Regulation aims to facilitate access to data for these entities, while ensuring that the corresponding obligations are scoped as proportionately as possible to avoid overreach. At the same time, a small number of very large companies have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. These companies include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and whom existing or new market operators are unable to challenge or contest. ~~The [~~Regulation **(EU) 2022/1925** on contestable and fair markets in the digital sector (Digital Markets Act)~~]~~[10] aims to redress these inefficiencies and imbalances by allowing the Commission to designate a provider as a "gatekeeper", and imposes a number of obligations on such designated gatekeepers, including a prohibition to combine certain data without consent, and an obligation to ensure effective rights to data portability under Article 20 of Regulation (EU) 2016/679. Consistent with ~~the [~~Regulation **(EU) 2022/1925** ~~on contestable and fair markets in the digital sector (Digital Markets Act)]~~, and given the unrivalled ability of these companies to acquire data, it would not be necessary to achieve the objective of this Regulation, and would thus be disproportionate in relation to data holders made subject to such obligations, to include such gatekeeper undertakings as beneficiaries of the data access right. **Such inclusion would also likely limit the benefits of the Data Act for the SMEs, linked to the fairness of the distribution of data value across market actors.** This means that an undertaking providing core platform services that has been designated as a gatekeeper cannot request or be granted access to users' data generated by the use of a product or related service or by a virtual assistant based on the provisions of Chapter II of this Regulation. ~~An undertaking providing core platform services designated as a gatekeeper pursuant to Digital Markets Act should be understood to include all legal entities of a group of companies where one legal entity provides a core platform service.~~ Furthermore, third parties to whom data are made available at the request of the user may not make the data available to a designated gatekeeper. For instance, the third party may not sub-contract the service provision to a gatekeeper. However, this does not prevent third parties from using data processing services offered by a designated gatekeeper. The~~is~~ exclusion of designated gatekeepers from the scope of the access right under this Regulation **means that they cannot receive data from the users and from third parties. It** ~~does~~ **should** not prevent these companies from obtaining **and using the same** data through other lawful means. **Notably, i~~t~~t should continue to be possible for manufacturers to contractually agree with gatekeepers that data from products they manufacture can be used by a gatekeeper company** ~~service~~. ~~, including when desired by a user of such products~~**. The access rights under Chapter II of the Data Act contribute to a wider choice of services for consumers. The limitation on granting access to gatekeepers would not exclude them from the market and prevent them from offering its services, as voluntary agreements between them and the data holders remain unaffected.**

(37) Given the current state of technology, it is overly burdensome to impose further design obligations in relation to products manufactured or designed and related services provided by micro and small enterprises. That is not the case, however, where a micro or small enterprise is sub-contracted to manufacture or design a product. In such situations, the enterprise, which

---

10 OJ L 265, 12.10.2022, p. 1–66.

has sub-contracted to the micro or small enterprise, is able to compensate the sub-contractor appropriately. A micro or small enterprise may nevertheless be subject to the requirements laid down by this Regulation as data holder, where it is not the manufacturer of the product or a provider of related services. **Similarly, enterprises that just have passed the thresholds qualifying as a medium-sized enterprise as well as medium-sized enterprises bringing a new product on the market should benefit from a certain period before being exposed to the potential competition based on the access rights under this Regulation on the market for services around products they manufacture.**

(38) **In order to take account of a variety of products in scope, producing data of different nature, volume and ~~speed~~ frequency, presenting different levels of data and cybersecurity risks, and providing economic opportunities of different value, t~~T~~his** Regulation **assumes that the data holder and the third party conclude a contractual agreement on the modalities under which the right to share data with third parties is to be fulfilled. Those modalities should be fair, reasonable, non-discriminatory and transparent. The non-binding model contractual terms for business-to-business data sharing to be developed and recommended by the Commission may help the parties to conclude a contractual agreement including fair, reasonable and non-discriminatory terms and implemented in a transparent way. The conclusion of such an agreement should, however, not mean that the right to share data with third parties is in any way conditional upon the existence of such agreement. Should parties be unable to conclude an agreement on the modalities, including with the support of dispute settlement bodies, the right to share data with third parties is enforceable in national courts.**

(38a) For the purpose of ensuring consistency of data sharing practices in the internal market, including across sectors, and to encourage and promote fair data sharing practices even in areas where no such right to data access is provided, this Regulation provides for horizontal rules **on modalities of access to data**~~,~~ whenever a data holder is obliged by law to make data available to a data recipient. **This should apply in addition to the rules that lay down the rights of access to data generated by products or related services** ~~Such access should be based on fair, reasonable, non-discriminatory and transparent conditions to ensure consistency of data sharing practices in the internal market, including across sectors, and to encourage and promote fair data sharing practices even in areas where no such right to data access is provided.~~ These general access rules do not apply to obligations to make data available under Regulation (EU) 2016/679. Voluntary data sharing remains unaffected by these rules.

(39) Based on the principle of contractual freedom, the parties should remain free to negotiate the precise conditions for making data available in their contracts, within the framework of the general access rules for making data available. **Such terms could include technical and organisational issues, including in relation to data security.**

(40) In order to ensure that the conditions for mandatory data access are fair for both parties, the general rules on data access rights should refer to the rule on avoiding unfair contract terms.

(41) **Any agreement concluded in business-to-business relations for making the data available should also be non-discriminatory between comparable categories of data recipients, independently whether they are large companies or micro, small or medium-sized enterprises.** In order to compensate for the lack of information on the conditions of different contracts, which makes it difficult for the data recipient to assess if the terms for making the data available are non-discriminatory, it should be on the data holder to demonstrate that a contractual term is not discriminatory. It is not unlawful discrimination,

where a data holder uses different contractual terms for making data available or different compensation, if those differences are justified by objective reasons. These obligations are without prejudice to Regulation (EU) 2016/679.

(42) In order to incentivise the continued investment in generating valuable data, including investments in relevant technical tools, **while at the same time avoiding excessive burden for access and use of data which make data sharing no longer commercially viable,** this Regulation contains the principle that the data holder may request reasonable compensation when legally obliged to make data available to the data recipient. ~~These provisions should not be understood as paying for the data itself, but in the case of micro, small or medium-sized enterprises, for the costs incurred and investment required for making the data available.~~

(42a) Such reasonable compensation may include firstly the costs incurred and investment required for making the data available. These costs can be technical costs, such as the costs necessary for data reproduction, dissemination via electronic means and storage, but not of data collection or production. Such technical costs could include also the costs for processing, necessary to make data available. Costs related to making the data available may also include the costs of organising answers to concrete data sharing requests. They may also vary depending on the arrangements taken for making the data available. Long-term arrangements between data holders and data recipients, for instance via a subscription model or the use of smart contracts, could reduce the costs in regular or repetitive transactions in a business relationship. Costs related to making data available are either specific to a particular request or shared with other requests. In the latter case, a single data recipient should not pay the full costs of making the data available. Reasonable compensation may include secondly a margin. Such margin may vary depending on factors related to the data itself, such as volume, format or nature of the data, or on the supply of and demand for the data. It may consider the costs for collecting the data. The margin may therefore decrease where the data holder has collected the data for its own business without significant investments or may increase where the investments in the data collection for the purposes of the data holder's business are high. The margin may also depend on the follow-on use of the data by the data recipient. It may be limited or even excluded in situations where the use of the data by the data recipient does not affect the own activities of the data holder. The fact that the data is co-generated by the user could also lower the amount of the compensation in comparison to other situations where the data are generated exclusively by the data holder.

(43) ~~In justified cases, including the need to safeguard consumer participation and competition or to promote innovation in certain markets, Union law or national legislation implementing Union law may impose regulated compensation for making available specific data types.~~ **It is not necessary to intervene in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company. In such cases, the companies are considered capable of negotiating the compensation within the limits of what is reasonable.**

(44) To protect micro, small or medium-sized enterprises from excessive economic burdens which would make it commercially too difficult for them to develop and run innovative business models, the **reasonable** compensation for making data available to be paid by them should not exceed the ~~direct~~ cost **directly related to** ~~of~~ making the data available ~~and be non-discriminatory~~.

~~(45)~~ Direct**ly related** costs ~~for making data available~~ are ~~the~~ **those** costs ~~necessary for data reproduction, dissemination via electronic means and storage but not of data collection or production. Direct costs for making data available should be limited to the share~~ **which are** attributable to the individual requests, taking into account that the necessary technical interfaces or related software and connectivity will have to be set up permanently by the data holder. ~~Long-term arrangements between data holders and data recipients, for instance via a subscription model, could reduce the costs linked to making the data available in regular or repetitive transactions in a business relationship.~~

(45a) In justified cases, including the need to safeguard consumer participation and competition or to promote innovation in certain markets, Union law or national legislation implementing Union law may impose regulated compensation for making available specific data types.

~~(46) It is not necessary to intervene in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company. In such cases, the companies are considered capable of negotiating any compensation if it is reasonable, taking into account factors such as the volume, format, nature, or supply of and demand for the data as well as the costs for collecting and making the data available to the data recipient.~~

(47) Transparency is an important principle to ensure that the compensation requested by the data holder is reasonable, or, in case the data recipient is a micro, small or medium-sized enterprise, that the compensation does not exceed the costs directly related to making the data available to the data recipient ~~and is attributable to the individual request~~. In order to put the data recipient in the position to assess and verify that the compensation complies with the requirements under this Regulation, the data holder should provide to the data recipient the information for the calculation of the compensation with a sufficient degree of detail.

(48) Ensuring access to alternative ways of resolving domestic and cross-border disputes that arise in connection with making data available should benefit data holders and data recipients and therefore strengthen trust in data sharing. In cases where parties cannot agree on fair, reasonable and non-discriminatory terms of making data available, dispute settlement bodies should offer a simple, fast and low-cost solution to the parties. **While this Regulation only lays down the conditions that dispute settlement bodies need to fulfill to be certified, Member States are free to regulate any specific rules on the certification procedure, including the expiration or revocation of the certification.**

(48a) The dispute settlement procedure under this Regulation is a voluntary procedure that enables both data holder and data recipient to agree on bringing their dispute before a dispute settlement body. In this regard, the parties should be free to address a dispute settlement body of their choice, be it within or outside of the Member States they are established in.

(49) To avoid that two or more dispute settlement bodies are seized for the same dispute, particularly in a cross-border setting, a dispute settlement body should be able to reject a request to resolve a dispute that has already been brought before another dispute settlement body or before a court or a tribunal of a Member State.

(49a) In order to ensure an uniform application of this Regulation, the dispute settlement bodies should take into account~~, as appropriate,~~ the non-binding model contractual terms developed and recommended by the Commission as well as sectoral regulation

specifying data sharing obligations or guidelines issued by sectoral authorities for the application of such Regulation.

(50) Parties to dispute settlement proceedings should not be prevented from exercising their fundamental rights to an effective remedy and to a fair trial. Therefore, the decision to submit a dispute to a dispute settlement body should not deprive those parties of their right to seek redress before a court or a tribunal of a Member State.

(50a) In order to avoid misuse of the new data access rights, the data holder may apply protective measures in relation to the data made available to the recipient to prevent unauthorised access and ensure compliance with the framework of data access in Chapter II and III. However, those technical measures should not hinder the effective access and use of data for the data recipient. In the case of abusive practices such as misleading the data holder with inaccurate information or developing a competing product on the basis of data, the data holder can, for example, request the deletion of data and the end of production of products or services based on the data received.

(51) Where one party is in a stronger bargaining position, there is a risk that that party could leverage such position to the detriment of the other contracting party when negotiating access to data and make access to data commercially less viable and sometimes economically prohibitive. Such contractual imbalances particularly harm micro, small and medium-sized enterprises without a meaningful ability to negotiate the conditions for access to data, who may have no other choice than to accept 'take-it-or-leave-it' contractual terms. Therefore, unfair contract terms regulating the access to and use of data or the liability and remedies for the breach or the termination of data related obligations should not be binding on micro, small or medium-sized enterprises when they have been unilaterally imposed on them. **The relevant moment to determine whether an enterprise is micro, small or medium-sized is the moment of conclusion of the contract.**

(52) Rules on contractual terms should take into account the principle of contractual freedom as an essential concept in business-to-business relationships. Therefore, not all contractual terms should be subject to an unfairness test, but only to those terms that are unilaterally imposed on micro, small and medium-sized enterprises. This concerns 'take-it-or-leave-it' situations where one party supplies a certain contractual term and the micro, small or medium-sized enterprise cannot influence the content of that term despite an attempt to negotiate it. A contractual term that is simply provided by one party and accepted by the micro, small or medium-sized enterprise or a term that is negotiated and subsequently agreed in an amended way between contracting parties should not be considered as unilaterally imposed.

(53) Furthermore, the rules on unfair contractual terms should only apply to those elements of a contract that are related to making data available, that is contractual terms concerning the access to and use of data as well as liability or remedies for breach and termination of data related obligations. Other parts of the same contract, unrelated to making data available, should not be subject to the unfairness test laid down in this Regulation.

(54) Criteria to identify unfair contractual terms should be applied only to excessive contractual terms, where a stronger bargaining position is abused. The vast majority of contractual terms that are commercially more favourable to one party than to the other, including those that are normal in business-to-business contracts, are a normal expression of the principle of contractual freedom and shall continue to apply.

(55) **In order to ensure legal certainty, this Regulation establishes a list with clauses that are always considered unfair and a list with clauses that are presumed unfair. In the latter case, the enterprise that imposed the contract term can rebut the presumption by demonstrating that the contractual term listed is not unfair in the specific case at hand.** If a contractual term is not included in the list of terms that are always considered unfair or that are presumed to be unfair, the general unfairness provision applies. In this regard, the terms listed as unfair terms should serve as a yardstick to interpret the general unfairness provision. Finally, model contractual terms for business-to-business data sharing contracts to be developed and recommended by the Commission may also be helpful to commercial parties when negotiating contracts. **If a clause is declared as being unfair, the contract should continue to apply without that clause, unless the unfair clause is not severable from the other terms of the contract.**

(56) In situations of exceptional need, it may be necessary for public sector bodies or Union institutions, agencies or bodies **in the performance of their statutory duties in the public interest** to use data held by an enterprise **as a data holder** to respond to public emergencies or in other exceptional cases. **The notion of data holder generally does not include public sector bodies. However, it may include public undertakings. Exceptional needs are circumstances which are unforeseeable and limited in time, in contrast to other circumstances which might be planned, scheduled, periodic or frequent.** Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law. To limit the burden on businesses, micro and small enterprises should be exempted from the obligation to provide public sector bodies and Union institutions, agencies or bodies data in situations of exceptional need.

(57) In case of public emergencies, such as public health emergencies, emergencies resulting from ~~environmental degradation and~~ major natural disasters including those aggravated by climate change **and environmental degradation**, as well as human-induced major disasters, such as major cybersecurity incidents, the public interest resulting from the use of the data will outweigh the interests of the data holders to dispose freely of the data they hold. In such a case, data holders should be placed under an obligation to make the data available to public sector bodies or to Union institutions, agencies or bodies upon their request. The existence of a public emergency ~~is~~ **should be** determined **and declared** according to the respective procedures in the Member States or of relevant international organisations.

(58) An exceptional need may also arise when a public sector body can demonstrate that the data are necessary either to prevent a public emergency, or to assist recovery from a public emergency, in circumstances that are reasonably proximate to the public emergency in question. Where the exceptional need is not justified by the need to respond to, prevent or assist recovery from a public emergency, the public sector body or the Union institution, agency or body should demonstrate that the lack of timely access to and the use of the data requested prevents it from effectively fulfilling a specific task in the public interest that has been explicitly provided in law. **The specific task should be within the competence of the public sector body or Union institution, agency or body requesting the data, and explicitly laid down in their mandate. Such tasks could be, inter alia, related to local transport or city planning, improving infrastructural services (such as energy, waste and water management), or producing reliable and up to date statistics. The conditions and principles for requests established in Article 17 (such as purpose limitation, proportionality, transparency, time limitation) should also apply to these requests.** ~~Such~~ **An** exceptional need may also occur in other situations, for example in relation to the timely compilation of official statistics when data is not otherwise available or when the burden on

statistical respondents will be considerably reduced. **This also includes a reduced burden on other companies that provide the necessary data to the statistical respondent, for example in the case of obtaining data from data-aggregating platforms, which would make requests to multiple companies superfluous.** At the same time, the public sector body or the Union institution, agency or body should, outside the case of responding to, preventing or assisting recovery from a public emergency, demonstrate that ~~no alternative means for obtaining the data requested exists~~ **it has exhausted all the means of obtaining the data at its disposal** and that the data cannot be obtained in a timely manner through the laying down of the necessary data provision obligations in new legislation.

(59) This Regulation should not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities. Obligations placed on data holders to provide data that are motivated by needs of a non-exceptional nature, notably where the range of data and of data holders is known**, including in cases of complying with the targeted information requests under the single market emergency instrument (SMEI)** ~~and~~ **or** where data use can take place on a regular basis, as in the case of reporting obligations and internal market obligations, should not be affected by this Regulation. Requirements to access data to verify compliance with applicable rules, including in cases where public sector bodies assign the task of the verification of compliance to entities other than public sector bodies, should also not be affected by this Regulation.

(59a) This Regulation complements and is without prejudice to the Union and national laws providing for the access to and enabling to use data for statistical purposes, in particular Regulation (EC) No 223/2009 on European statistics and its related legal acts as well as national legal acts related to official statistics.

(60) For the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal and administrative offences, the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes, public sector bodies and Union institutions, agencies and bodies should rely on their powers under sectoral legislation. This Regulation accordingly does not affect instruments for the sharing, access and use of data in those areas. **This Regulation should not apply to situations concerning national security or defence.**

(61) **In accordance with Article 6(1)(e) and 6(3) of Regulation (EU) 2016/679,** ~~A~~**a** proportionate, limited and predictable framework at Union level is necessary **when providing for the legal basis** for the making available of data by data holders, in cases of exceptional needs, to public sector bodies and to Union institution, agencies or bodies ~~both to ensure legal certainty and to minimise the administrative burdens placed on businesses~~. To this end, data requests by public sector bodies and by Union institution, agencies and bodies to data holders should be transparent and proportionate in terms of their scope of content and their granularity. The purpose of the request and the intended use of the data requested should be specific and clearly explained, while allowing appropriate flexibility for the requesting entity to perform its tasks in the public interest. **The principle of purpose limitation and other principles of data protection law should also apply to situations where the public sector body or EU institution, agency or body shares the data received under this Chapter with third parties to whom they have outsourced any function.** The request should also respect the legitimate interests of the businesses to whom the request is made. The burden on data holders should be minimised by obliging requesting entities to respect the once-only principle, which prevents the same data from being requested more than once by more than one public sector body or Union institution, agency or body where those data are needed to respond to a public emergency. To ensure transparency, data requests made by public sector bodies and by Union

institutions, agencies or bodies should be made public without undue delay by the entity requesting the data**, which should also notify the competent authority of the Member State where the public sector body is established or the Commission, if the request is made by the Commission, the European Central Bank or Union bodies.** ~~and~~ **O**~~o~~nline public availability of all requests justified by a public emergency should be ensured.

(62) The objective of the obligation to provide the data is to ensure that public sector bodies and Union institutions, agencies or bodies have the necessary knowledge to respond to, prevent or recover from public emergencies or to maintain the capacity to fulfil specific tasks explicitly provided by law. The data obtained by those entities may be commercially sensitive. Therefore, Directive (EU) 2019/1024 of the European Parliament and of the Council[11] should not apply to data made available under this Regulation and should not be considered as open data available for reuse by third parties. This however should not affect the applicability of Directive (EU) 2019/1024 to the reuse of official statistics for the production of which data obtained pursuant to this Regulation was used, provided the reuse does not include the underlying data. In addition, it should not affect the possibility of sharing the data for conducting research or for the compilation of official statistics, provided the conditions laid down in this Regulation are met. Public sector bodies should also be allowed to exchange data obtained pursuant to this Regulation with other public sector bodies to address the exceptional needs for which the data has been requested.

(63) Data holders should have the possibility to either ask for a modification of the request made by a public sector body or Union institution, agency and body or its cancellation in a period of 5 or 15 working days depending on the nature of the exceptional need invoked in the request. In case of requests motivated by a public emergency, justified reason not to make the data available should exist if it can be shown that the request is similar or identical to a previously submitted request for the same purpose by another public sector body or by another Union institution, agency or body. A data holder rejecting the request or seeking its modification should communicate the underlying justification for refusing the request to the public sector body or to the Union institution, agency or body requesting the data. In case the *sui generis* database rights under Directive 96/6/EC of the European Parliament and of the Council[12] apply in relation to the requested datasets, data holders should exercise their rights in a way that does not prevent the public sector body and Union institutions, agencies or bodies from obtaining the data, or from sharing it, in accordance with this Regulation.

(64) **In case of exceptional need related to public emergency, P**~~p~~**public sector bodies should use non-personal data, including anonymised data, wherever possible. In cases of requests based on an exceptional need not related to public emergency, personal data can be used only if a legal basis for its processing exists in Union or Member State law. Whenever personal data is requested, T**~~t~~**he data holder should anonymise the data and can request compensation for that, pursuant to the rules on the compensation in cases of exceptional need.** Where it is strictly necessary to include personal data in the data **to be** made available to a public sector body or to a Union institution, agency or body **or where anonymisation proves impossible, the body requesting the data should demonstrate the strict necessity and the specific and limited purposes for processing. T**~~t~~he applicable rules on personal data protection should be complied with**. The data holder should apply technological means such as pseudonymisation and aggregation, prior to making the data available, for which**

---

11 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ L 172, 26.6.2019, p. 56).

12 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ L 77, 27.3.1996, p.. 20).

compensation can also be requested. ~~and t~~**T**he making available of the data and their subsequent use should ~~and~~ be accompanied by safeguards for the rights and interests of individuals concerned by those data. ~~The body requesting the data should demonstrate the strict necessity and the specific and limited purposes for processing. The data holder should take reasonable efforts to anonymise the data or, where such anonymisation proves impossible, the data holder should apply technological means such as pseudonymisation and aggregation, prior to making the data available.~~

(65) Data made available to public sector bodies and to Union institutions, agencies and bodies on the basis of exceptional need should only be used for the purpose for which they were requested, unless the data holder that made the data available has expressly agreed for the data to be used for other purposes. The data should be ~~destroyed~~ **erased** once it is no longer necessary for the purpose stated in the request, unless agreed otherwise, and the data holder should be informed thereof.

(66) When reusing data provided by data holders, public sector bodies and Union institutions, agencies or bodies should respect both existing applicable legislation and contractual obligations to which the data holder is subject. Where the disclosure of trade secrets of the data holder to public sector bodies or to Union institutions, agencies or bodies is strictly necessary to fulfil the purpose for which the data has been requested, confidentiality of such disclosure should be ensured to the data holder.

(67) When the safeguarding of a significant public good is at stake, such as is the case of responding to public emergencies, the public sector body or the Union institution, agency or body should not be expected to compensate enterprises for the data obtained. Public emergencies are rare events and not all such emergencies require the use of data held by enterprises. The business activities of the data holders are therefore not likely to be negatively affected as a consequence of the public sector bodies or Union institutions, agencies or bodies having recourse to this Regulation. However, as cases of an exceptional need other than responding to a public emergency might be more frequent, including cases of prevention of or recovery from a public emergency, data holders should in such cases be entitled to a reasonable compensation which should not exceed the technical and organisational costs incurred in complying with the request and the reasonable margin required for making the data available to the public sector body or to the Union institution, agency or body. The compensation should not be understood as constituting payment for the data itself and as being compulsory. **The public sector body, the Commission, the European Central Bank or Union bodies can challenge the level of compensation requested by the data holder by bringing the matter to the competent authority of the Member State where the data holder is based.**

(68) The public sector body or Union institution, agency or body may share the data it has obtained pursuant to the request with other entities or persons when this is needed to carry out scientific research activities or analytical activities it cannot perform itself. Such data may also be shared under the same circumstances with the national statistical institutes and Eurostat for the compilation of official statistics. ~~Such r~~**R**esearch activities should however be compatible with the purpose for which the data was requested and the data holder should be informed about the further sharing of the data it had provided. Individuals conducting research or research organisations with whom these data may be shared should act either on a not-for-profit basis or in the context of a public-interest mission recognised by the State. Organisations upon which commercial undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, which could result in preferential access to the results of the research, should not be considered research organisations for the purposes of this Regulation.

(68a) **In order to deal with a cross-border public emergency or another exceptional need, data requests may be addressed to data holders in different Member States than the one of the requesting public sector body. In this case, the request should be communicated to the competent authority of the Member State where the data holder is based, in order to let it examine the request against the criteria established in this Regulation. The same would apply to requests made by the Commission, the European Central Bank or Union bodies. The competent authority would be entitled to advise the public sector body or the Commission, the European Central Bank or Union body to cooperate with the competent authority of the data holder's Member State on the need to ensure a minimised administrative burden on the data holder. When the competent authority has justified reservations in relation to compliance of the request with this Regulation, it should return the request to the public sector body or to the Commission, the European Central Bank or Union body which should take those reservations into account before resubmitting the request.**

(69) The ability for customers of data processing services, including cloud and edge services, to switch from one data processing service to another, while maintaining a minimum functionality of service, is a key condition for a more competitive market with lower entry barriers for new service providers.

(70) Regulation (EU) 2018/1807 of the European Parliament and of the Council encourages service providers to effectively develop and implement self-regulatory codes of conduct covering best practices for, *inter alia*, facilitating the switching of data processing service providers and the porting of data. Given the limited efficacy of the self-regulatory frameworks developed in response, and the general unavailability of open standards and interfaces, it is necessary to adopt a set of minimum regulatory obligations on providers of data processing services to eliminate contractual, economic and technical barriers to effective switching between data processing services.

(71) Data processing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other virtual or physical infrastructure, operating systems, software, including software development tools, storage, applications and services. The capability of the customer of the data processing service to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the service provider could be described as on-demand administration. The term 'broad remote access' is used to describe that the computing capabilities are provided over the network and accessed through mechanisms promoting the use of heterogeneous thin or thick client platforms (from web browsers to mobile devices and workstations). The term 'scalable' refers to computing resources that are flexibly allocated by the data processing service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase or decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing. The term 'highly distributed' is used to describe data processing services that involve data processing closer to where data are being generated or collected, for instance in a connected

data processing device. Edge computing, which is a form of such highly distributed data processing, is expected to generate new business models and cloud service delivery models, which should be open and interoperable from the outset.

(71a) The generic concept 'data processing service' by definition covers a very large number of services, with a very broad range of different purposes, functionalities and technical set-ups. As commonly understood by providers and users and in line with broadly used standards, data processing services fall into one or more of the following three data processing service delivery models: IaaS (infrastructure-as-a-service), PaaS (platform-as-a-service) and SaaS (software-as-a-service). These service delivery models indicate the level and type of computing resources (hardware and/or software) offered by the provider of a given service, relative to the computing resources that remain in control of the user of that service. In a much more detailed categorisation, data processing services can be categorised in a non-exhaustive multiplicity of different 'service types', meaning sets of data processing services that share the same primary objective and main functionalities. Examples of such service types could be customer relationship management systems, office suites or cloud-based software suites tailored to a specific sector, such as cloud-based banking software. Typically, services falling under the same service type also share the same data processing service model.

(72) This Regulation aims to facilitate switching between data processing services, which encompasses all conditions and actions that are necessary for a customer to terminate a contractual agreement of a data processing service, to conclude one or multiple new contracts with different providers of data processing services, to port all its digital assets, including data, to the concerned other providers and to continue to use them in the new environment while benefitting from functional equivalence. Digital assets refer to elements in digital format for which the customer has the **sustained** 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. Functional equivalence means the maintenance of a minimum level of functionality of a service after switching, and should be deemed technically feasible whenever both the originating and the destination data processing services cover (in part or in whole) the same service type. **Services can only be expected to facilitate functional equivalence for the functionalities that both the originating and destination services offer. This Regulation does not instate an obligation of facilitating functional equivalence for data processing services of the PaaS and/or SaaS service delivery model.** Metadata, generated by the customer's use of a service, should also be portable pursuant to this Regulation's provisions on switching.

(72a) An extension - on the ground of technical unfeasibility to the switching obligations proposed in this Regulation – may only be invoked in exceptional cases. The burden of proof in this regard should be fully on the provider of the concerned data processing service.

(72b) After a transition period of three years after this Regulation enters into force, all 'switching charges' should be abolished. Switching charges are charges imposed by data processing providers to their customers for the switching process. Typically, those charges are intended to pass on costs, which the originating provider may incur because of the switching process, to the customer that wishes to switch. Examples of common switching charges are costs related to the transit of data from one provider to the other or to an on-premise system ('data egress costs') or the costs incurred for specific support

actions during the switching process, for example in terms of additional human resources provided by the originating data processing service provider.

(73) Where providers of data processing services are in turn customers of data processing services provided by a third party provider, they will benefit from more effective switching themselves, while simultaneously invariably bound by this Regulation's obligations for what pertains to their own service offerings.

(74) Data processing service providers should be required to offer all assistance and support that is required to make the switching process **to a service of a different data processing service provider** successful and effective~~.~~ **including in cooperation with the data processing service provider of the destination service. Data processing service providers should also be required to remove obstacles for customers wishing to switch to an on-premise system. This Regulation does not require** ~~without requiring those~~ data processing service providers to develop new categories of services within or on the basis of the IT-infrastructure of different data processing service providers to guarantee functional equivalence in an environment other than their own systems. ~~Nevertheless, service providers are required to offer all assistance and support that is required to make the switching process effective.~~ Existing rights relating to the termination of contracts, including those introduced by Regulation (EU) 2016/679 and Directive (EU) 2019/770 of the European Parliament and of the Council[13] should not be affected.

(75) To facilitate switching between data processing services, providers of data processing services should consider the use of implementation and/or compliance tools, notably those published by the Commission in the form of a Rulebook relating to cloud services. In particular, standard contractual clauses are beneficial to increase confidence in data processing services, to create a more balanced relationship between users and service providers and to improve legal certainty on the conditions that apply for switching to other data processing services. **Alternatively, codes of conduct developed pursuant to Article 6 of Regulation (EU) 2018/1807 could be considered as implementation and/or compliance tools, provided they fully reflect the requirements of Chapter VI of this Regulation.** In this light, users and service providers should consider the use of standard contractual clauses developed by relevant bodies or expert groups established under Union law.

(76) Open interoperability specifications and standards developed in accordance with paragraph 3 and 4 of Annex II of Regulation (EU) 1025/2021 in the field of interoperability and portability enable a seamless multi-vendor cloud environment, which is a key requirement for open innovation in the European data economy. As market-driven processes have not demonstrated the capacity to establish technical specifications or standards that facilitate effective cloud interoperability at the PaaS (platform-as-a-service) and SaaS (software-as-a-service) levels, the Commission should be able, on the basis of this Regulation and in accordance with Regulation (EU) No 1025/2012, to request European standardisation bodies to develop such standards, particularly for service types where such standards do not yet exist. In addition to this, the Commission will encourage parties in the market to develop relevant open interoperability specifications. The Commission, by way of delegated acts, can mandate the use of European standards for interoperability or open interoperability specifications for specific service types through a reference in a central Union standards repository for the interoperability of data processing services. European standards and open interoperability specifications will only be referenced if in compliance with the criteria specified in this

[13] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019, p. 1).

Regulation, which have the same meaning as the requirements in paragraphs 3 and 4 of Annex II of Regulation (EU) No 1025/2021 and the interoperability facets defined under the ISO/IEC 19941:2017.

(77) Third countries may adopt laws, regulations and other legal acts that aim at directly transferring or providing governmental access to non-personal data located outside their borders, including in the Union. Judgments of courts or tribunals or decisions of other judicial or administrative authorities, including law enforcement authorities in third countries requiring such transfer or access to non-personal data should be enforceable when based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. In other cases, situations may arise where a request to transfer or provide access to non-personal data arising from a third country law conflicts with an obligation to protect such data under Union law or national law, in particular as regards the protection of fundamental rights of the individual, such as the right to security and the right to effective remedy, or the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data, including the protection of trade secrets, and the protection of intellectual property rights, and including its contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, transfer or access should only be allowed if it has been verified that the third country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent court in the third country, which is empowered to take duly into account the relevant legal interests of the provider of such data. Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality.

(78) To foster further trust in the data, it is important that safeguards in relation to Union citizens, the public sector and businesses are implemented to the extent possible to ensure control over their data. In addition, Union law, values and standards should be upheld in terms of (but not limited to) security, data protection and privacy, and consumer protection. In order to prevent unlawful **governmental** access to non-personal data by **third country authorities**, providers of data processing services subject to this instrument, such as cloud and edge services, should take all reasonable measures to prevent access to the systems where non-personal data is stored, including, where relevant, through the encryption of data, the frequent submission to audits, the verified adherence to relevant security reassurance certification schemes, and the modification of corporate policies.

(79) Standardisation and semantic interoperability should play a key role to provide technical solutions to ensure interoperability. **within the common European data spaces, which are 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**. **This Regulation lays down certain essential requirements for interoperability. Operators within the data spaces, which are entities facilitating or engaging in data sharing within the common European data spaces, including data holders, should comply with these requirements. Compliance with these rules can occur by adhering to the requirements laid down, or by adapting to already existing standards via a presumption of conformity.** In order to

facilitate the conformity with the requirements for interoperability, it is necessary to provide for a presumption of conformity for interoperability solutions that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council. The Commission should adopt common specifications in areas where no harmonised standards exist or where they are insufficient in order to further enhance interoperability for the common European data spaces, application programming interfaces, cloud switching as well as smart contracts. Additionally, common specifications in the different sectors could remain to be adopted, in accordance with Union or national sectoral law, based on the specific needs of those sectors. Reusable data structures and models (in form of core vocabularies), ontologies, metadata application profile, reference data in the form of core vocabulary, taxonomies, code lists, authority tables, thesauri should also be part of the technical specifications for semantic interoperability. Furthermore, the Commission should be enabled to mandate the development of harmonised standards for the interoperability of data processing services.

(80) To promote the interoperability of **tools for the automated execution of data sharing agreements** ~~smart contracts in data sharing applications~~, it is necessary to lay down essential requirements for smart contracts ~~for~~ **which** professionals ~~who~~ create ~~smart contracts~~ for others or integrate ~~such smart contracts~~ in applications that support the implementation of agreements for sharing data. In order to facilitate the conformity of such smart contracts with those essential requirements, it is necessary to provide for a presumption of conformity for smart contracts that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council. **The notion of "smart contract" in this Regulation is technologically neutral. Smart contracts can be connected to any kind of electronic ledger, be it a centrally operated ledger or a ledger operated in distributed manner. The obligation should not apply to tools for the automated execution of data sharing agreements that are used exclusively for internal purposes of an organisation, within closed systems. The essential requirement to ensure that smart contracts can be interrupted and terminated implies mutual consent by the parties to the data sharing agreement.**

(80a) Besides the obligation on professional developers of smart contracts to comply with essential requirements, it is also necessary to oblige those operators within data spaces that facilitate data sharing within and across the common European data spaces to support interoperability of tools for data sharing including smart contracts. Such operators shall, therefore, select only tools for the automated execution of data sharing agreements that comply with technical specifications so that all operators within data spaces can share data amongst one another.

(81) In order to ensure the efficient implementation of this Regulation, Member States should designate one or more competent authorities. If a Member State designates more than one competent authority, it should also designate a coordinating competent authority. Competent authorities should cooperate with each other. **Through the exercise of their powers of investigation in accordance with applicable national procedures, ~~C~~competent authorities should be able to search for and obtain information ~~that is located in their national territory~~, in particular due to an entity's activity in their jurisdiction, and including in the context of joint investigations, with due regard to the fact that oversight and enforcement measures concerning an entity under the jurisdiction of another Member State should be adopted by the competent authority of that other Member State, where relevant in accordance with the procedures relating to cross-border cooperation. Competent authorities should assist each other in a timely manner, in particular when a**

competent authority in a Member State holds relevant information for an investigation carried out by the competent authorities in other Member States, or is able to gather such information ~~located in its territory~~ to which the competent authorities in the Member State where the entity is established do not have access. The authorities responsible for the supervision of compliance with data protection and competent authorities designated under sectoral legislation should have the responsibility for application of this Regulation in their areas of competence. **In order to avoid conflict of interest, the competent authorities responsible for the application and enforcement of this Regulation in the area of making data available following requests based on exceptional need should not benefit from the right to request data based on exceptional need.**

(82) In order to enforce their rights under this Regulation, natural and legal persons should be entitled to seek redress for the infringements of their rights under this Regulation by lodging complaints with competent authorities. Those authorities should be obliged to cooperate to ensure the complaint is appropriately handled and resolved. In order to make use of the consumer protection cooperation network mechanism and to enable representative actions, this Regulation amends the Annexes to the Regulation (EU) 2017/2394 of the European Parliament and of the Council[14] and Directive (EU) 2020/1828 of the European Parliament and of the Council[15].

(83) Member States competent authorities should ensure that infringements of the obligations laid down in this Regulation are sanctioned by penalties**, which could be in the form of financial penalties, warnings, reprimands or orders to bring business practices in compliance with the obligations under this Regulation. Where appropriate, Member States' competent authorities should make use of interim measures to limit the effects of an alleged violation while the investigation of such violation is on-going**. When doing so, they should take into account the nature, gravity, recurrence and duration of the infringement in view of the public interest at stake, the scope and kind of activities carried out, as well as the economic capacity of the infringer. They should take into account whether the infringer systematically or recurrently fails to comply with its obligations stemming from this Regulation. **In order to ensure that the principle of *ne bis in idem* is respected, and in particular to avoid that the same infringement of the obligations laid down in this Regulation is sanctioned more than once, each Member State that intends to exercise its competence in respect of such entity should, without undue delay, inform all other authorities, including the Commission.**

(83a) In order to help enterprises to draft and negotiate contracts, the Commission should develop and recommend non-mandatory model contractual terms for business-to-business data sharing contracts, where necessary taking into account the conditions in specific sectors and the existing practices with voluntary data sharing mechanisms. These model contractual terms should be primarily a practical tool to help in particular smaller enterprises to conclude a contract. When used widely and integrally, these model contractual terms should also have the beneficial effect of influencing the design of contracts about access to and use of data and therefore lead more broadly towards fairer contractual relations when accessing and sharing data.

---

14 Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, p. 1).

15 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

(84) In order to eliminate the risk that holders of data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service claim the *sui generis* right under Article 7 of Directive 96/9/EC where such databases do not qualify for the *sui generis* right, and in so doing hinder the effective exercise of the right of users to access and use data and the right to share data with third parties under this Regulation, this Regulation should clarify that the *sui generis* right does not apply to such databases as the requirements for protection would not be fulfilled.

(85) In order to take account of technical aspects of data processing services, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of supplementing this Regulation to introduce a monitoring mechanism on switching charges imposed by data processing service providers on the market, to further specify the essential requirements for operators of data spaces and data processing service providers on interoperability and to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[16]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(86) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of supplementing this Regulation to adopt common specifications to ensure the interoperability of common European data spaces and data sharing, the switching between data processing services, the interoperability of smart contracts as well as for technical means, such as application programming interfaces, for enabling transmission of data between parties including continuous or real-time and for core vocabularies of semantic interoperability, and to adopt common specifications for smart contracts. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[17].

(87) This Regulation should not affect specific provisions of acts of the Union adopted in the field of data sharing between businesses, between businesses and consumers and between businesses and public sector bodies that were adopted prior to the date of the adoption of this Regulation. To ensure consistency and the smooth functioning of the internal market, the Commission should, where relevant, evaluate the situation with regard to the relationship between this Regulation and the acts adopted prior to the date of adoption of this Regulation regulating data sharing, in order to assess the need for alignment of those specific provisions with this Regulation. This Regulation should be without prejudice to rules addressing needs specific to individual sectors or areas of public interest. Such rules may include additional requirements on technical aspects of the data access, such as interfaces for data access, or how data access could be provided, for example directly from the product or via data intermediation services. Such rules may also include limits on the rights of data holders to access or use user data, or other aspects beyond data access and use, such as governance aspects. This Regulation

---

16 OJ L 123, 12.5.2016, p. 1.

17 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

also should be without prejudice to more specific rules in the context of the development of common European data spaces.

(88) This Regulation should not affect the application of the rules of competition, and in particular Articles 101 and 102 of the Treaty. The measures provided for in this Regulation should not be used to restrict competition in a manner contrary to the Treaty.

(89) In order to allow the economic actors to adapt to the new rules laid out in this Regulation, they should apply from a year after entry into force of the Regulation.

(90) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42 of Regulation (EU) 2018/1725 and delivered a joint opinion on [XX XX 2022].

HAVE ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and scope

1. This Regulation lays down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients, ~~and~~ on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest, **on facilitating switching between data processing services, on introducing safeguards against unlawful third party access to non-personal data, and on providing for the development of interoperability standards for data to be accessed, transferred and used**.

1a. This Regulation covers personal and non-personal data, including the following types of data or in the following contexts:

(a) Chapter II applies to data concerning the performance, use and environment of products and related services.

(b) Chapter III applies to any private sector data that is subject to statutory data sharing obligations.

(c) Chapter IV applies to any private sector data accessed and used on the basis of contractual agreements between businesses.

(d) Chapter V applies to any private sector data with a focus on non-personal data.

(e) Chapter VI applies to any data processed by data processing services.

(f) Chapter VII applies to any non-personal data held in the Union by providers of data processing services.

2. This Regulation applies to:

(a) manufacturers of products and suppliers of related services placed on the market in the Union**, irrespective of their place of establishment,** and ~~the users~~ **the use** of such products or **related** services **in the Union;**

(b) data holders**, irrespective of their place of establishment,** that make data available to data recipients in the Union;

(c) data recipients**, irrespective of their place of establishment,** ~~in the Union~~ to whom data are made available;

(d) public sector bodies and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the

performance of a task carried out in the public interest and the data holders that provide those data in response to such request;

(e) providers of data processing services**, irrespective of their place of establishment,** ~~offering~~ **providing** such services to customers in the Union~~.~~;

(f) operators within data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of agreements to make data available.

2a. Where this Regulation refers to products or related services, such reference shall also be understood to include virtual assistants insofar as they ~~are used to access or control~~ interact with a product or related service.

3. Union law **and national law** on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. ~~**In particular, t**~~This Regulation ~~shall not affect the applicability of Union law on the protection of personal data~~ **is without prejudice to**, in particular Regulation**s** (EU) 2016/679 **and (EU) 2018/1725** and Directive**s** 2002/58/EC **and (EU) 2016/680**, including **with regard to** the powers and competences of supervisory authorities. Insofar as **data subjects are concerned,** the rights laid down in Chapter II of this Regulation ~~are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation~~ shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679~~.~~ **and shall not adversely affect data protection rights of others.**

4. **This Regulation does not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities.** This Regulation shall not affect Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including Regulation (EU) 2021/784 of the European Parliament and of the Council[18] and the [e-evidence proposals [COM(2018) 225 and 226] once adopted, and international cooperation in that area. This Regulation shall not affect the collection, sharing, access to and use of data under Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing and Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying the transfer of funds. This Regulation shall not affect the competences of the Member States regarding activities concerning public security, defence, national security, customs and tax administration and the health and safety of citizens in accordance with Union law~~.~~ **or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.**

4a. This Regulation adds generally applicable obligations on cloud switching going beyond the self-regulatory approach of Regulation (EU) 2018/1807 on the free flow of non-personal data in the European Union.

---

18 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79).

4b. This Regulation does not affect Directive 93/13/EEC on Unfair Terms in Consumer Contracts.

Article 2
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;

(1a) 'personal data' means personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(1ab) 'non-personal data' means data other than personal data;

(1ac) 'consent' means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679;

(1ad) 'data subject' means data subject as referred to in Article 4, point (1), of Regulation (EU) 2016/679;

(1ae) 'readily available data' means data generated by the use of a product that the data holder obtains or can obtain without disproportionate effort, going beyond a simple operation;

(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 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**;

(3) 'related service' means a digital service, including software, 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;

(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;

(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~~;

(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 data~~ **or means of access, in the case of non-personal data**;

(7) 'data recipient' means a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or **a** related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law;

(8) 'enterprise' means a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person's trade, business, craft or profession;

(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;

(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 repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s) **and which is determined and 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.

(11) 'processing' means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(12) 'data processing service' means a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature;

(**12a**) **'customer' means a natural or legal person that has entered into a contractual relationship with a provider of data processing services with the objective of using one or more data processing services.**

(**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.**

(**12c**) **'on-premise' means a digital data processing infrastructure operated by the customer itself to serve its own needs.**

(13) 'service type' means a set of data processing services that share the same primary objective and **main functionalities** ~~basic data processing service model~~;

(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;

(15) 'open interoperability specifications' mean ICT technical specifications, as defined in Regulation (EU) No 1025/2012, which are performance oriented towards achieving interoperability between data processing services;

(15a) 'operators within data spaces' mean legal persons that facilitate or engage in data sharing within and across the common European data spaces;

(16) 'smart contract' means a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger;

(17) 'electronic ledger' means **a sequence of electronic data records which ensures their integrity and the accuracy of their chronological ordering** ~~an electronic ledger within the meaning of Article 3, point (53), of Regulation (EU) No 910/2014~~;

(18) 'common specifications' means a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation;

(19) 'interoperability' means the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data in order to perform their functions;

(20) 'harmonised standard' means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012.

(21) 'Union bodies' means the Union bodies, offices and agencies set up in acts adopted on the basis of the Treaties.

CHAPTER II
RIGHT OF USERS TO USE DATA OF CONNECTED PRODUCTS AND RELATED SERVICES ~~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***

1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use **that are ~~accessible~~ readily available to the data**

holder 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.**

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 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.

Article 4

The right of users to access and use data generated by the use of products or related services

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,** 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 the basis of a simple request through electronic means where technically feasible.

1a. Any agreement between the data holder and the user shall not be binding when it narrows the access rights pursuant to paragraph 1.

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.

2a. The data holder shall not coerce, deceive or manipulate in any way the user or the data subject where the user is not a data subject, 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 such measures do not suffice, t~~T~~**he data holder and the user **~~can~~ shall** agree **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.**

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.

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.

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.

6. The data holder shall only use any non-personal data generated by the use of a product or related service 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.

Article 5
*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,** 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.**

2. Any undertaking designated as a gatekeeper, pursuant to Article **3** ~~[…]~~ of ~~[~~Regulation ~~XXX~~ **(EU) 2022/1925**~~]~~, 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 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).

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.

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.

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 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.

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.

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 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. ~~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.**

9. ~~The right referred to in paragraph 1 shall not adversely affect data protection rights of others~~.

Article 6
Obligations of third parties 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 data when they are no longer necessary for the agreed purpose.

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 data subject,** ~~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 third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;

   (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.

Article 7
Scope of business to consumer and business to business data sharing obligations

1. The obligations of this Chapter shall not apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as micro or small enterprises, 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 or small enterprise. **The same shall apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as medium-sized enterprises as defined in that same Recommendation, for either medium-sized enterprises that meet the threshold of that category for less than one year or that where it concerns products that a medium-sized enterprise has been placed on the market for less than one year.**

2. ~~Where this Regulation **C**~~**hapter** ~~refers to products or related services, such reference shall also be understood to include virtual assistants, insofar as they are used to access or control a product or related service.~~

3. Any contractual term which, to the detriment of the user, excludes the application of, derogates from or varies the effect of the user's rights under this Chapter shall not be binding on the user."

CHAPTER III
HORIZONTAL OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE IN BUSINESS-TO-BUSINESS RELATIONS

Article 8
Conditions under which data holders make data available to data recipients

1. Where**, in business-to-business relations,** a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation ~~implementing~~ **adopted in accordance with** Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV.

2. A data holder shall agree with a data recipient the terms for making the data available. A contractual term concerning the access to and use of the data or the liability and remedies for the breach or the termination of data related obligations shall not be binding if it fulfils the conditions of Article 13 or if**, to the detriment of the user,** it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II.

3. A data holder shall not discriminate between comparable categories of data recipients, including partner enterprises or linked enterprises, as defined in Article 3 of the Annex to Recommendation 2003/361/EC, of the data holder, when making data available. Where a data recipient considers the conditions under which data has been made available to it to be discriminatory, ~~it shall be for~~ the data holder **shall without undue delay provide the data recipient, upon its request, with information showing** ~~the data holder to demonstrate~~ that there has been no discrimination.

4. A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II.

5. Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation ~~implementing~~ **adopted in accordance with** Union law.

6. Unless otherwise provided by Union law, including Article**s 4(3), 5(8) and** 6 of this Regulation, or by national legislation ~~implementing~~ **adopted in accordance with** Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.

Article 9
Compensation for making data available

1. Any compensation agreed between a data holder and a data recipient for making data available **in business-to-business relations** shall be reasonable.

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 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.~~

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.

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.

Article 10
Dispute settlement

1. Data holders and data recipients shall have access to dispute settlement bodies, certified in accordance with paragraph 2 of this Article, to settle disputes in relation to ~~the~~ ~~determination of~~ fair, reasonable and non-discriminatory terms for and the transparent manner of making data available in accordance with Articles 8, ~~and~~ 9 **and 13**.

2. The Member State where the dispute settlement body is established shall, at the request of that body, certify the body, where the body has demonstrated that it meets all of the following conditions:

(a) it is impartial and independent, and it will issue its decisions in accordance with clear**, non-discriminatory** and fair rules of procedure;

(b) it has the necessary expertise in relation to the determination of fair, reasonable and non-discriminatory terms**, including compensation**, for and the transparent manner of making data available, allowing the body to effectively determine those terms;

(c) it is easily accessible through electronic communication technology;

(d) it is capable of issuing its decisions in a swift, efficient and cost-effective manner and in at least one official language of the Union.

If no dispute settlement body is certified in a Member State by [date of application of the Regulation], that Member State shall establish and certify a dispute settlement body that fulfils the conditions set out in points (a) to (d) of this paragraph.

3. Member States shall notify to the Commission the dispute settlement bodies certified in accordance with paragraph 2. The Commission shall publish a list of those bodies on a dedicated website and keep it updated.

4. Dispute settlement bodies shall make the fees, or the mechanisms used to determine the fees, known to the parties concerned before those parties request a decision.

5. Dispute settlement bodies shall refuse to deal with a request to resolve a dispute that has already been brought before another dispute settlement body or before a court or a tribunal of a Member State.

6. Dispute settlement bodies shall grant the parties the possibility, within a reasonable period of time, to express their point of view on matters those parties have brought before those bodies. In that context, dispute settlement bodies shall provide those parties with the submissions of the other party and any statements made by experts. Those bodies shall grant the parties the possibility to comment on those submissions and statements.

7. Dispute settlement bodies shall issue their decision on matters referred to them no later than 90 days after the request for a decision has been made. Those decisions shall be in writing or on a durable medium and shall be supported by a statement of reasons supporting the decision.

7a. Dispute settlement bodies shall make publicly available annual activity reports. The annual report shall include in particular the following general information:

(a) the number of disputes received;

(b) the outcomes of those disputes;

(c) the average time taken to resolve the disputes;

(d) common problems that occur frequently and lead to disputes between the parties; such information may be accompanied by recommendations as to how such problems

can be avoided or resolved, in order to facilitate the exchange of information and best practices.

8. The decision of the dispute settlement body shall only be binding on the parties if the parties have explicitly consented to its binding nature prior to the start of the dispute settlement proceedings.

9. This Article does not affect the right of the parties to seek an effective remedy before a court or tribunal of a Member State.

Article 11
Technical protection measures and provisions on unauthorised use or disclosure of data

1. The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means **to discriminate between data recipients or** to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1).

2. **Where a** ~~A~~ data recipient ~~that~~ has, for the purposes of obtaining data,

   - provided inaccurate **or incomplete** ~~or false~~ information to the data holder, deployed deceptive or coercive means or abused evident gaps in the technical infrastructure of the data holder designed to protect the data,

   - has used the data made available for unauthorised purposes**, including the development of a competing product in the sense of Article 6(2)(e),** or

   - has disclosed those data to another party without the data holder's authorisation,

   the data holder may request the data recipient to, without undue delay: ~~shall without undue delay, unless the data holder or the user instruct otherwise:~~

   (a) ~~destroy~~ **erase** the data made available by the data holder and any copies thereof;

   (b) end the production, offering, placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods.

2a Where the data recipient has acted in violation of Article 6(2)(a) and 6(2)(b), users shall have the same rights as data holders under paragraph 2. Paragraph 3 shall apply *mutatis mutandis*.

3. Paragraph 2, point (b), shall not apply in either of the following cases:

   (a) use of the data has not caused significant harm to the data holder **or the user respectively; or** ~~;~~

   (b) it would be disproportionate in light of the interests of the data holder **or the user**.

Article 12
Scope of obligations for data holders legally obliged to make data available

1. This Chapter shall apply where, **in business-to-business relations,** a data holder is obliged under Article 5, or under Union law or national legislation ~~implementing~~ **adopted in accordance with** Union law, to make data available to a data recipient.

2. Any contractual term in a data sharing agreement which, to the detriment of one party, or, where applicable, to the detriment of the user, excludes the application of this Chapter, derogates from it, or varies its effect, shall not be binding on that party.

3. This Chapter shall only apply in relation to obligations to make data available under Union law or national legislation implementing Union law, which enter into force after [date of application of the Regulation].

CHAPTER IV
UNFAIR CONTRACTUAL TERMS RELATED TO DATA ACCESS AND USE ~~BETWEEN ENTERPRISES~~

Article 13
Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise

1. A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized 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,** shall not be binding on the latter enterprise if it is unfair.

2. A contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.

3. A contractual term is unfair for the purposes of ~~this Article~~ **paragraph 2, in particular** if its object or effect is to:

   (a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;

   (b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in case of breach of those obligations;

   (c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract.

4. A contractual term is presumed unfair for the purposes of ~~this Article~~ **paragraph 2** if its object or effect is to:

(a) inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;

(b) allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;

(c) prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner;

(d) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof;

(e) enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so.

5. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied ~~**drafted in advance**~~ by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied ~~**drafted in advance a**~~ **the** contractual term bears the burden of proving that that term has not been unilaterally imposed.

6. Where the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding.

7. This Article does not apply to contractual terms defining the main subject matter of the contract ~~or to contractual terms determining the price to be paid~~ **nor to the adequacy of the price, as against the data supplied in exchange**.

8. The parties to a contract covered by paragraph 1 may not exclude the application of this Article, derogate from it, or vary its effects.

CHAPTER V
~~I~~MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, ~~AND UNION INSTITUTIONS, AGENCIES~~ THE COMMISSION,

THE EUROPEAN CENTRAL BANK OR UNION BODIES BASED ON EXCEPTIONAL NEED

Article 14
Obligation to make data available based on exceptional need

1. Upon request, a data holder shall make data**, which could includeing relevant metadata,** 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 to use the data requested **in order to carry out their legal competencies statutory duties in the public interest**.

2. This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.

Article 15
Exceptional need to use data

An exceptional 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;

(b) where the data request is limited in time and scope and necessary to prevent a public emergency or to assist the recovery from a public emergency; **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

(1) 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 **purchaseing of** the data on the market at **by offering** market rates or by relying on existing obligations to make data available, and **or** the adoption of new legislative measures **which could guarantee** cannot ensure the timely availability of the data; or

(2) 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.

Article 16
*Relationship with other obligations to make data available to public sector bodies and Union institutions, agencies and bodies **the Commission, the European Central Bank and Union bodies***

1. This Chapter shall not affect obligations laid down in Union or national law for the purposes of reporting, complying with information requests or demonstrating or verifying compliance

with legal obligations**, including ~~in relation to official statistics~~ the obtaining of data for the purpose of compiling official statistics, not based on an exceptional need.**

2. The rights from this Chapter **including the right to access, share and use of data** shall not be exercised by public sector bodies and ~~Union institutions, agencies and bodies~~ **the Commission, the European Central Bank and Union bodies** in order to carry out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration. This Chapter **shall** ~~does~~ not affect the applicable Union and national law on the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, or for customs or taxation administration.

Article 17
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 body~~ **the Commission, the European Central Bank or Union body** shall:

   (a) specify what data are required**, including relevant metadata**;

   (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 European Central Bank** or **Union** body to modify or withdraw the request.

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;

   (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 the competent authority referred to in Article 31, of the Member State where the requesting public sector body is established. The Commission, the European Central Bank and Union bodies shall make their requests available online without undue delay and inform the Commission thereof.**

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.

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 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.

Article 18
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.

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).

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.

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.

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**.

Article 19

*Obligations of public sector bodies and ~~Union institutions, agencies~~ **the Commission, the European Central Bank and Union** bodies*

1. A public sector body or ~~a Union institution, agency or~~ **the Commission, the European 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;

(c) **erase** ~~destroy~~ the data as soon as they are no longer necessary for the stated purpose and inform the data holder **without undue delay** that the data have been **erased** ~~destroyed~~.

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.**

Article 20
Compensation in cases of exceptional need

1. Data made available to respond to a public emergency pursuant to Article 15, point (a), shall be provided free of charge.

2. Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15, points (b) or (c), 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.

3. Where the public sector body or the ~~Union institution, agency or~~ Commission, the European Central Bank or Union body wishes to challenge the level of compensation requested by the data holder, the matter shall be brought to the competent authority referred to in Article 31 of the Member State where the data holder is established.

Article 21
Further sharing of data obtained in the context of exceptional needs with ~~*Contribution of*~~ *research organisations or statistical bodies* ~~*in the context of exceptional needs*~~

1. A public sector body or ~~a Union institution, agency or~~ **the Commission, the European Central Bank or Union** body shall be entitled to share data received under this Chapter

(a) with individuals or organisations in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested, or

(b) ~~to~~ **with** national statistical institutes and Eurostat for the compilation of official statistics.

2. Individuals or organisations receiving the data pursuant to paragraph 1 shall **use the data exclusively** ~~act~~ on a not-for-profit basis or in the context of a public-interest mission recognised in Union or Member State law. They shall not include organisations upon which

commercial undertakings have a decisive influence or which could result in preferential access to the results of the research.

3. Individuals or organisations receiving the data pursuant to paragraph 1 shall comply with the provisions of Article 17(3) and Article 19.

4. 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 paragraph 1, it shall notify **without undue delay** the data holder from whom the data was received**, stating the identity of the organisation or the individual receiving the data and the technical and organisational protection measures taken, including where personal data or trade secrets are involved**.

Article 22
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.

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 for examination**. ~~This requirement shall also apply to requests by Union institutions, agencies and bodies.~~

4. After **having examined the request in the light of the requirements under Article 17,** ~~having been notified in accordance with paragraph 3~~, the relevant competent authority shall ~~**may**~~ **:**

a) transmit the request to the data holder;

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.

c) return the request with duly justified reservations to the public sector body requesting the data 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 resubmitting the request.

d) return the request with duly justified reservations to the Commission, the European Central Bank or the requesting Union body. The Commission, the European Central Bank or the requesting Union body shall take the reservations into account before resubmitting the request.

The competent authority shall act without undue delay.

CHAPTER VI

SWITCHING BETWEEN DATA PROCESSING SERVICES

Article 23
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 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 commercial, technical, contractual and organisational obstacles, which inhibit customers from:

   (a) terminating, after a maximum notice period of 30 calendar days, 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 originaing 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**;

   (d) **in accordance with paragraph 2,** 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~~.

2. Paragraph 1 shall only apply to obstacles that are related to the services, contractual agreements or commercial practices provided by the original provider.

Article 24

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, applications and **other** digital assets generated directly or indirectly by 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,** during which the data processing service provider shall:

      (1) assist and, where technically feasible, complete the ~~switching~~ **porting** process;

      (2) ensure full continuity in the provision of the respective functions or services**;**~~.~~

      (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(c) of this article.

   (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;

   (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 accordance with paragraph 1, point (a) and paragraph 2~~.~~**;**

   (d) a clause guaranteeing full deletion of all customer data directly after the expiration of the period set out in paragraph 1(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(c).

   (e) details of all the standards and open interoperability specifications, data structures and data formats in which the exportable data described according to paragraph (1) b) will be available.

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).~~

Article 25
Gradual withdrawal of switching charges

1. From [date X+3yrs] onwards, providers of data processing services shall not impose any charges on the customer for the switching process.

2. From [date X, the date of entry into force of the Data Act] until [date X+3yrs], providers of data processing services may impose reduced charges on the customer for the switching process.

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.

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 data processing service providers on the market to ensure that the withdrawal of switching charges as described in paragraph 1 of this Article will be attained in accordance with the deadline provided in the same paragraph.

Article 26
Technical aspects of switching

1. Providers of data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall ~~ensure~~ **take all measures in their power, including in cooperation with the data processing service provider of the destination service, to facilitate** that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the ~~new~~ **destination** service.

2. For data processing services other than those covered by paragraph 1, providers of data processing services shall make open interfaces ~~publicly~~ available **to an equal extent to all their customers and the concerned destination service providers** ~~and~~ free of charge**, including sufficient information about the concerned service to enable the development of software to communicate with the service**.

3. For data processing services other than those covered by paragraph 1, providers of data processing services shall ensure compatibility with open interoperability specifications **and**/or European standards for interoperability ~~that are~~ identified **in the central Union data processing service standards repository** in accordance with Article 29(5) of this Regulation**, starting one year after the publication of the relevant open interoperability specifications and/or European standards in the repository**.

4. Where the open interoperability specifications or European standards referred to in paragraph 3 do not exist for the service type concerned, the provider of data processing services shall, at the request of the customer, export all data generated or co-generated, including the relevant data formats and data structures, in a structured, commonly used and machine-readable format.

CHAPTER VII
UNLAWFUL INTERNATIONAL GOVERNMENTAL ACCESS AND TRANSFER OF ~~CONTEXTS~~ NON-PERSONAL DATA ~~SAFEGUARDS~~

Article 27
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 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.

2. Any decision or judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a provider of data processing services to transfer from or give access to non-personal data within the scope of this Regulation held in the Union may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State.

3. In the absence of such an international agreement, where a provider of data processing services is the addressee of a decision of a court or a tribunal or a decision of an administrative authority of a third country to transfer from or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only:

   (a) where the third-country system requires the reasons and proportionality of the decision or judgement to be set out, and it requires such decision or judgement, as the case may be, to be specific in character, for instance by establishing a sufficient link to certain suspected persons, or infringements;

   (b) the reasoned objection of the addressee is subject to a review by a competent court or tribunal in the third-country; and

   (c) the competent court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member State.

   The addressee of the decision may ask the opinion of the relevant competent bodies or authorities, pursuant to this Regulation, in order to determine whether these conditions are met, notably when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States.

The European Data Innovation Board established under Regulation [xxx – DGA] shall advise and assist the Commission in developing guidelines on the assessment of whether these conditions are met.

4. If the conditions in paragraph 2 or 3 are met, the provider of data processing services shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation thereof.

5. The provider of data processing services shall inform the data holder about the existence of a request of an administrative authority in a third-country to access its data before complying with its request, except in cases where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

CHAPTER VIII
INTEROPERABILITY

Article 28
Essential requirements regarding interoperability

1. Operators ~~of~~ **within** data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services:

   (a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

   (b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists**, where available,** shall be described in a publicly available and consistent manner;

   (c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously**, in bulk download** or in real-time in a machine-readable format;

   (d) **where applicable,** the means to enable the interoperability of **tools for automating the execution of data sharing agreements, such as** smart contracts ~~within their services and activities shall be provided~~.

   These requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements coming from other Union or national sectoral legislation.

2. The Commission is empowered to adopt delegated acts, in accordance with Article 38 to supplement this Regulation by further specifying the essential requirements referred to in paragraph 1.

3. Operators ~~of~~ **within** data spaces that meet the harmonised standards or parts thereof published by reference in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements referred to in paragraph 1 of this Article, to the extent those standards cover those requirements.

4. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements under paragraph 1 of this Article

5. The Commission shall, by way of implementing acts, adopt common specifications, where harmonised standards referred to in paragraph 4 of this Article do not exist or in case it considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article, where necessary, with respect to any or all of the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

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

Article 29
Interoperability for data processing services

1. Open interoperability specifications and European standards for the interoperability of data processing services shall:

   (a) be performance oriented towards achieving interoperability **in a secure manner** between different data processing services that cover the same service type;

   (b) enhance portability of digital assets between different data processing services that cover the same service type;

   (c) ~~guarantee~~ **ensure**, where technically feasible, functional equivalence between different data processing services that cover the same service type.

2. Open interoperability specifications and European standards for the interoperability of data processing services shall **adequately** address:

   (a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;

   (b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;

   (c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

3. Open interoperability specifications shall comply with paragraph 3 and 4 of Annex II of Regulation (EU) No 1025/2012.

4. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft European standards applicable to specific service types of data processing services.

5. For the purposes of Article 26(3) of this Regulation, the Commission shall be empowered to adopt delegated acts, in accordance with Article 38, to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services in central Union standards repository for the interoperability of data processing services, where these satisfy the criteria specified in paragraph 1 and 2 of this Article.

Article 30
Essential requirements regarding smart contracts for data sharing

1. The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements:

   (a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

   (b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;

   (c) data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and

   (d) access control: a smart contract shall be protected through rigorous access control mechanisms at the governance and smart contract layers.

2. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall perform a conformity assessment with a view to fulfilling the essential requirements under paragraph 1 and, on the fulfilment of the requirements, issue an EU declaration of conformity.

3. By drawing up the EU declaration of conformity, the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall be responsible for compliance with the requirements under paragraph 1.

4. A smart contract that meets the harmonised standards or the relevant parts thereof drawn up and published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements under paragraph 1 of this Article to the extent those standards cover those requirements.

5. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential the requirements under paragraph 1 of this Article.

6. Where harmonised standards referred to in paragraph 4 of this Article do not exist or where the Commission considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article in a cross-border context, the Commission may, by way of implementing acts, adopt common specifications in respect of the essential requirements set out in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

CHAPTER IX
IMPLEMENTATION AND ENFORCEMENT

Article 31
Competent authorities

1. Each Member State shall designate one or more competent authorities as responsible for the application and enforcement of this Regulation. Member States may establish one or more new authorities or rely on existing authorities.

2. ~~Without prejudice to~~ **Notwithstanding** paragraph 1 ~~of this Article~~:

   (a) the independent supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned. Chapters VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to the processing of personal data;

   (b) for specific sectoral data exchange issues related to the implementation of this Regulation, the competence of sectoral authorities shall be respected;

   (c) the national competent authority responsible for the application and enforcement of Chapter VI of this Regulation shall have experience in the field of data and electronic communications services.

3. Member States shall ensure that the respective tasks and powers of the competent authorities designated pursuant to paragraph 1 of this Article are clearly defined and include:

   (a) promoting awareness among users and entities falling within scope of this Regulation of the rights and obligations under this Regulation;

   (b) handling complaints arising from alleged violations of this Regulation, and investigating, to the extent appropriate, the subject matter of the complaint and informing the complainant**, in accordance with national law,** of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another competent authority is necessary;

   (c) conducting investigations into matters that concern the application of this Regulation, including on the basis of information received from another competent authority or other public authority;

   (d) imposing, through administrative procedures, dissuasive financial penalties which may include periodic penalties and penalties with retroactive effect, or initiating legal proceedings for the imposition of fines;

   (e) monitoring technological developments of relevance for the making available and use of data;

(f) cooperating with competent authorities of other Member States to ensure the consistent application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay;

(g) ensuring the online public availability of requests for access to data made by public sector bodies in the case of public emergencies under Chapter V;

(h) cooperating with all relevant competent authorities to ensure that the obligations of Chapter VI are enforced consistently with other Union legislation and self-regulation applicable to providers of data processing service;

(i) ensuring that charges for the switching between providers of data processing services are withdrawn in accordance with Article 25.

4. Where a Member State designates more than one competent authority, the competent authorities shall, in the exercise of the tasks and powers assigned to them under paragraph 3 of this Article, cooperate with each other, including, as appropriate, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 **or sectoral authorities**, to ensure the consistent application of this Regulation. In such cases, relevant Member States shall designate a coordinating competent authority.

5. Member States shall communicate the name of the designated competent authorities and their respective tasks and powers and, where applicable, the name of the coordinating competent authority to the Commission. The Commission shall maintain a public register of those authorities.

6. When carrying out their tasks and exercising their powers in accordance with this Regulation, the competent authorities shall remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions **in individual cases** from any other public authority or any private party.

7. Member States shall ensure that the designated competent authorities are provided with the necessary resources to adequately carry out their tasks in accordance with this Regulation.

8. **In accordance with Regulation (EU) 2018/1725, the EDPS shall be responsible for monitoring the application of Chapter V insofar as the processing of personal data by the Commission or Union bodies is concerned.**

9. Competent authorities shall cooperate with competent authorities of other Member States to ensure a consistent and efficient application of this Regulation. Such mutual assistance shall include the exchange of all relevant information by electronic means, without undue delay, in particular to carry out the tasks referred to in paragraph (3), points (b), (c) and (d).

Where a competent authority in one Member State requests assistance or enforcement measures from a competent authority in another Member State, it shall submit a reasoned request. The competent authority shall, upon receiving such a request, provide a response, detailing the actions that have been taken or which are intended to be taken, without undue delay.

Competent authorities shall respect the principles of confidentiality and of professional and commercial secrecy and shall protect personal data in accordance with Union and

national law. Any information exchanged in the context of assistance requested and provided under this Article shall be used only in respect of the matter for which it was requested.

10. Entities falling within the scope of this Regulation shall be subject to the jurisdiction of the Member State where the entity is established. In case the entity is established in more than one Member State, it shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment, that is, where the entity has its head office or registered office within which the principal financial functions and operational control are exercised.

11. An entity falling within scope of this Regulation that offers products or services in the Union but is not established in the Union, nor has designated a legal representative therein, shall be under the jurisdiction of all Member States, where applicable, for the purposes of ensuring the application and enforcement of this Regulation. Any competent authority may exercise its competence, provided that the entity is not subject to enforcement proceedings for the same facts by another competent authority.

Article 32
Right to lodge a complaint with a competent authority

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed.

2. The competent authority with which the complaint has been lodged shall inform the complainant**, in accordance with national law,** of the progress of the proceedings and of the decision taken.

3. Competent authorities shall cooperate to handle and resolve complaints, including by exchanging all relevant information by electronic means, without undue delay. This cooperation shall not affect the specific cooperation mechanism provided for by Chapters VI and VII of Regulation (EU) 2016/679 **and by Regulation (EU) 2017/2394**.

Article 33
Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

1a. **Member States shall take into account the following non-exhaustive and indicative criteria for the imposition of penalties for infringements of this Regulation, where appropriate:**

(a) the nature, gravity, scale and duration of the infringement;

(b) any action taken by the infringer to mitigate or remedy the damage caused by the infringement;
(c) any previous infringements by the infringer;
(d) the financial benefits gained or losses avoided by the infringer due to the infringement, insofar as such benefits or losses can be reliably established;
(e) any other aggravating or mitigating fators applicable to the circumstances of the case.

2. Member States shall by [date of application of the Regulation] notify the Commission of those rules and measures and shall notify it without delay of any subsequent amendment affecting them.

3. For infringements of the obligations laid down in Chapter II, III and V of this Regulation, the supervisory authorities referred to in Article 51 of the Regulation (EU) 2016/679 may within their scope of competence impose administrative fines in line with Article 83 of Regulation (EU) 2016/679 and up to the amount referred to in Article 83(5) of that Regulation.

4. For infringements of the obligations laid down in Chapter V of this Regulation, the supervisory authority referred to in Article 52 of Regulation (EU) 2018/1725 may impose within its scope of competence administrative fines in accordance with Article 66 of Regulation (EU) 2018/1725 up to the amount referred to in Article 66(3) of that Regulation.

Article 34
Model contractual terms ***and standard contractual clauses***

The Commission shall develop and recommend non-binding model contractual terms on data access and use **and standard contractual clauses for cloud computing contracts** to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations

Article 34a

Role of the European Data Innovation Board

The European Data Innovation Board to be set up as a Commission expert group in accordance with Article 29 of Regulation (EU) 2022/868 shall support the consistent application of this Regulation by:

(a) advising and assisting the Commission with regard to developing a consistent practice of competent authorities relating to the enforcement of Chapters II, III, V and VII;

(b) facilitating cooperation between competent authorities through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the enforcement of the rights and obligations under Chapters II, III and V in cross-border cases, including coordination with regard to the setting of penalties;

(c) advising and assisting the Commission with regard to:

- whether to request the drafting of harmonised standards referred to in Article 28(4) and Article 30(5);

- the preparation of the drafts of the implementing acts referred to in Article 28(5) and Article 30(6);

- the preparation of the delegated acts referred to in Articles 25(4) and 28(2); and

- the adoption of the guidelines laying down interoperability specifications for the functioning of common European data spaces referred to in Article 28(6).

CHAPTER X
SUI GENERIS RIGHT UNDER DIRECTIVE ~~19~~96/9/EC

Article 35
Databases containing certain data

~~In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation,~~ [**For the purposes of the exercise of the rights provided for in Articles 4 and 5 of this Regulation**, the sui generis right provided for in Article 7 of Directive 96/9/EC ~~does~~ **shall** not apply ~~to databases containing data~~ **when data is** obtained from or generated by a product or related service.] OR **[T**he sui generis right provided for in Article 7 of Directive 96/9/EC ~~**does**~~ **shall** not apply ~~to databases containing data~~ **when data is** obtained from or generated by the use of a product or a related service.]

CHAPTER XI
FINAL PROVISIONS

Article 36
Amendment to Regulation (EU) No 2017/2394

In the Annex to Regulation (EU) No 2017/2394 the following point is added:

'29. [Regulation (EU) XXX of the European Parliament and of the Council [Data Act]].'

Article 37
Amendment to Directive (EU) 2020/1828

In ~~the~~ Annex **I** to Directive (EU) 2020/1828 the following point is added:

'67. [Regulation (EU) XXX of the European Parliament and of the Council [Data Act]]'

Article 38
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 25(4), 28(2) and 29(5) shall be conferred on the Commission for an indeterminate period of time from [~~...~~ **date of entry into force of this Regulation**].

3. The delegation of power referred to in Articles 25(4), 28(2) and 29(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 25(4), 28(2) and 29(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 39
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 40
Other Union legal acts governing rights and obligations on data access and use

1. The specific obligations for the making available of data between businesses, between businesses and consumers, and on exceptional basis between businesses and public bodies, in Union legal acts that entered into force on or before [~~xx XXX xxx~~ **date of entry into force of this Regulation**], and delegated or implementing acts based thereupon, shall remain unaffected.

2. This Regulation is without prejudice to Union legislation specifying, in light of the needs of a sector, a common European data space, or an area of public interest, further requirements, in particular in relation to:

   (a) technical aspects of data access;

   (b) limits on the rights of data holders to access or use certain data provided by users;

   (c) aspects going beyond data access and use.

Article 41
Evaluation and review

By [*two years after the date of application of this Regulation*], the Commission shall carry out an evaluation of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee. That evaluation shall assess, in particular:

(a) other categories or types of data to be made accessible;

(b) the exclusion of certain categories of enterprises as beneficiaries under Article 5;

(c) other situations to be deemed as exceptional needs for the purpose of Article 15;

(d) changes in contractual practices of data processing service providers and whether this results in sufficient compliance with Article 24;

(e) diminution of charges imposed by data processing service providers for the switching process, in line with the gradual withdrawal of switching charges pursuant to Article 25~~;~~**.**

(f) other categories of services to which access and use rights or the switching obligations could apply.

Article 42
Entry into force and application

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 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].

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*