Council of the European Union

Brussels, 7 July 2023
(OR. en)

11284/23

**Interinstitutional File: 2022/0047(COD)**

**LIMITE**

**TELECOM 218**
**COMPET 713**
**MI 580**
**DATAPROTECT 190**
**JAI 944**
**PI 108**
**CODEC 1246**



**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Permanent Representatives Committee |
| No. Cion doc.: | 6596/22 |
| Subject: | Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair assess tot and use of data (Data Act)<br>- Analysis of the final compromise text in view to agreement |

## 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. The mandate for opening negotiations with the European Parliament on the Data Act was granted by Coreper on 24 March 2023. After the opening trilogue on 29 March, during which the technical level was mandated to work on the entire proposal, the Swedish Presidency has held 23 technical meetings with the European Parliament.

3. On 17 May, Coreper indicated its flexibilities to the Presidency with regard to Chapter V[2]. On that basis, the second trilogue was held on 23 May.

[1] Doc. 6596/22.
[2] Doc. 9105/23

4. On 23 June, Coreper granted the Presidency a revised mandate to continue the negotiations on the whole proposal. The third trilogue was held on 27 June. During this trilogue the Council and the European Parliament came to an agreement on all political issues and successfully closed the negotiations.

5. In the Annex to this document delegations will find the Proposal for a Regulation on on harmonised rules on fair access to and use of data (Data Act), updated according to the provisional political agreement reached at the third trilogue.



## II. MAIN ELEMENTS OF THE COMPROMISE

1) **IoT data and subjects of rights and obligations (Chapter II)** – With regard to IoT data, the draft agreement provides for a clearer definition of the data falling within the scope of the Regulation, as well as of the different actors' rights and obligations. In addition, the draft agreement introduces a distinction between 'product data' and 'related service data', while keeping the horizontal concept of 'readily available data' as a mix of both these categories of data that can be shared without disproportionate effort by data holders.

2) **Protection of trade secrets (Articles 4(3), (3a) and 3(b), 5(8), (8a) and (8b), and Recital 28a)** – The draft agreement provides for a fine balance between the protection of trade secrets and the main objectives of the Data Act. The data holder can withhold or suspend data sharing when the confidentiality of trade secrets can be undermined. In exceptional circumstances, the data holder may refuse on a case-by-case basis the request for access to the specific data, when it can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets.

3) **B2G data sharing (Chapter V)** – With regard to B2G data sharing, the draft agreement limits the EU institutions benefitting from data sharing at favourable conditions to the Commission, the European Central Bank and Union bodies. It also includes micro and small-sized enterprises as addressees of data sharing requests in emergency cases, while providing for their right to compensation. The sharing of personal data has been limited to emergency cases only (Article 15(1)(a)) and the mitigation of and recovery from public emergencies have been assimilated to tasks in the public interest (Article 15(1)(b)).

4) **Safety and security of products (Article 4(1a))** - The draft agreement has introduced the possibility to allow for contractually agreed restrictions to the access, use or further sharing of data, in light of potential serious adverse effect on the health, safety or security of human beings.

5) **Switching between data processing services (Chapter VI)** - The provision concerning effective switching have been clarified and made more widely applicable. The draft agreement also includes the obligation for providers of data processing services not to impose (or remove, if they exist) obstacles inhibiting customers from unbundling data processing services from one another (Article 23(1)(da)).

6) **Governance model (Article 31)** – Member States will have a high level of flexibility to organise the implementation and enforcement tasks at national level. The draft agreement provides that, in those Member States where more than one competent authority is designated in accordance with Article 31, the coordinating authority will act as a single point of contact and could be labelled as 'Data coordinator'.

7) **Date of application (Article 42)** – The draft agreement also contains a revised date of application of the Data Act, which has been extended from 12 to 20 months from the date of entry to force.

## III. CONCLUSION

1. The Presidency invites the Committee of the Permanent Representatives to:

a. endorse the annexed compromise text as agreed with the European Parliament during the final trilogue, and

b. mandate the Presidency to inform the European Parliament that, should the European Parliament adopt its position at first reading, in accordance with Article 294 paragraph 3 of the Treaty, in the form set out in the compromise package contained in the Annex to this document (subject to revision by the lawyer linguists of both institutions), the Council would, in accordance with Article 294, paragraph 4 of the

Treaty, approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the European Parliament's position.

**ANNEX**



2022/0047 (COD)

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017 /2394 and Directive (EU) 2020/1828**

(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 Central Bank[1]

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,

[1] OJ C 402, 19.10.2022, p. 5.
[2] OJ C 365, 23.9.2022, , p. 18.
[3] OJ C 375, 30.9.2022, , p. 112,.

Whereas:

(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 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 regard 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 is entitled to use product or related services data, 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 data
holders 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 . This Regulation also ensures that data holders make available to public sector bodies of the Member States and to the Commission, the European Central Bank or Union 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 as conferring any new right on data holders to use data generated by the use of a product or related service.

(6) Data generation is the result of the actions of at least two actors, the designer or manufacturer of a product, who may in many cases also be a provider of related services 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 including to encourage data sharing based on voluntary agreements and the development of data-driven value creation by European companies, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use. This Regulation provides a horizontal approach, which could be followed by sectoral legislation to account for the specific situations of the respective sectors.

(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. Any processing of personal data in accordance with this Regulation should comply with all conditions and rules provided by data protection legislation, including but not limited to the need for a valid legal basis under Article 6 of Regulation (EU) 2016/679, where relevant the conditions of Article 9 of Regulation (EU) 2016/679 and Article 5(3) of Directive 2002/58/EC. This Regulation does not constitute a legal basis for the collection or generation of personal data by the data holder. However, in certain circumstances this Regulation imposes the obligation on data holders to make data available by providing that, 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. The access should be provided to personal data that are processed by the data holder based on any of the legal bases mentioned in Article 6 of Regulation (EU) 2016/679. Where the user is not the data subject, this Regulation does not create a legal basis to provide access to personal data or make it available to a third party and should not be understood as conferring any new right on the data holder to use personal data generated by the use of a product or related service. In these cases, it could be in the interest of the user to facilitate meeting the requirements of Article 6 of Regulation (EU) 2016/679. As this Regulation should not adversely affect the data protection rights of others, including the data subject, the data holder can comply with requests inter alia by anonymising personal data or transferring only personal data relating to the user.

(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 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 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], Regulation (EU) 2022/2065, 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 does not apply to areas that fall outside the scope of Union law and in any event is without prejudice to the competences of the Member States concerning public security, defence, national security, customs and tax administration and the health and safety of citizens, regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences.

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

---

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 84/450/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.

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

(13) This Regulation is without prejudice to Union and national legal acts providing for the protection of intellectual property, including Directives 2001/29/EC, 2004/48/EC, and (EU) 2019/790 of the European Parliament and of the Council.

(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 an electronic communications service, a physical connection, or on-device access (often referred to as the Internet of Things) should be covered by this Regulation with the exception of prototypes. Examples of such electronic communications services include in particular land-based telephone networks, television cable networks, satellite-based networks and near-field communication networks. Such connected products are found in all aspects of the economy and society, including in private, civil or commercial infrastructure, vehicles, health and lifestyle equipment, ships, aircraft, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery. Manufacturers' design choices, and, where relevant, sectoral legislation to address sector-specific needs and objectives or relevant decisions
from the competition authorities, should determine which data a connected product is capable of making available.

(14a) The data represent the digitization of user actions and events and should accordingly be accessible to the user. The rules for access and use of data from connected products and related services in this Regulation address both product data and related service data. Product data refers to data, generated by the use of a connected product, that the manufacturer designed to be retrievable from the product by a user, data holder or a third party, including, where relevant, the manufacturer. Related service data refers to data, which also represent the digitization of user actions or events related to the connected product which are generated during the provision of a related service by the provider. Data generated by the use of a product or related service should be understood to cover data recorded intentionally or indirectly resulting from the user's action, such as data about the product's

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

environment or interactions. This should include data on the use of a product generated by a user interface or via a related service, and not be limited to the information that such action happened, but also include all data that the product generates as a result of such action, such as data generated automatically by sensors and data recorded by embedded applications, including applications indicating hardware status and malfunctions. This should also include data generated by the product or related service during times of inaction by the user, such as when the user chooses to not use a product for a given period of time and keep it in stand-by or even switched off, as the status of a product or its components, e.g. batteries, can vary when the product is in stand-by or switched off. In scope of this Regulation are those product data which are not substantially modified, meaning data in raw form (also known as source or primary data, which refers to data points that are automatically generated without any further form of processing) as well as data having been pre-processed for the purpose of making it understandable and useable prior to further processing and analysis, including data collected from a single sensor or a connected group of sensors, for the purpose of making the collected data comprehensible for wider use-cases by determining a physical quantity or quality or the change in a physical quantity, such as temperature, pressure, flow rate, audio, pH, liquid level, position, acceleration or speed. The term ‘ pre-processed data’ should not be interpreted in such a manner as to impose an obligation on the data holder to make substantial investments in cleaning and transforming the data. Such data should include the relevant metadata, including basic context and timestamp to make the data usable, 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, including though facilitating the maintenance and repair of the products in question. By contrast, information derived from this data, which is the outcome of additional investments into assigning values or insights from the data, in particular, by means of proprietary, complex algorithms, including those that are a part of proprietary software, should not be considered to fall within the scope of this Regulation and consequently not be subject to the obligation for a data holder to make it available to a user or data recipient, unless agreed otherwise between the user and the data holder. Such data could include, in particular, information derived by means of sensor fusion, which infers or derives data from multiple sensors, collected in the connected product, using proprietary, complex algorithms and may be subject to intellectual property rights.

(15) This Regulation enables users of connected products to benefit from aftermarket, ancillary and other services based on data collected by sensors embedded in such products the collection of these data being of potential value in improving the performance of the connected products. It is important to delineate between markets for the provision of such sensor-equipped connected products and related services on the one hand and on the other hand markets for unrelated software and content such as textual, audio or audiovisual content often covered by intellectual property rights. As a result, data that such products generate when the user records, transmits, displays or plays content, as well as the content itself, often covered by intellectual property rights, amongst others for the use by an online service should not be covered by this Regulation. This Regulation should also not cover data, which was obtained, generated or accessed from the connected product, or transmitted to it, for the purpose of storage or processing on behalf of other parties, who are not the user, such as may be the case with servers or cloud infrastructure operated by their owners entirely on behalf of third parties, amongst others for the use by an online service.

(16) It is necessary to lay down rules regarding products that are connected with a related service at the time of the purchase, rent or lease in such a way that its absence would prevent the product from performing one or more of its functions, or which are subsequently connected to the product by the manufacturer or a third party to add to or adapt the functionality of the product. Such related services involve the exchange of data between the connected product and the service provider and should be understood as explicitly linked to the operation of the product's functions, such as services that, where applicable, transmit commands to the connected product that are able to impact its action or behaviour. Services, which do not impact the operation of the connected product and do not involve the transmitting of data or commands to the product by the service provider should not be considered as related services. Such services could include, for example, auxiliary consulting, analytics, or financial services, or regular repair and maintenance. Related services can be offered as a part of the sale, rent or lease agreement. Such related services could also normally be provided for products of the same type and users 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 provided by a third party. In the event of doubt as to whether the service is provided as part of the sale, rent or lease contract, this Regulation should apply. Neither the power supply, nor the supply of the connectivity are to be interpreted as related services under this Regulation.

(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, that is either the owner of a connected product, or someone that has received certain temporary rights, for example by means of a rental or lease agreement, to access or use data obtained from the connected product, or that receives related services for the connected product. Those access rights should in no way alter or interfere with the rights of data subjects, who may be interacting with connected product or related service, to personal data generated by the connected product or during the provision of the related service. Such 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.

(18a) 'Data literacy' refers to skills, knowledge and understanding that allows users, consumers and businesses, in particular medium, small and micro companies falling under the scope of this regulation, to gain awareness on the potential value of the data they generated, produce and share and motivated to offer and provide access to their data in compliance with the relevant legal rules. Data literacy should go beyond learning about tools and technologies and aiming to equip and empower citizens and businesses with the ability to benefit from an inclusive and fair data market. The spread of data literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions, and ultimately sustain the consolidation and the innovation path of the data economy in the Union. Competent authority should promote tools and take measures to advance data literacy and awareness among users and entities falling within the scope of this Regulation of the rights and obligations under this Regulation.

(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. 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 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 product and related service data are always easily accessible to a user, free of charge in a comprehensive, structured, commonly used and machine-readable format, with the related metadata necessary to interpret and use the data including for the purpose of retrieving, using or sharing the data. Product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, such as by means of the products' design, the data holder's contract with the user for the provision of related services, and its technical means of data access, without disproportionate effort, are referred to as readily available data. 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 on the central computing unit of a product. This should not prevent the manufacturer or data holder to voluntarily agree with the user on making such adaptations. The design obligations in this Regulation are also without prejudice to the data minimisation principle as described in Article 5(1)(c) of Regulation (EU) 2016/679 and should not be understood as an obligation to design products and related services in such a way that they process or store any personal data besides what is necessary in relation to the purposes for which they are processed. Sectoral legislation could be introduced to outline further specificities, such as the minimum level of product data that should be accessible from connected products or related services, given that such data may be essential for the efficient operation, repair or maintenance. Where subsequent updates or alterations to the connected product, by the manufacturer or another party, lead to additional accessible data or a restriction of initially accessible data, such changes could be communicated to the user in the context of the update or alteration.

(20) In case several persons or entities are considered as user, for example in the case of co-ownership or when an owner, renter or lessee share rights to data access and use the design of the connected product or related service or the relevant interface should enable each user to have access to data they generate. Users of connected products that generate data typically require a user account to be set up. This allows for identification of the user by a data holder, which may be the manufacturer, as well as a means to communicate to exercise and process data access requests. In case several manufacturers or related services providers have sold, rented out or leased products or provided services integrated together to the same user, the user should turn to each of the parties with whom it has a contractual agreement. 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 users to delete their account and the data related to it, and could allow users to stop data access, use or sharing, or request to do so, 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 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. Data processors as defined in Regulation (EU) 2016/679 are by default not considered to act as data holders, unless specifically tasked by the data controller. Products may be designed to permit the user or a third party to process the data on the product, 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 and professional environments and serve as an easy-to-use interface to play content, obtain information, or

activate products connected to the internet . 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 , 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 services. Such virtual assistants should be covered by the data access right provided for in this Regulation . Data generated when a user interacts with a product via a virtual assistant provided by an entity other than the manufacturer of the connected product should also be covered. However, only the data stemming from the interaction between the user and a connected product or related service through the virtual assistant should fall within the scope . Data produced by the virtual assistant unrelated to the use of a connected product or related service is not the object of this Regulation.

(23) Before concluding a contract for the purchase*, rent, or lease* of a connected product, clear and sufficient information should be provided by the seller, the rentor or the lessor, which can be the manufacturer, to the user, with regard to the product data which the connected product is capable of generating, including the type, format and the estimated volume of such data. This could include information on data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, as well as clear and sufficient information relevant for the exercise of the user's rights on how the data may be stored, retrieved or accessed, including terms of use and quality of service of application programming interfaces or, where applicable the provision of software development kits. This obligation provides transparency over the product data generated and enhances the easy access for the user. The information obligation could be fulfilled, 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, which could be provided by the seller, the rentor or the lessor, which can be the manufacturer, to the user before concluding the contract for the purchase, rent or lease of a connected product. 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 (EU) 2016/679. The information obligation before concluding a contract for the provision of a related service should be on the prospective data holder, independently of whether it concludes a contract for the purchase, rent or lease of a connected product. In case any information changes during the lifetime of the connected product or the contract period for the related service, 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.

(24) This Regulation should not be understood as conferring any new right on data holders to use product or related service data. Where the manufacturer of a connected product is a data holder, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user. This agreement should be part of an agreement for the provision of the related service, which can be provided together with the sale, rent or lease agreement relating to the connected product. Any contractual term in the agreement stipulating that the data holder may use product or related service data should be transparent to the user, including as regards the purpose for which the data holder intends to use the data. Such purpose could include improving the functioning of the connected product or related services, developing new products or services, or aggregating data with the aim of making available the resulting derived data to third parties, as long as such derived data does not allow the identification of specific data transmitted to the data holder from the connected product, or allow a third party to derive those data from the data set. 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 data, or certain categories thereof, by a data holder. It should also not prevent users and manufacturers of connected products, which are not data holders, to contractually agree for users to making product or related service data available, either directly, where users can access such data from the connected product or related service, or, where applicable, via another 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. This Regulation does not prevent users,

in business-to-business relations, from making data available to third parties or data holders under any lawful contractual term, including by agreeing to limit or restrict further sharing

of such data, and to be compensated proportionately, for example in exchange for foregoing their right to use or share such data lawfully. The notion of data holder generally does not include public sector bodies. However, it may include public undertakings.

(24a) To foster the emergence of liquid, fair and efficient markets for non-personal data, users of connected products should be able to share data with others, including for commercial purposes, with minimal legal and technical effort. It is currently often difficult for businesses to justify the personnel or computing costs that are necessary for preparing non-personal data sets or data products and offer them to potential counterparties via data marketplaces, including data intermediation services, as defined in Regulation (EU) 2022/868 of the European Parliament and of the Council[1]. A substantial hurdle to non-personal data sharing by businesses thus results from the lack of predictability of economic returns from investing in the curation and making available of data sets or data products. In order to allow for the emergence of liquid, efficient and fair markets for non-personal data in the Union, it must be clarified which party has the right to offer such data on a marketplace. Users should therefore have the right to share non-personal data with data recipients for commercial and non-commercial purposes. Such data sharing could be performed directly by the user, upon the request of the user via a data holder or through data intermediation services. Data intermediation services, as regulated by Regulation (EU) 2022/868 could facilitate a data economy by establishing commercial relationships between users, data recipients and third parties and may support users in exercising their right to use data, such as ensuring the proper anonymisation of the data or aggregation of access to data from multiple individual users. Where data are excluded from a data holder's obligation to make it available to users or third parties, the scope of such data could be specified in the contractual agreement between the user and the data holder for the provision of a related service so that users can easily determine which data is available for them for sharing with data recipients or third parties. Data holders should not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user. This should be without prejudice to legal requirements based on Union or national law for a data holder to make data available. Where relevant, data holders should contractually bind third parties not to further share data received from them.

(25) In sectors characterised by the concentration of a small number of manufacturers supplying connected products to end users, there may only be limited options available to users with regard to access, use and sharing of data. In such circumstances, contractual agreements may

be insufficient to achieve the objective of user empowerment, 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, data holders should not use any product or related service data 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 connected product or related service generating data, EU consumer law, in particular, Directive 2005/29/EC and 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 an enterprise, this Regulation provides that such unfair terms should not be binding on that enterprise.

(27) Data holders 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, data holders 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 a data holder, or to instruct the data holder to do so. The request should be put forward by the user or by an

authorised third party acting on user's behalf, including an authorised data intermediation service in the meaning of the Regulation (EU) 2022/868. Data holders should ensure that the data made available to 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 connected product or related service. Any 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. 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. Other lawful purposes for the use of the data could include lawful reverse engineering, provided that it complies with the requirements set out in this Regulation, Union and national law. This may be the case for the purposes of repairing, prolonging the lifetime of a product or providing aftermarket services to connected products.

(28b) Directive (EU) 2016/943 provides that the acquisition, use or disclosure of a trade secret shall be considered lawful notably where such acquisition, use or disclosure is required or allowed by Union or national law. While this Regulation requires data holders to disclose certain data to users or third parties of the user's choice even when such data qualify for protection as trade secrets, it should be interpreted in a manner to preserve the protection afforded to trade secrets under that Directive.

In this context, data holders should be able to require the user, or third parties of the users' choice, to preserve the confidentiality of data considered as trade secrets.

To that end, data holders should identify trade secrets prior to the disclosure, and should have the possibility to agree with the user, or third parties of the users' choice, on appropriate measures to preserve their confidentiality, including by the use of model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct. In addition to the model contractual terms to be developed by the Commission, the establishment of codes of conduct and technical standards related to the protection of trade secrets in handling the data could help achieve the aim of this Regulation and should be encouraged. In cases where there is no agreement

or if the user or third parties of the users' choice fail to implement those measures or undermine the confidentiality of trade secrets, the data holder should be able to withhold or suspend the sharing of data identified as trade secrets. In such cases, the data holder should communicate to the user or the third party the decision and notify without undue delay the national competent authority of the Member State in which the data holder is established that it has withheld or suspended the sharing of data and identify which measures have not been agreed or implemented or, where relevant, which trade secrets have had their confidentiality undermined. Data holders cannot in principle refuse a data access request under this Regulation only on the basis of certain data considered as trade secrets, as this would undo the intended effects of this Regulation. However, in exceptional circumstances, a data holder who is a trade secret holder, may refuse on a case by case basis the request if it can demonstrate to the user or the third party that, in spite of technical and organisational measures, serious economic damage is highly likely to result from the disclosure of the trade secret. 'Serious economic damage' implies serious and irreparable economic losses. The data holder should duly substantiate its refusal in writing and without undue delay to the user or the third party and notify the national competent authority. This justification should be based on objective elements, demonstrating the concrete risk of a serious economic damage expected from a specific data disclosure and the reasons why the measures taken to safeguard the requested data are not sufficient. A possible negative impact on cybersecurity can be taken into account in this context. Without prejudice to the right to seek redress before a court or a tribunal of a Member State, where the user, or a third party, wishes to challenge the data holder's decision to refuse, withhold or suspend the sharing of data, it can lodge a complaint with the national competent authority who should decide, without undue delay, whether and under which conditions the data sharing shall start or resume, or agree with the data holder to refer the matter to a dispute settlement body. The exceptions to data access rights in this Regulation should not in any case limit the access and data portability rights of data subjects under Regulation (EU) 2016/679.

(28c) The aim of this Regulation is 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 which is regarded as interchangeable or substitutable

by users, in particular based on the product's characteristics, its price and intended use. This Regulation provides for no prohibition to develop a related service using data obtained under this Regulation as this would have an undesirable discouraging effect on innovation. Prohibiting the use of data accessed under this Regulation for developing a competing product protect data holders' innovation efforts. Whether a product competes with the product from which the data originates depends on whether the two products are in competition on the same product market. This would be determined based on the established principles of Union competition law for defining the relevant product market.

(29) A third party to whom data is made available may be a legal or natural person, such as an enterprise, a research organisation, a not-for-profit organisation or an entity acting in a professional capacity. In making the data available to the third party, a 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 product or related service data 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. The user should be able to share non-personal data with third parties for commercial purposes. Upon the agreement with the user, and subject to the provisions of this Regulation, third parties should be able to transfer the data access rights granted by the user to other third parties, including in exchange for compensation. Business-to-business data intermediaries and personal information management systems (PIMS), referred to as data intermediation services in Regulation (EU) 2022/868, may support users or third parties in establishing commercial relations with an undetermined number of potential counterparties, for any lawful purpose falling within the scope of this Regulation. They could play an instrumental role in aggregating access to data from a large number of individual potential data 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[8]. 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 the performance of a contract to which the data subject is a party. 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) Product or related service data 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

[8] OJ L 303, 28.11.2018, p. 59–68.

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 any product or related service data , 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 Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of 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 data holders to set reasonable compensation to be met by third parties, but not by the user, for 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') 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 with the agreement of the user to such sharing.

(34) In line with the data minimisation principle, third parties 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 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. Third parties or data holders should not make the exercise of the rights or choices of users unduly difficult including by offering choices to users in a non-neutral manner, or 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 or data holders 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 and data holders 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) Third parties 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, including in the context of automated decision making. The requirement to delete data when no longer required for the purpose agreed with the user, unless otherwise agreed in relation to non-personal data, complements the right to erasure of the data subject pursuant to Article 17 of Regulation (EU) 2016/679. Where a third party is a provider of a data intermediation service within the meaning of Regulation (EU) 2022/868, 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. Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)[9] 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 Regulation (EU) 2022/1925 , 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. 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. It should not prevent these companies from obtaining and using the same data through other lawful means. 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 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

[9] OJ L 265, 12.10.2022, p. 1–66.

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 frequency, presenting different levels of data and cybersecurity risks, and providing economic opportunities of different value and 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. 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. 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.

(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 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 the responsibility of the data holders 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 , 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 and making available 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 in business- to business relations data holders may request reasonable compensation when legally obliged to make data available to a data recipient. These provisions should not be understood as paying for the data itself. The Commission should develop guidance on the calculation of reasonable compensation in the data economy.

(42a) Such reasonable compensation may include firstly the costs incurred 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, including costs associated formatting of data. Costs related to making the data available may also include the costs of facilitating concrete data sharing requests. They may also vary depending on the volume of the data as well as 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, except for micro and small enterprises and research organisations that use the data on a not-for-profit basis. Such margin may vary depending on factors related to the data itself, such as volume, format or

nature of 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. 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 a connected product owned, leased or rented by the user could also lower the amount of the compensation in comparison to other situations where the data are generated by the data holder for example during the provision of a related service.

(43) 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 and non-discriminatory.

(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 cost directly related to making the data available. The same regime should apply to those research organisations that use the data on a not-for-profit basis.

(45) Directly related costs are those costs 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.

(45a) In duly 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.

(47) Transparency is an important principle to ensure that the compensation requested by a data holder is reasonable, or, if 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 data recipients 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. The provisions in this Regulation on dispute settlement should not require Member States to establish dispute settlement bodies.

(48a) The dispute settlement procedure under this Regulation is a voluntary procedure that enables users, data holders and data recipients 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 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. Dispute settlement bodies should make annual activity reports publicly available.

(50a) Data holders may apply technical protection measures to prevent unlawful disclosure of and access to data. However, those measures should neither discriminate between data recipients, nor hinder the access and use of data for users or data recipients. In the case of abusive practices on the part of the data recipient, such as misleading the data holder by providing false information with the intend to use the data for unlawful purposes, including developing a competing product on the basis of data, the data holder or the user can request the data recipient to implement corrective or remedial measures without undue delay. Any such requests, and in particular the requests to end the production, offering or placing on the market of goods, derivative data or services, as well as those to end importation, export, storage of infringing goods or their destruction, should be assessed in the light of their proportionality in relation to the interests of the data holder or the user.

(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 harm all 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 enterprises when they have been unilaterally imposed on them.

(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 . This concerns 'take-it-or-leave-it' situations where one party supplies a certain contractual term and the other 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 other 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. For the purposes of this Chapter, to grossly deviate from good commercial practices would include, amongst other circumstances of the case to *objectively impair the ability of the party upon whom the term has been unilaterally imposed to protect its legitimate commercial interest in the data in question.*

(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, the Commission, the European Central Bank or Union bodies in the performance of their statutory duties in the public interest to use existing data including, where relevant, accompanying metadata 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 only be under the obligation

to provide data to public sector bodies, the Commission, the European Central Bank or Union bodies in situations of exceptional need to respond to a public emergency.

(57) In case of public emergencies, such as public health emergencies, emergencies resulting from 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, the Commission, the European Central Bank or Union bodies upon their request. The existence of a public emergency should be determined or declared according to the respective procedures in Member States or relevant international organisations, or Union or national law. In such cases, the public sector body should demonstrate that the data in scope of the request could not be otherwise obtained in a timely and effective manner and under equivalent conditions, for instance by a voluntary provision of data by another company or via consultation of a public database.

(58) An exceptional need may also stem from non-emergency situations. In such cases, the public sector body, the Commission, the European Central Bank and Union bodies should be allowed to request only non-personal data. The public sector body should demonstrate that the data are necessary for the fulfilment of a specific task in the public interest that has been explicitly provided by law, such as official statistics or the mitigation or recovery from a public emergency. In addition, such a request can be made only when the public sector body or the Union institution or body has identified specific data could not be otherwise obtained in a timely and effective manner and under equivalent conditions and only if it has exhausted all other means at its disposal to obtain such data, such as obtaining the data through voluntary agreements, including buying data on the market by offering market rates or relying on existing obligations to make data available, or the adoption of new legislative, measures which could guarantee the timely availability of data. Conditions and principles for requests such as purpose limitation, proportionality, transparency, time limitation should also apply. In case of requests for data necessary for the production of official statistics, the requesting public sector body should also demonstrate that the applicable law does not allow it to purchase data on the market.

(59) This Regulation should not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities, including the provision of data by SMEs, and is without prejudice to Union acts providing for mandatory information requests by public entities to private 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, 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 law 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, the Commission, the European Central Bank or Union 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.

(61) In accordance with Article 6(1) and 6(3) of Regulation (EU) 2016/679, 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 specific, 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 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 the Commission, the European Central Bank or Union 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. Online public availability of all requests justified by a public emergency should be ensured. Upon the receipt of such notification, the competent authority can decide to assess the lawfulness of the request and exercise its functions in relation to the enforcement and implementation of this Regulation. Online public availability of all requests should be ensured by the data coordinator.

(62) The objective of the obligation to provide the data is to ensure that public sector bodies, the Commission, the European Central Bank or Union 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, neither Directive (EU) 2019/1024 of the European Parliament and of the Council[3] nor Regulation (EU) 2022/868 should 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, provided the conditions laid down in this Regulation are met, it should not affect the possibility of sharing the data for conducting research or for the development, production and dissemination of official statistics. Public sector bodies should also be allowed to exchange data obtained pursuant to this Regulation with other public sector bodies, the Commission, the European Central Bank or Union body 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, the Commission, the European Central Bank or Union or Union

[3] 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).

body or decline it in a period of 5 or 30 working days depending on the nature of the exceptional need invoked in the request. The data holder should have this possibility where it does not have control over the data requested, namely where it does not have immediate access to the data and cannot determine its availability. 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 96/9/EC of the European Parliament and of the Council[4] apply in relation to the requested datasets, data holders should exercise their rights in a way that does not prevent the public sector body, the Commission, the European Central Bank 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, public sector bodies should use non-personal data wherever possible. In cases of requests based on an exceptional need not related to public emergency, personal data cannot be requested. Whenever personal data is requested, the data holder should anonymise the data. 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. The applicable rules on personal data protection should be complied with. The making available of the data and their subsequent use should be accompanied by safeguards for the rights and interests of individuals concerned by those data.

(65) Data made available to public sector bodies, the Commission, the European Central Bank or Union 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 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. This Regulation builds on the existing access regimes in Union and Member States and does not change the national rules for public access to documents in

[4] 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).

the context of transparency obligations. Data should be erased once it is no longer needed to comply with such obligations.

(66) When reusing data provided by data holders, public sector bodies, the Commission, the European Central Bank or Union bodies should respect both existing applicable legislation and contractual obligations to which the data holder is subject. They should refrain from developing or enhancing a product or service that compete with the product or service of the data holder as well as from sharing the data with a third party for those purposes. They should likewise provide public recognition to the data holders upon their request and should be responsible for maintaining the security of the data received. Where the disclosure of trade secrets of the data holder to public sector bodies, the Commission, the European Central Bank or Union bodies is strictly necessary to fulfil the purpose for which the data has been requested, confidentiality of such disclosure should be guaranteed prior to the disclosure of data.

(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. At the same time, the obligation to provide data might constitute a considerable burden for micro and small enterprises. They should therefore be allowed to claim remuneration even in the context of public emergency response. The business activities of the data holders are therefore not likely to be negatively affected as a consequence of the public sector bodies, the Commission, the European Central Bank or Union bodies having recourse to this Regulation. However, as cases of an exceptional need other than responding to a public emergency might be more frequent, data holders should in such cases be entitled to a reasonable remuneration 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 remuneration should not be understood as constituting payment for the data itself and as being compulsory. Data holders should not be able to claim remuneration in cases where Member State law prevents national statistical institutes or other national authorities responsible for the production of statistics from compensating data holders for making data available. The public sector body, the Commission, the European Central Bank or Union

bodies can challenge the level of remuneration 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 the Commission, the European Central Bank or Union 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 provided that those activities are compatible with the purpose for which the data was requested. It should inform the data holder of such sharing in a timely manner. Such data may also be shared under the same circumstances with the national statistical institutes and Eurostat for the development, production and dissemination of official statistics. Such research 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 significant 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 reject the request of the public sector body or of 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, and without downtime of services, or to use the services of several providers simultaneously without undue obstacles and data transfer costs, is a key condition for a more competitive market with lower entry barriers for new providers of data processing services, and for ensuring further resilience for the users of those services. Customers benefiting from free-tier offerings should also benefit from the provisions for switching that are laid down in this Regulation, so that these offerings do not result in a lock-in situation for customers.

(70) Regulation (EU) 2018/1807 of the European Parliament and of the Council encourages providers of data processing services to effectively develop and implement self-regulatory codes of conduct covering best practices for, inter alia, facilitating the switching of providers of data processing service and the porting of data. Given the limited uptake 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 pre-commercial, commercial, technical, contractual and organisational barriers, which are not limited to reduced speed of data transfer at the customer's exit, which hamper effective switching between data processing services.

(71) Data processing services should cover services that allow ubiquitous and on-demand network access to a configurable, scalable and elastic shared pool of distributed computing resources. Those computing resources include resources such as networks, servers or other virtual or physical infrastructure , 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 provider of data processing services could be described as requiring minimal management effort and as entailing minimal interaction between provider and customer. The term 'ubiquitous' 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 provider of data processing services, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term

'elastic ' 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 'shared pool' 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 services' covers a substantial 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). Those service delivery models represent a specific, pre-packaged combination of IT resources offered by a provider of data processing service. These three fundamental data processing delivery models are further completed by emerging variations, each comprised of a distinct combination of IT resources, such as Storage-as-a-Service and Database-as-a-Service. Data processing services can be categorised in more granular way and a non-exhaustive multitude of different 'same service types', meaning sets of data processing services that share the same primary objective and main functionalities as well as the same type of data processing models, that are not related to the service's operational characteristics. Services falling under the same service type may share the same data processing service model, however, two databases might appear to share the same primary objective, but after considering their data processing model, distribution model and the use cases that they are targeted at, such databases could fall into a more granular subcategory of similar services. Services of the same service type may have different and competing characteristics such as performance, security, resilience, and quality of service.

(71b) Undermining the extraction of the exportable data that belongs to the customer from the source provider of data processing services can impede restoration of the service functionalities in the infrastructure of the destination provider. In order to facilitate the customer's exit strategy, avoid unnecessary and burdensome tasks and to ensure that the customer does not lose any of their data as a consequence of the switching process, the source provider of data processing services should inform the customer in advance of the scope of the data that can be exported once he or she decides to switch to a different service provided by another provider of data processing services or to move to an on-premise infrastructure. The scope of exportable data should include at a minimum input and output data, including metadata, directly or indirectly generated, or cogenerated, by the customer's use of the data processing service, excluding any data processing service provider's or third party's assets or data. The exportable data should exclude any data of data processing service provider that is protected by intellectual property rights or constitutes trade secrets of that provider, third party's assets or or data related to the integrity and security of the service , the export of which will expose the data processing service provider to cybersecurity vulnerabilities. These exclusions should not impede or delay the switching process.

(71c) Digital assets refer to elements in digital format for which the customer has the right of use, including applications and metadata related to configuration of settings, security, and access and control rights management, and other elements such as manifestations of virtualisation technologies, including virtual machines and containers. Digital assets can be transferred in cases the customer has the right of use independently from the contractual relationship of the data processing service it intends to switch from. These other elements are essential for the effective use of the customer's data and applications in the environment of the destination service provider.

(72) This Regulation aims to facilitate switching between data processing services, which encompasses 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 its exportable data and digital assets, and where applicable, benefit from functional equivalence.

(72a) Switching is a customer-driven operation consisting of several steps, including (i) data extraction, i.e. downloading data from a source provider's ecosystem; (ii) transformation,

when the data is structured in a way that does not match the schema of the target location; and (iii) the uploading of the data in a new destination location. In a specific situation outlined in this Regulation, unbundling of a particular service from the contract and moving it to another provider should also be considered as switching. The switching process is sometimes managed on behalf of the customer by a third-party entity. Accordingly, all rights and obligations of the customer established by this Regulation, including the obligation to collaborate in good faith, should be understood to apply to such a third-party entity in those circumstances. Providers of data processing services and customers have different levels of responsibilities, depending on the steps of the process referred to. For instance, the source provider of data processing services is responsible for extracting the data to a machine-readable format, but it is the customer and the destination provider who will upload the data to the new environment, unless specific professional transition service has been obtained. The customer who intends to exercise its rights related to switching, which are foreseen in the Chapter VI of this Regulation, should inform the source provider of data processing services of their decision to either switch to another provider of data processing services, switch to an on-premise infrastructure or to delete its assets and exportable data.

(72b) Functional equivalence means re-establishing, on the basis of the customer's data and digital assets, a minimum level of functionality of a service in the environment of a new data processing service after switching, where the destination service delivers a materially comparable outcome in response to the same input for shared features supplied to the customer under the contractual agreement. Providers of data processing services can only be expected to facilitate functional equivalence for the features that both the source and destination services offer independently. This Regulation does not constitute an obligation of facilitating functional equivalence for data processing service providers other than those offering services of the IaaS delivery model.

(72c) Data processing services are used across sectors and vary in complexity and service type. This is an important consideration with regard to the porting process and timeframes. Nonetheless, an extension of the transition period - on the grounds of technical unfeasibility to finalise the switching process in the given timeframe may only be invoked in duly justified cases. The burden of proof in this regard should be fully on the provider of the concerned data processing service. This is without prejudice to the exclusive right of the customer to extend the transition period once with a period that the customer deems more appropriate for its own needs. The customer may evoke this right for extension prior to or

during the transition period, taking into account that the contractual agreement remains applicable during the transition period.

(72d) 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 on their customers for the switching process. Typically, those charges are intended to pass on costs, which the source provider may incur because of the switching process, to the customer who 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 charges ) or the costs incurred for specific support actions during the switching process. Unnecessarily high data egress charges and other unjustified charges unrelated to actual switching costs, inhibit customers from switching, restrict the free flow of data, have the potential to limit competition and cause lock-in effects for the customers of data processing services by reducing incentives to choose a different or additional service provider.

(72e) As a result of the new obligations foreseen in this Regulation, the source provider of data processing services might outsource certain tasks and remunerate third-party entities in order to comply with those obligations. The customer should not bear costs arising from the outsourcing of services concluded by the source provider of data processing services during the switching process and such costs should be considered as unjustified, unless these costs cover work undertaken by the provider of data processing services at the customer’s request for additional support in the switching process, beyond the switching obligations of the provider as expressly set forth in the Chapter VI. Nothing in this Regulation prevents a customer from remunerating third-party entities for support in the migration process or parties from agreeing on contracts for data processing services of a fixed duration, including proportionate early termination penalties to cover the early termination of said contracts, in accordance with national and Union law. In order to foster competition, the gradual withdrawal of the charges associated with the switching between different providers of data processing services should specifically include data egress charges imposed by the data processing service on a customer. Standard service fees for the provision of the data processing services themselves are not switching charges. These standard service fees are not subject to withdrawal and remain applicable until the contract for the provision of the respective services ceases to apply. Consequently, this Regulation allows the customer to request the provision of additional services that go beyond the switching obligations of the

provider explicitly described in Chapter VI. These additional services, can hence be performed and charged by the provider, when these are performed at the customer's request and the customer agrees upfront to the price thereof.

(72f) An ambitious and innovation-inspiring regulatory approach to interoperability is needed to overcome vendor lock-in, which undermines competition and the development of new services. Interoperability between data processing services involves multiple interfaces and layers of infrastructure and software and is rarely confined to a binary test of being achievable or not. Instead, the building of such interoperability is subject to a cost-benefit analysis which is necessary to establish whether it is worthwhile to pursue reasonably predictable results. The ISO/IEC 19941:2017 is an important reference for the achievement of the objectives of this Regulation, as it contains technical considerations clarifying the complexity of such a process.

(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) Providers of data processing services should be required to offer all assistance and support within their capacity and proportionate to their respective obligations that is required to make the switching process to a service of a different data processing service provider successful, effective and secure. This Regulation does not require providers of data processing services to develop new categories of data processing services, including 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. A source provider of data processing services does not have access and insights into the environment of the destination provider of data processing services. Functional equivalence should not be understood as obliging the provider to rebuild the service in question within the destination provider's infrastructure. Instead, the source provider should take all reasonable measures within their power to facilitate the process of achieving functional equivalence through providing capabilities, adequate information, documentation, technical support and, where appropriate, the necessary tools.

(74a) Data processing service providers should also be required to remove existing obstacles and not impose new ones,

including for customers wishing to switch to an on-premise system. Obstacles can, inter alia, be of pre-commercial, commercial, technical, contractual and organisational nature. A provider of data processing services should also be required to remove obstacles to unbundling a specific individual service from other data processing services provided under a contract and make the respective service available for switching, in the absence of major and demonstrated technical obstacles that prevent such unbundling.

(74b) Throughout the switching process, a high level of security should be maintained. This means that the source provider of data processing services should extend the level of security to which it committed for the service to all technical modalities for which such provider is responsible during the switching process (such as network connections or physical devices). 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[1] should not be affected. Chapter VI of this Regulation should not be understood as preventing a provider of data processing services from provisioning to its customers new and improved services, features and functionalities or from competing with other providers of data processing services on that basis.

(74c) The information to be provided by providers of data processing services to the customer could support the customer's exit strategy and should include procedures for initiating switching from the data processing service, the machine-readable data formats that the user's data can be exported to, the tools, including at least one open interface and ensure compatibility with harmonised standards or open interoperability specifications, foreseen to export data, information on known technical restrictions and limitations that could impact the switching process and the estimated time necessary to complete the switching process.

(75) To facilitate interoperability and 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 providers of data processing services and to improve legal certainty on the conditions that apply for switching to other data processing services. In this light, users and providers of data

processing services should consider the use of standard contractual clauses or other self-regulatory compliance tools provided that they fully reflect the requirements of Chapter VI and relevant provisions of Chapter VIII of this Regulation, developed by relevant bodies or expert groups established under Union law.

(75a) In order to facilitate switching between data processing services, all parties involved, including providers of both source and destination data processing services, should collaborate in good faith with a view to enabling an effective switching process and the secure and timely transfer of necessary data in a commonly used, machine-readable format, and by means of an open standard data portability interface, and avoiding service disruptions and maintaining the continuity of the service.

(75b) Data processing services which concern services of which the majority of main features have been custom-built to respond to the specific demands of an individual customer or where all components have been developed for the purposes of an individual customer should be exempted from some of the obligations applicable to data processing service switching. This should not include services which the provider offers at a broad commercial scale via their services catalogue. It is part of the provider's obligations to duly inform prospective customers of such services, prior to the conclusion of a contractual agreement, of the obligations in this chapter that do not apply to the respective services. Nothing prevents the service provider from eventually deploying such services at scale, in which case the provider would have to comply with all obligations for switching as set out in Chapter VI.

(75d) In line with its minimum requirements to allow for switching between providers, this Regulation also aims to improve interoperability for in-parallel use of multiple data processing services with complementary functionalities. This relates to situations where customers do not terminate a contractual agreement to switch to a different provider of data processing services, but where multiple services of different providers are used in-parallel, in an interoperable manner, to benefit from the complementary functionalities of the different services in the customer's system set-up. However, it is recognised that the egress of data from one data processing service provider to another in order to facilitate in-parallel use of services can be an ongoing activity, in contrast to the one-off egress required as part of switching process. Therefore, data processing service providers may continue to charge for data egress for purposes of in-parallel use beyond the transition period foreseen in

Article 25, but not exceeding the costs incurred. This is important, inter alia, for the successful deployment of 'multi-cloud' strategies, which allow customers to implement future-proof IT strategies and which decrease dependence on individual providers of data processing services. Facilitating a multi-cloud approach for customers of data processing services can also contribute to increasing their digital operational resilience, as recognised for financial service institutions in the Digital Operational Resilience Act (DORA).

(76) Open interoperability specifications and standards developed in accordance with Annex II to Regulation (EU) 1025/2012 of the European Parliament and of the Council[1] in the field of interoperability and portability are expected to enable a multi-vendor cloud environment, which is a key requirement for open innovation in the European data economy. As the market take-up of identified standards under the cloud standardisation coordination (CSC) initiative concluded in 2016 has been limited, the Commission also needs to rely on parties in the market to develop relevant open interoperability specifications to keep up with the fast pace of technological development in this industry. Such open interoperability specifications can then be adopted by the Commission in the form of common specifications. In addition, where market-driven processes have not demonstrated the capacity to establish technical specifications or standards that facilitate effective cloud interoperability at the PaaS and SaaS 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 for same services 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. Following consultation with stakeholders, the Commission, by way of implementing acts, can mandate the use of standards for interoperability or common specifications for specific service types through a reference in a central Union standards repository for the interoperability of data processing services. Providers of data processing services should ensure compatibility with those standards and open interoperability specifications, which should not adversely impact the security and integrity of data. Standards for the interoperability of data processing services and open interoperability specifications will only be referenced if in compliance with the criteria specified in this Regulation, which have the same meaning as the requirements in paragraphs 3 and 4 of Annex II to Regulation (EU) No 1025/2012 and the interoperability facets defined under the ISO/IEC 19941:2017. In addition, the standardisation should take into account the needs of SMEs.

(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 before granting access to that data 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 and among 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. Participants of data spaces that offer data or data-based services to other participants, which are entities facilitating or engaging in data sharing within the common European data spaces, including data holders, should comply with these requirements in as far as elements under their control are concerned. Compliance with these rules can be ensured by adhering to the essential requirements laid down in this Regulation, or presumed by complying with standards or common specifications 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, which represents the framework by default to elaborate standards that provide for such presumptions. The Commission should assess barriers to interoperability and prioritise standardisation needs, based on which it may request one or more European standardisation organisation in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council to draft harmonised standards which fulfil the essential requirements laid down in this Regulation. In case such requests do not result in harmonised standards or such harmonised standards are insufficient to ensure conformity with the essential requirements set out in this Regulation, the Commission should be able to adopt common specifications in these areas provided that in doing so it duly respects the standardisation organisations' role and functions, as an exceptional fall back solution to facilitate the manufacturer's obligation to comply with the essential requirements laid down in this Regulation, when the standardisation process is blocked or when there are delays in the establishment of appropriate harmonised standards. If such delay is due to the technical complexity of the standard in question, this should be considered by the Commission before contemplating the

establishment of common specifications. Common specifications should be developed in an open and inclusive manner and take into account, where relevant, positions adopted by the European Data Innovation Board according to Regulation (EU) 2022/868. Additionally, common specifications in the different sectors could be adopted, in accordance with Union or national sectoral law, based on the specific needs of those sectors. 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 , it is necessary to lay down essential requirements for smart contracts which professionals create for others or integrate 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, for instance, be connected to an electronic ledger. The obligation should apply only to the vendors of smart contracts, but not to the in-house development of smart contracts exclusively for internal use. The essential requirement to ensure that smart contracts can be interrupted and terminated implies mutual consent by the parties to the data sharing agreement. The applicability of the relevant rules of civil, contractual and consumer protection law to the data sharing agreements remains/should remain unaffected by the use of smart contracts for the automated execution of these agreements.

(80a) To demonstrate fulfilment of the essential requirements in this Regulation, 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 executing an agreement to make data available within the sense of this Regulation, should perform a conformity assessment and issue an EU declaration of conformity This conformity assessment should be subject to the general principles set out in Regulations (EC) No 765/2008 and (EC) No 768/2008.

(80b) Besides the obligation on professional developers of smart contracts to comply with essential requirements, it is also important to encourage those participants within data spaces that offer data or data-based services to other participants within and across common

European data spaces to support interoperability of tools for data sharing including smart contracts.

(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 from among them a data coordinator. Competent authorities should cooperate with each other. Through the exercise of their powers of investigation in accordance with applicable national procedures, competent authorities should be able to search for and obtain information , in particular in relation to an entity's activity under their competence, and including in the context of joint investigations, with due regard to the fact that oversight and enforcement measures concerning an entity under the competence 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 to which the competent authorities in the Member State where the entity is established do not have access. Designated competent authorities and data coordinators should be identified in the public register maintained by the Commission. The data coordinator could be an additional means for facilitating collaboration for cross-border situations, such as when a competent authority from a given Member State does not know which authority it should approach in the data coordinator's Member State (e.g. the case is related to more than one competent authority or sector). Among its tasks, the data coordinator should act as a single point of contact for all issues related to the implementation of this Regulation. In case no data coordinator has been designated the competent authority should assume the tasks assigned to the data coordinator under this Regulation. 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. The data coordinator should upon request, provide all the necessary information to natural and legal persons for lodging their complaints to the appropriate competent authority. Those authorities should be obliged to cooperate to ensure the complaint is appropriately handled and resolved swiftly and effectively. 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[10] and Directive (EU) 2020/1828 of the European Parliament and of the Council[11].

(83) Member States competent authorities should ensure that infringements of the obligations laid down in this Regulation are sanctioned by penalties, which could be inter alia in the form of financial penalties, warnings, reprimands or orders to bring business practices in compliance with the obligations under this Regulation. Penalties set by the Member States should be effective, proportionate and dissuasive, and should take into account the recommendations of the European Data Innovation Board, established under Regulation (EU) 2022/868, thus contributing to achieving the greatest possible level of consistency in the setting and application of penalties 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.

---

10 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).

11 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)

(83a) The European Data Innovation Board, established as a Commission expert group under Regulation (EU) 2022/868, should advise and assist the Commission in coordinating national practices and policies on the topics covered by this Regulation as well as in delivering on its objectives in relation to technical standardisation to enhance interoperability. It should also play a key role in facilitating comprehensive discussions between competent authorities concerning the implementation and enforcement of this Regulation. This exchange of information is designed to increase effective access to justice as well as enforcement and judicial cooperation across the Union. Among other functions, the competent authorities should make use of the European Data Innovation Board as a platform to evaluate, coordinate and adopt recommendations on the setting of penalties for infringements of this Regulation. It should allow for competent authorities, with the assistance of the Commission, to coordinate the optimal approach to determining and imposing such penalties. This approach prevents fragmentation while allowing for Member State's flexibility, and should lead to effective recommendations that support the consistent application of this Regulation. The European Data Innovation Board should also have an advisory role in the standardisation processes and the adoption of common specifications in the form of implementing acts, in the adoption of delegated acts to introduce a monitoring mechanism for egress and switching charges imposed by data processing service providers and to further specify the essential requirements for the interoperability of data, data sharing mechanisms and services, as well as the common European data spaces. It should also advise and assist the Commission in the adoption of the guidelines laying down interoperability specifications for the functioning of the common European data spaces.

(83b) 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.

(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

or other machine-generated data, claim the sui generis right under Article 7 of Directive 96/9/EC, and in so doing hinder in particular 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, it should be clarified that the sui generis right does not apply to such databases. That does not affect the possible application of the *sui generis* right under Article 7 of Directive 96/9/EC to databases containing data falling outside the scope of this Regulation provided the requirements for protection in accordance with Article 7(1) of that Directive are 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 participants of data spaces that offer data or data services to other participants, and data processing service providers on interoperability. 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 of 13 April 2016 on Better Law-Making[12]. 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[13].

---

12 OJ L 123, 12.5.2016, p. 1.

13 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

(87) 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 or security requirements, including cybersecurity requirements. This Regulation also should be without prejudice to more specific rules in the context of the development of common European data spaces as well as, with the exception of Chapter V, to Union and national law providing for access to and authorising the use of data for scientific research purposes.

(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, and make the necessary technical arrangements, they should apply from 20 months 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 4 May 2022[14],

HAVE ADOPTED THIS REGULATION:

## CHAPTER I

## GENERAL PROVISIONS

### Article 1

### Subject matter and scope

---

control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

14 OJ C XXX, XX.XX.2022, p. X.

1. This Regulation lays down harmonised rules on making product or related service data available to the user of that connected product or service, on the making data available by data holders to data recipients, on the making data available by data holders to public sector bodies, the Commission, the European Central Bank or Union 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 connected products and related services;

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

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

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

(e) Chapter VI applies to any data and services 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 connected products and providers of related services placed on the market in the Union, irrespective of their place of establishment;

(aa) users of such connected 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 in the Union to whom data are made available;

(d) public sector bodies, the Commission, the European Central Bank or Union bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a specific 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, providing such services to customers in the Union;

(ea) participants of 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 executing an agreement.

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

3. Union 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. This Regulation is without prejudice to that law, in particular to Regulation (EU) 2016/679, Regulation (EU) 2018/1725, and Directive 2002/58/EC, including with regard to the powers and competences of supervisory authorities and the rights of data subjects. Insofar the users are data subjects, the rights laid down in Chapter II of this Regulation shall complement the rights of access and of data portability under Articles 15 and 20 of Regulation (EU) 2016/679. In the event of a conflict between this Regulation and Union law on the protection of personal data or privacy or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data or privacy shall prevail.

4. This Regulation does not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities, in particular voluntary arrangements for the sharing of data. Content shall not be covered by this Regulation. 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[15] 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 does not apply to areas that fall outside the scope of Union law and in any event shall not affect the competences of the Member States concerning public security, defence or national security, regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences, or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order. This Regulation shall not affect the competences of the Member States concerning customs and tax administration and the health and safety of citizens.

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.

4c. 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.

4d. This Regulation complements and does not affect the applicability of 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, including Directives 2005/29/EC, 2011/83/EU and 93/13/EEC.

4f. This Regulation shall not preclude the conclusion of voluntary lawful data sharing contracts, including contracts concluded on a reciprocal basis, which comply with the requirements set out in this Regulation.

[15] 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).

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;

(1b) ‘non-personal data’ means data other than personal data;

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

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

(1e) ‘readily available data’ means product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort, going beyond a simple operation;

(1f) ‘product data’ means data, generated by the use of a connected product, that the manufacturer designed to be retrievable, via an electronic communications service, a physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer.

(1fa) ‘related service data’ means data representing the digitization of user actions or events related to the connected product, recorded intentionally by the user or as a by-product of the user’s action, which is generated during the provision of a related service by the provider;

(1g) ‘making available on the market’ means any supply of a product for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(1h) 'placing on the market' means the first making available of a product on the Union market;

(2) 'connected 'product' means an item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate product data via an electronic communications service, a physical, connection or on-device access and whose primary function is not the storing, processing or transmission of data on behalf of third parties, other than the user;

(3) 'related service' means a digital service other than an electronic communications service, including software, which is connected with the product at the time of the purchase in such a way that its absence would prevent the product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the product;

(4) 'virtual assistants' means 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 services or control the functions of connected products;

(4a) 'consumer' means any natural person who, is acting for purposes which are outside that person's trade, business, craft or profession;

(5) 'user' means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services;

(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 use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;

(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, limited in time such as public health emergencies, emergencies resulting from natural disasters, as well as human-induced major disasters, including major cybersecurity incidents, negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, financial stability, or the substantial and immediate degradation of economic assets in the Union or the relevant Member State(s) and which is determined or officially declared according to the relevant procedures under Union or national law;

(11) 'processing' means any operation or set of operations which is performed on data or on sets of data , 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 enabling ubiquitous, and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature, provided to a customer, that can be rapidly provisioned and released with minimal management effort or service provider interaction;

(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, including applications, for which the customer has the right of use, independently from the contractual relationship of the data processing service it intends to switch from;

(12c) ‘on-premise’ means an ICT infrastructure and computing resources leased, rented or owned by the customer, located in its own data centre and operated by the customer or by a third-party;

(13) ‘same service type’ means a set of data processing services that share the same primary objective, data processing service model, and main functionalities;

(13b) ‘switching’ means the process involving a source provider of data processing services, a customer of a data processing service and a destination provider of data processing services, whereby the customer of a data processing service changes from using one data processing service to using another data processing service of the same service type, or other service, offered by a different provider of data processing services, including through extracting, transforming and uploading the data;

(13c) ‘data egress charges’ refers to data transfer fees charged to the customers of a provider of data processing services for extracting their data through the network from the ICT infrastructure of a provider of data processing services to the systems of another provider or to on-premise infrastructures;

(13d) ‘switching charges’ mean charges, other than standard service fees, imposed by a data processing provider on a customer for the actions mandated by this Regulation for the switching to the systems of another provider, and other than early termination penalties. Switching charges also include data egress charges;

(14) ‘functional equivalence’ means re-establishing on the basis of the customer’s exportable data and digital assets, a minimum level of functionality in the environment of a new data processing service of the same service type after the switching process, where the destination service delivers materially comparable outcome in response to the same input for shared features supplied to the customer under the contractual agreement;

(14a) 'exportable data’ for the purpose of Chapter VI and Article 29 means the input and output data, including metadata, directly or indirectly generated, or cogenerated, by the customer’s use of the data processing service, excluding any data processing service

provider's or third party's assets or data protected by intellectual property rights or constituting a trade secret;

(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;

(16) 'smart contract' means a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering;

(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.

(20b) 'metadata' means a structured description of the contents or the use of data facilitating the discovery or use of that data;

(20c) 'data intermediation service' means data intermediation service as referred to in Article 2, point (8), of Regulation (EU) 2022/868;

(20e) 'trade secret' means information which meets all the requirements of Article 2, point (1) of Directive (EU) 2016/943;

(20f) 'trade secret holder' means a trade secret holder as referred to in Article 2, point (2) of Directive (EU) 2016/943.

(20a) 'Union bodies' means the Union bodies, offices and agencies set up in acts adopted on the basis of the Treaties.

## CHAPTER II

Article 3

Obligation to make product and related service data accessible to the user

1. Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use the data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user.

2. Before concluding a contract for the purchase, rent or lease of a connected product, the seller, the rentor or the lessor, which can be the manufacturer, shall provide at least the following information to the user, in a clear and comprehensible format:

(a) the type, format and estimated volume of product data, which the connected product is capable of generating;

(b) whether the connected product is capable of generating data continuously and in real-time;

(ba) whether the connected product is capable of storing data on-device or on a remote server, including the intended duration of retention;

(c) how the user may access, retrieve, or where relevant, delete those data, including the technical means to do so, as well as their terms of use and quality of service;

2a. Before concluding a contract for the provision of a related service, at least the following information shall be provided to the user in a clear and comprehensible format:

(a) the nature, estimated volume and collection frequency of product data that the prospective data holder is expected to obtain and, where relevant, the modalities for the user to access or retrieve such data, including the prospective data holder's data storage and retention policy.

(b) the nature and estimated volume of related service data to be generated, as well as the modalities for the user to access or retrieve such data, including the prospective data holder's data storage and retention policy;

(d) whether the prospective data holder expects to use readily available data itself and the purposes for which those data will be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user;

(e) the identity of the prospective data holder, such as its trading name and the geographical address at which it is established and where applicable, other data processing parties;

(f) the means of communication which make it possible to contact the prospective 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, and, where applicable, end the data sharing;

(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;

(i) whether a prospective data holder is the holder of trade secrets contained in the data likely to be accessed from the connected product or generated during the provision of related service, and, if not, the identity of the trade secret holder;

(j) the duration of the agreement between the user and the prospective data holder, as well as the modalities to terminate such an agreement.

Article 4

The rights and obligations of users and data holders to access, use and make available product and related service data

1. Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the metadata that is necessary to interpret and use that data, accessible to the user without undue delay, easily, securely and in a comprehensive, structured, commonly used and machine-readable

format, free of charge and, where relevant and technically feasible, 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. Users and data holders may agree contractually on restricting or prohibiting the access, use or further sharing of data, if such processing could undermine security requirements of the product, as laid down by Union or national law, resulting in serious adverse effect on the health, safety or security of human beings. Sectoral competent authorities may provide technical expertise in this context. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.

1b. Without prejudice to the user's right to seek redress at any stage before a court or a tribunal of a Member State, the user may, in relation to any dispute with the data holder concerning the contractual restrictions or prohibitions referred to in paragraph 1a:

(a) lodge in accordance with Article 31(3), point b), a complaint with the national competent authority ; or

(b) agree with the data holder to refer the matter to a dispute settlement body in accordance with Article 10(1a).

1c. Data holders shall not make the exercise of the choices or rights under this Article of the user unduly difficult, including by offering choices to the users in a non-neutral manner or by subverting or impairing the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user interface or a part thereof.

2. In order to verify the quality as a user pursuant to paragraph 1, a data holder shall not require the user to provide any information beyond what is necessary. A 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 user's access request and for the security and the maintenance of the data infrastructure.

3. Trade secrets shall be preserved and shall only be disclosed provided that the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality in particular with respect to third parties. The data holder or the trade secret holder when it is not the data holder shall identify the data which are protected as trade

secrets, including in the relevant metadata, and shall agree with the user proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.

3a. Where there is no agreement on the necessary measures or if the user fails to implement the agreed measures or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing without undue delay to the user. In such cases, the data holder shall notify the national competent authority designated in accordance with Article 31 that it has withheld or suspended the sharing of data and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality compromised.

3b. In exceptional circumstances, when the data holder who is a trade secret holder can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the user, that data holder may refuse on a case-by-case basis the request for access to the specific data in question. Such demonstration shall be duly substantiated, based on objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, the uniqueness and novelty of the product, and provided in writing and without undue delay. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.

3c. Without prejudice to the user's right to seek redress at any stage before a court or a tribunal of a Member State, the user wishing to challenge the data holder's decision to refuse, withhold or suspend the sharing of data in accordance with paragraphs 3a and 3b within this Article may:

(a) lodge in accordance with Article 31(3), point (b), a complaint with the national competent authority, which shall, without undue delay, decide whether and under which conditions the data sharing shall start or resume; or

(b) agree with the data holder to refer the matter to a dispute settlement body in accordance with Article 10(1a).

4. The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate, nor share the data with another third party with that intent and shall not use such data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable the data holder.

4a. The user shall not deploy coercive means or abuse evident gaps in the technical infrastructure of a data holder designed to protect the data in order to obtain access to data.

5. Where the user is not 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 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 and Article 5(3) of Directive (EU) 2002/58 are fulfilled.

6. A data holder shall only use any readily available data that is non-personal on the basis of a contractual agreement with the user. A data holder shall not use such data 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.

6a. Data holders shall not make available non-personal product data, referred to in point (a) of Article 3(2), to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them.

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 readily available data, as well as the metadata that is necessary to interpret and use that data, to a third party, without undue delay, free of charge to the user, of the same

quality as is available to the data holder, easily, securely, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The making available of the data by the data holder to the third party shall be done in compliance with Articles 8 and 9.

1a. The right under paragraph 1 shall not apply to readily available data in the context of testing of other new products, substances or processes that are not yet placed on the market unless use by a third party is contractually permitted.

2. Any undertaking 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), 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. In order to verify the quality as user or as third party pursuant to paragraph 1, the user or third party shall not be required to provide any information beyond what is necessary. Data holders 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 gaps in the technical infrastructure of a data holder designed to protect the data in order to obtain access to data.

5. A data holder shall not use any readily available data 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 given permission to such use and has the technical possibility to easily withdraw that permission at any time.

6. Where the user is not the data subject whose personal data is requested, any personal data generated by the use of a product or related service, including data derived and inferred from that use, shall only be made available where there is a valid legal basis under Article 6 of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 and Article 5(3) of Directive (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 be preserved and 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. The data holder or the trade secret holder when it is not the data holder shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the third party all proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.

8a. Where there is no agreement on the necessary measures or if the third party fails to implement the agreed measures or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing without undue delay to the third party.

In such cases, the data holder shall notify the national competent authority designated in accordance with Article 31 that it has withheld or suspended the sharing of data and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality compromised.

8b. In exceptional circumstances, when the data holder who is a trade secret holder can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the third party, that data holder may refuse on a case-by-case basis the request for access to the specific data in question. Such demonstration shall be duly substantiated, based on objective

elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, the uniqueness and novelty of the product, and provided in writing and without undue delay. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.

8c. Without prejudice to the third party's right to seek redress at any stage before a court or a tribunal of a Member State, the third party wishing to challenge the data holder's decision to refuse, withhold or suspend the sharing of data in accordance with paragraphs 8a and 8b may:

(a) lodge in accordance with Article 31(3), point b), a complaint with the national competent authority, which shall, without undue delay, decide whether and under which conditions the data sharing shall start or resume; or

(b) agree with the data holder to refer the matter to a dispute settlement body in accordance with Article 10(1a).

9. The right referred to in paragraph 1 shall not adversely affect the rights of other data subjects pursuant to the applicable data protection law.

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 where all conditions and rules provided by the applicable data protection law are complied with,subject to the rights of the data subject insofar as personal data are concerned. The third party shall delete the data when they are no longer necessary for the agreed purpose, unless otherwise agreed with the user in relation to non-personal data.

2. The third party shall not:

(a) make the exercise of the rights or choices of users unduly difficult including by offering choices to the users in a non-neutral manner, or coerce, deceive or manipulate the user, by subverting or impairing the autonomy, decision-making or

choices of the user, including by means of a digital interface with the user *or a part thereof*;

(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 necessary to provide the service requested by the user, notwithstanding Article 22(2), points (a) and (c) of Regulation (EU) 2016/679;

(c) make the data it receives available to another third party, unless contractually agreed with the user, and provided that the other third party takes all necessary measures agreed between the data holder and the third party to preserve the confidentiality of trade secrets;

(d) make the data it receives available to an undertaking designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925;

(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; third parties shall also not use any non-personal product or related service data made available to them to derive insights about the economic situation, assets and production methods of or use by the data holder;

(ea) use the data it receives in a manner that adversely impacts the security of the product or related service(s);

(eb) disregard the specific measures agreed with a data holder or with the trade secrets holder pursuant to article 5(8) of this Regulation and break the confidentiality of trade secrets;

(f) prevent the user that is a consumer, 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 and where the micro and small enterprise is not subcontracted to manufacture or design a product or provide a related service. 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.

1a. 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

## OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE

### 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 adopted in accordance with Union law, it *shall* agree, with a data recipient the modalities for making the data available and 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 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 with respect to the modalities of making data available 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, the data holder shall without undue delay provide the data recipient, upon its reasoned request, with information showing that there has been no discrimination.

4. A data holder shall not make data available to a data recipient, including 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 adopted in accordance with Union law.

6. Unless otherwise provided by Union law, including Articles 4(3), 5(8) of this Regulation, or by national legislation 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 upon between a data holder and a data recipient for making data available in business-to-business relations shall be *non - discriminatory and* reasonable and may include a margin.

1a. The data holder and the data recipient shall take into account in particular:

(a) the costs incurred for making the data available, including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage;

(b) the investment in the collection and production of data, where applicable, taking into account whether other parties contributed to the obtaining, generating or collecting the data in question.

1b. Such compensation may also depend on the volume, format and nature of the data.

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, and also non- profit research organisations, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC, which do not qualify as a micro, small or medium enterprise, any compensation agreed shall not exceed the costs set out in paragraph 1a(a).

2a. The Commission shall adopt guidelines on the calculation of reasonable compensation, taking into account the opinion of the European Data Innovation Board established under Regulation (EU) 2022/868.

3. This Article shall not preclude other Union law or national legislation 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 assess whether the requirements of paragraph 1 and, where applicable, paragraph 2 are met.

Article 10

Dispute settlement

1. Users, 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 fulfilment of the data holder's obligation to make data available to the data recipient as well as to the fair, reasonable and non-discriminatory terms for and the transparent manner of making data available in accordance with Article 5(8), this Chapter and Chapter IV.

1a. 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.

1b. Users 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 Articles 4(3b) and 5(8b).

1c. For disputes referred to in paragraph 1a, where the dispute settlement body decides the dispute in favour of the user or the data recipient, the data holder shall bear all the fees charged by the dispute settlement body, and shall reimburse that user or data recipient for any other reasonable expenses that it has paid in relation to the dispute settlement. If the dispute settlement body decides the dispute in favour of the data holder, the user or data recipient shall not be required to reimburse any fees or other expenses that the data holder paid or is to pay in relation to the dispute settlement, unless the dispute settlement body finds that the user or data recipient manifestly acted in bad faith.

1d. Customers and providers of data processing services shall have access to dispute settlement bodies, certified in accordance with paragraph 2, to settle disputes in relation to breaches of the rights of customers and the obligations of providers of data processing services, in accordance with Chapter VI.

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 particular 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.

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.

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:

(b) an aggregation of the outcomes of those disputes;

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

(d) the most common reasons that lead to disputes between the parties.

7b. In order to facilitate the exchange of information and best practices, the public dispute settlement body may decide to include recommendations as to how such problems can be avoided or resolved.

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. A data holder may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to the data, including metadata, and to ensure compliance with Articles 5, 6, 8, and 9, as well as with the agreed contractual terms for making data available. Such technical protection measures shall neither discriminate between data recipients, nor hinder the user's right to effectively obtain a copy, retrieve, use or access data or 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). Users and third parties shall not alter or remove such technical protection measures unless agreed by the data holder.

2. Where a third party or a data recipient has:

- for the purposes of obtaining data provided false information to a data holder, deployed deceptive or coercive means or abused gaps in the technical infrastructure of the data holder designed to protect the data,

- used the data made available for unauthorised purposes, including the development of a competing product within the meaning of Article 6 (2) (e),

- unlawfully disclosed data to another party,

- not maintained the technical and organisational measures agreed in accordance with Article 5(8), or,

- altered or removed technical protection measures applied by the data holder, in accordance with Article 11(1), without the agreement of the data holder;

the third party or data recipient shall comply without undue delay with the requests of the data holder or where applicable, the trade secret holder when they are not the same person, or the user to:

(a) erase the data made available by the data holder and any copies thereof, without undue delay;

(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, where there is a serious risk that the unlawful use of those data will cause a significant harm to the data holder or the user or where such a measure would not be disproportionate in light of the interests of the data holder or the user;

(ba) inform the user of the unauthorised use or disclosure of the data and measures taken to put an end to the unauthorised use or disclosure of the data;

(c) compensate the party suffering from the misuse or disclosure of such unlawfully accessed or used data.

2a. Where a user alters or removes technical protection measures applied by the data holder or does not maintain the technical and organisational measures taken by the user in agreement with the data holder or the trade secrets holder, if it is not the data holder, in order to preserve trade secrets, the data holder shall have the same rights against the user's behaviour under paragraphs 2 and 3. The same shall apply to any other third party having received the data from the user in violation of this Regulation.

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

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 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 adopted in accordance with 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 another 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 another enterprise, shall not be binding on the latter enterprise if it is unfair.

1a. A contractual term which reflects mandatory provisions of Union law or provisions of Union law, which would apply if the contractual terms did not regulate the matter, is not to be considered 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. In particular, a contractual term is unfair for the purposes of paragraph 2, 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 the case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in the case of a 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 paragraph 2 if its object or effect is to:

(a) inappropriately limit the remedies in the case of non-performance of contractual obligations or the liability in the case of a breach of those obligations, or extend the liability of the enterprise upon whom the term has been imposed;

(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, in particular when such data contains commercially sensitive data or are protected by trade secrets or by intellectual property rights*;*

(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 an adequate manner;

(cb) prevent the party upon whom the term has been unilaterally imposed from terminating the agreement within a reasonable time period;

(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;

(ea) enable the party that unilaterally imposed the term to substantially alter the price stipulated in the contract or any other substantive condition related to the nature,

format, quality or quantity of the data to be shared, without a valid reason which is specified in the contract and without the right of the other party to terminate the contract in case of such alteration. This shall not affect terms by which the party that unilaterally imposed the term reserves the right to unilaterally alter the terms of a contract of an indeterminate duration, provided that there is a valid reason specified in that contract, that the party that unilaterally imposed the term is required to inform the other contracting party with reasonable notice, and that the other contracting party is free to terminate the contract at no cost in the case of such an alteration.

5. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied 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 a the contractual term bears the burden of proving that that term has not been unilaterally imposed. The party that supplied the contested term may not argue that the term is an unfair term.

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 nor to the adequacy of the price, as against the data supplied in exchange.

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

## CHAPTER V

## MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, 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. Where a public sector body, or the Commission, the European Central Bank or a Union body demonstrates an exceptional need, as laid out in Article 15, to use certain data, including metadata necessary to interpret and use those data, to carry out its statutory duties in the public interest, data holders that are legal persons, other than public sectors bodies, which hold those data shall make them available upon a duly justified request.



Article 15

Exceptional need to use data

1. An exceptional need to use data within the meaning of this Chapter shall be limited in time and scope and shall be deemed to exist only in any of the following circumstances:

   (a) where the data requested is necessary to respond to a public emergency and the public sector body, the Commission, the European Central Bank or Union body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions;

   (b) in circumstances not covered by paragraph 1(a) and only in so far as non-personal data is concerned, where:
   - a public sector body, the Commission, the European Central Bank or a Union body is acting on the basis of Union or national law and have identified specific data, the lack of which prevents it from fulfilling a specific task in the public interest, that has been explicitly provided by law, such as official statistics or the mitigation or recovery from a public emergency; and

   - the public sector body, the Commission, the European Central Bank or Union agency or body has exhausted all other means at its disposal to obtain such data, including, but not limited to, purchase of the data on the market by offering market rates or relying on existing obligations to make data available, or the adoption of new legislative measures which could guarantee the timely availability of the data.

2. Letter (b) of paragraph 1 shall not apply to small and micro enterprises as defined in article 2 of the Annex to Recommendation 2003/361/EC.

3. The obligation to demonstrate that the public sector body was unable to obtain data by purchasing of the data on the market shall not apply in case the specific task in the public interest is the production of official statistics and where the purchase of data is not allowed by national law.

Article 16

Relationship with other obligations to make data available to public sector bodies and 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 access to information requests or demonstrating or verifying compliance with legal obligations.

2. This Chapter shall not apply to public sector bodies and Union institutions, agencies and the Commission, the European Central Bank and Union bodies when carrying out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or to customs or taxation administration. This Chapter 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 the Commission, the European Central Bank or Union body shall:

(a) specify what data are required, including metadata that is necessary to interpret and use that data;

(b) demonstrate that the conditions necessary for the existence of the exceptional need as referred to in Article 15 for the purpose of 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, the duration of that use, and, where relevant, how the processing of personal data is to address the exceptional need;

(ca) specify, if possible, when the data is expected to be deleted by all parties that have access to it;

(cb) justify the choice of data holder to which the request is addressed;

(cc) specify any other public sector bodies, Union institutions, agencies or bodies and the third parties with which the data requested is expected to be shared with;

(cf) where personal data are requested, specify any measures necessary and proportionate to implement data protection principles, data protection safeguards such as the level of aggregation or pseudonymisation, and whether anonymisation can be applied by the data holder before making data available;

(d) state the legal provision allocating to the requesting public sector body or to the Commission, the European Central Bank or Union bodies the specific public interest task relevant for requesting the data;

(e) specify the deadline referred to in Article 18 and by which the data are to be made available and within which the data holder may request the public sector body, the Commission, the European Central Bank or Union body to modify or withdraw the request.

(eb) make its best effort to avoid that compliance with the data request results in the data holders' liability for infringement of Union or national law.

2. A request for data made pursuant to paragraph 1 of this Article shall:

(a) be made in writing and be expressed in clear, concise and plain language understandable to the data holder;

(ab) be specific with regards to the type of data requested and correspond to data which the data holder has control over at the time of the request;

(b) be justified and proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested;

(c) respect the legitimate aims of the data holder, committing to ensuring the protection of trade secrets in accordance with Article 19(2), and the cost and effort required to make the data available;

(d) concern non-personal data, and only if this is demonstrated to be insufficient to respond to the exceptional need to use data, in accordance with Article 15(1)(a), request personal data in aggregated or pseudonymised form and set out the technical and organisational measures that will be taken to protect the data;

(e) inform the data holder of the penalties that shall be imposed pursuant to Article 33 by the competent authority referred to in Article 31 in the event of non-compliance with the request;

(f) be transmitted to the data coordinator referred to in Article 31 where the requesting public sector body is established, who shall make the request publicly available online without undue delay unless it considers that this would create a risk for public security. The Commission, the European Central Bank and Union bodies, offices and agencies shall make their requests available online without undue delay and inform the Commission thereof.

(fa) in case personal data are requested, be notified without undue delay to the independent supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 in the member state where the data holder is established.

3. A public sector body or 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 the Commission, the European Central Bank or Union body to exchange data obtained pursuant to this Chapter with another public sector body, Commission, the European Central Bank or Union body in view of completing the tasks in Article 15, as specified in the request in accordance with

Article 17, paragraph 1, point (cc) 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 pursuant to Article 19, in particular safeguards to preserve the confidentiality of trade secrets, shall apply also to such third parties. Where a public sector body, the European Commission, the European Central bank or Union body transmits or makes data available under this paragraph, it shall notify the data holder from whom the data was received without undue delay.

4a. Where the data holder considers that its rights under this chapter have been infringed by the transmission or making available of data, it may lodge a complaint with the competent authority referred to in Article 31 of the Member State where the data holder is established.

5. The Commission shall develop a model template for requests pursuant to this Article.

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 the Commission, the European Central Bank or Union body without undue delay, taking into account necessary technical, organisational and legal measures.

2. Without prejudice to specific needs regarding the availability of data defined in sectoral legislation, the data holder may decline or seek the modification of the request without undue delay and not later than within 5 working days following the receipt of a request for the data necessary to respond to a public emergency and without undue delay and not later than within 30 working days in other cases of exceptional need, on either of the following grounds:

(a) the data holder does not have control over the data requested;

(ab) a similar request for the same purpose has been previously submitted by another public sector body, the Commission, the European Central Bank or Union body and

the data holder has not been notified of the erasure of the data pursuant to Article 19(1) point (c);

(b) the request does not meet the conditions laid down in Article 17(1) and (2).

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 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 the compliance with the request to make data available to a public sector body or the Commission, the European Central Bank or Union body requires the disclosure of personal data. In that case the data holder shall aggregate or pseudonymise the data.

6. Where the public sector body or the Commission, the European Central Bank or Union body wishes to challenge a data holder's refusal to provide the data requested, 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 the Commission, the European Central Bank and Union *bodies*

1. A public sector body or the Commission, the European Central Bank or Union body 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 implemented technical and organisational measures that preserve the confidentiality and integrity of the requested data and the security of the data transfers, in particular personal data, as well as safeguard the rights and freedoms of data subjects;

(c) erase the data as soon as they are no longer necessary for the stated purpose and inform the data holder and individuals or organisations that received the data pursuant to paragraph 1 of Article 21 without undue delay that the data have been erased unless archiving of the data is required in accordance with Union and national law on public access to documents in the context of transparency obligations.

1a. A public sector body, the Commission, the European Central Bank, a Union body or a third party receiving data under this Chapter shall not:

(a) use the data or insights about the economic situation, assets and production or operation methods of the data holder to develop or enhance a product or service that compete with the product or service of the data holder;

(c) share the data with another third party for any of those purposes.

2. Disclosure of trade secrets to a public sector body or to 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 a request under Article 15. In such a case, the data holder or the trade secret holder, if it is not the same shall identify the data which are protected as trade secrets, including the relevant metadata. The public sector body or the Commission, the European Central Bank or Union body shall take, prior to the disclosure, all necessary and appropriate technical and organizational measures, to preserve the confidentiality of those trade secrets, including as appropriate through the use of model contractual terms, technical standards and the application of codes of conduct.

2c. A public sector body or a Union institution, agency or body shall be responsible for the security of the data that they receive.

Article 20

Compensation in cases of exceptional need

1. Data holders other than small and micro enterprises as defined in article 2 of the Annex to Recommendation 2003/361/EC shall make available data necessary to respond to a public emergency pursuant to Article 15(1), point (a), free of charge. The public sector body or

the Union institution, agency or body that has received data shall provide public recognition to the data holder if requested by the data holder.

2. The data holder shall be entitled to fair remuneration for making data available in compliance with a request made pursuant to Article 15(1), point (b), such compensation shall cover the technical and organisational costs incurred to comply with the request including, where applicable, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the 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.

2a. Paragraph 2 shall also apply where a small and micro enterprise as defined in article 2 of the Annex to Recommendation 2003/361/EC claims compensation for making data available.

2b. Data holders shall not be able to request compensation for making data available in compliance with a request made pursuant to Article 15, point (b) in case the specific task in the public interest is the production of official statistics and where the purchase of data is not allowed by national law. Member States shall notify the Commission where the purchase of data for the production of official statistics is not allowed by national law.

2c. Where the public sector body or the Commission, the European Central Bank or Union body disagrees with the level of compensation requested by the data holder, they may submit a complaint to the competent authority referred to in Article 31 of the Member State where the data holder is established.

Article 21

Sharing of data obtained in the context of exceptional needs with research organisations or statistical bodies

1. A public sector body 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) with national statistical institutes and Eurostat for the production of official statistics.

2. Individuals or organisations receiving the data pursuant to paragraph 1 shall 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 significant influence which is likely to 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 same obligations that are applicable to the public sector bodies or the Commission, the European Central Bank or Union bodies pursuant to Article 17(3) and Article 19.

3a. Notwithstanding Article 19, paragraph 1 (c), individuals or organisations receiving the data pursuant to paragraph 1 may keep the data received for the purpose for which the data was requested for up to 6 months following erasure of the data by the public sector bodies, the Commission, the European Central bank and Union bodies.

4. Where a public sector body or the Commission, the European Central Bank or a Union body intends to transmit or make data available under paragraph 1, it shall notify without undue delay the data holder from whom the data was received, stating the identity and contact details of the organisation or the individual receiving, the purpose of the transmission or making available of the data, the period for which the data will be used and the technical and organisational protection measures taken, including where personal data or trade secrets are involved. Where the data holder disagrees with the transmission or making available of data, it may lodge a complaint with the competent authority referred to in Article 31 of the Member State where the data holder is established.

Article 22

Mutual assistance and cross-border cooperation

1. Public sector bodies 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. This requirement shall also apply to requests by the Commission, the European Central Bank and Union bodies. The request shall be evaluated by the competent authority of the Member State where the data holder is established.

4. After having examined the request in the light of the requirements under Article 17, the relevant competent authority shall take one of the following actions:

   (a) transmit the request to the data holder and, if applicable, 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;

   (b) reject the request of the public sector body requesting the data for duly substantiated reasons, in accordance with this Chapter. The requesting public sector body shall take the advice of the relevant competent authority into account before possibly resubmitting the request;

   (c) reject the request of the Commission, the European Central Bank or the requesting Union body for duly substantiated reasons, in accordance with this Chapter. The Commission, the European Central Bank or the requesting Union body shall take the reservations into account before possibly resubmitting the request.

The competent authority shall act without undue delay.

# CHAPTER VI

# SWITCHING BETWEEN DATA PROCESSING 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, 24a, 24c, 25 and 26 to enable customers to switch to another data processing service, covering the *same* service *type*, which is provided by a different provider of data processing services or, where relevant, to use several providers of data processing services at the same time. In particular, providers of a data processing service shall not impose and shall remove pre-commercial, commercial, technical, contractual and organisational obstacles, which inhibit customers from:

   (a) terminating, after the maximum notice period and the successful finalisation of the switching process, in accordance with Article 24, the contractual agreement of the service;

   (b) concluding new contractual agreements with a different provider of data processing services covering the same service type;

   (c) porting the customer's exportable data, other digital assets to another provider of data processing services or to an on-premise infrastructure, including after having benefited from a free-tier offering;

   (d) in accordance with Article 23a, achieving functional equivalence in the use of the new service in the IT-environment of the different provider or providers of data processing services covering the same service type.

   (da) unbundling, where technically feasible, data processing services referred to in Article 26(1) from other data processing services provided by the data processing service provider.

Article 23a

Scope of the technical obligations

The responsibilities of data processing service providers as defined in Articles 23, 24, 25, 26 and 28a shall only apply to the services, contractual agreements or commercial practices provided by the source provider of data processing services.

Article 24

Contractual terms concerning switching between providers of data processing services

1. The rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services or, where applicable, to an on-premise infrastructure shall be clearly set out in a written contract which is made available to the customer prior to signing the contract in a way that allows the customer to store and reproduce the contract.

1a. 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 services or to port all exportable data, applications and digital assets to an on-premise ICT infrastructure, without undue delay and in any event no longer than mandatory maximum transition period of 30 calendar days, to be initiated after the maximum notice period referred to in point (aa), during which the service contract remains applicable and during which the provider of data processing services shall:

(i) provide reasonable assistance to the customer and third parties authorized by the customer in the switching process;

(ii) act with due care to maintain business continuity, and continue the provision of the respective functions or services under the contract;

(iii) provide clear information concerning known risks to continuity in the provision of the respective functions or services on the part of the provider of source data processing services;

(iv) ensure that a high level of security is maintained throughout the switching process, notably the security of the data during their transfer and the continued security of the data during the retention period specified in point (c), in line with applicable laws;

(aa) an obligation of the provider of data processing services to support the customer's exit strategy relevant to the contracted services, including through providing all relevant information;

(ab) a clause specifying that the contract shall be deemed terminated and the customer shall be notified of the termination, in one of the following cases:

(i) where applicable, upon the successful completion of the switching process to another provider of data processing services or an on-premise system;

(ii) at the end of the maximum notice period referred to in paragraph (aa), in the case that the customer does not wish to switch but to delete all its digital assets upon service termination;

(ac) a maximum notice period for initiation of the switching process, which shall not exceed 2 months;

(b) an exhaustive specification of all categories of data and digital assets that can be ported during the switching process, including, at a minimum, all exportable data;

(ba) an exhaustive specification of categories of data specific to the internal functioning of provider's service that will be exempted from the exportable data under point (b), where a risk of breach of trade secrets of the provider exists. These exemptions shall however never impede or delay the porting process as foreseen in Article 23;

(c) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the provider of data processing services, in accordance with paragraph 1, point (a) and paragraph 2;

(ca) a clause guaranteeing full erasure of all exportable data and digital assets generated directly by the customer and/or relating to the customer directly after the expiration of the period set out in point (c) or after the expiration of an alternative agreed period later than the expiration of the period set out in point (c), provided that the switching process has been completed successfully;

(cc) data egress charges and switching charges that may be imposed by providers of data processing services in accordance with Article 25.

1b. The contract as defined in paragraph 1 shall include provisions providing that the customer may notify the data processing service provider of its decision to perform one or more of the following actions upon termination of the notification period:

(a) switch to another provider of data processing services, in which case the customer shall provide the necessary details of that provider;

(b) switch to an on-premise system;

(c) delete its digital assets and exportable data.

2. Where the mandatory transition period as defined in paragraph 1, points (a) and (c) of this Article is technically unfeasible, the provider of data processing services shall notify the customer within 14 working days after the switching request has been made, and shall duly motivate the technical unfeasibility and indicate an alternative transition period, which may not exceed 7 months. In accordance with paragraph 1 of this Article, service continuity shall be ensured throughout the alternative transition period against reduced charges, referred to in Article 25(2).

2a. Without prejudice to paragraph 2, the contract as defined in paragraph 1 shall include provisions providing the customer with the right to extend the transition period once with a period that the customer deems more appropriate for its own ends.

Article 24a

Information obligation of providers of data processing services

1. The provider of data processing services shall provide the customer with:

(a) information on available procedures for switching and porting to the data processing service, including information on available porting methods and formats as well as restrictions and technical limitations which are known to the provider of destination data processing services;

(b) reference to an up-to-date online register hosted by the data processing service provider, with details of all the data structures and data formats as well as the relevant standards and open interoperability specifications, in which the exportable data described according to Article 24(1) point (b) will be available.

Article 24b

Good faith obligation

All parties involved, including providers of destination data processing services, shall collaborate in good faith to make the switching process effective, enable the timely transfer of data and maintain the continuity of the service.

Article 24c

Contractual transparency obligations on international access and transfer

1. Providers of data processing services shall make the following information available on their websites, and keep the information updated:

(a) the jurisdiction to which the IT infrastructure deployed for data processing of their individual services is subject;

(b) a general description of the technical, organisational and contractual measures adopted by the data processing service provider in order to prevent governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State.

2. The websites defined in paragraph 1 of this Article shall be referenced in contractual agreements of all data processing services offered by data processing service providers.

Article 25

Gradual withdrawal of switching charges including data egress charges

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

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

3. The reduced switching 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.

3a. Before entering into a contractual agreement with a customer, providers of data processing services shall provide the prospective customer with clear information on standard service fees and early termination penalties that might be imposed on the customer, as well as on the reduced switching charges, including data egress charges that might be imposed on customers during the timeframe referred to in Article 25 paragraph 2.

3b. Where relevant, providers of data processing services shall provide information on services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture.

3c. Where applicable, providers of data processing services shall make this information publicly available to customers via a dedicated section of their website or in any other easily accessible way.

4. The Commission is empowered to adopt delegated acts in accordance with Article 38 to supplement this Regulation in order to introduce a monitoring mechanism for the Commission to monitor switching charges including data egress charges imposed by providers of data processing services on the market to ensure that the withdrawal and reduction of switching charges including data egress charges as described in paragraphs 1 and 2 will be attained in accordance with the deadlines provided in those paragraphs.

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, in line with Article 24b, take all reasonable measures in their power to facilitate that the customer, after switching to a service covering the same service type offered by a destination provider of data processing services, achieves functional equivalence in the use of the destination service. The source provider of data processing services shall facilitate the process through providing capabilities, adequate information, documentation, technical support and, where appropriate, the necessary tools.

2. Providers of data processing services, other than those covered by paragraph 1, shall make open interfaces available to an equal extent to all their customers and the concerned destination service providers free of charge to facilitate switching. These interfaces shall include sufficient information on the service concerned to enable the development of software to communicate with the services, for the purposes of data portability and interoperability.

3. For data processing services other than those covered by paragraph 1, providers of data processing services shall ensure compatibility with common specifications based on open interoperability specifications or harmonised standards for interoperability at least twelve months after the references to these open interoperability specifications or harmonised standards were published in the central Union data processing service standards repository following the publications of the underlying implementing acts in the Official Journal of the European Union in accordance with Article 29(5).

3a. Data processing service providers of services other than those covered by paragraph 1 shall update the online register as referred to in [point (e) of Article 24(1)] in accordance with their obligations under paragraph 3.

4. In case of switching between services of the same service type, for which open interoperability specifications or harmonised standards referred to in paragraph 3 of this

Article have not been identified in the central Union data processing service repository in accordance with Article 29(5), the provider of the processing services shall, at the request of the customer, export all exportable data in a structured, commonly used and machine-readable format.

4a. Providers of data processing services shall not be required to develop new technologies or services, disclose or transfer digital assets protected by intellectual property rights or constituting a trade secret to a customer or to another provider of data processing services or compromise the customer's or provider's security and integrity of service.

Article 26a

Specific regime for certain data processing services

1. The obligations set out in Article 23(1), point (d), and Articles 25 and 26(1) and (3) shall not apply to data processing services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where these data processing services are not offered at broad commercial scale via the service catalogue of the data processing service provider.

2. The obligations set out in this Chapter shall not apply to data processing services provided as a non-production version for testing and evaluation purposes, and for a limited period of time.

3. Prior to the conclusion of a contractual agreement on the provision of the data processing services referred to in this Article, the provider of data processing services shall inform the prospective customer that the Articles listed in paragraph 1 do not apply to the respective service.

## CHAPTER VII

## UNLAWFUL INTERNATIONAL GOVERNMENTAL ACCESS AND TRANSFER OF NON-PERSONAL DATA

Article 27

International governmental access and transfer

1. Providers of data processing services shall take all adequate technical, legal and organisational measures, including contractual arrangements, in order to prevent international and third-country governmental access and transfer of such 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 third-country court or tribunal and any decision of a third-country administrative authority requiring a provider of data processing services to transfer or give access to non-personal data falling within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only 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 an international agreement as referred to in paragraph 2 of this Article, where a provider of data processing services is the addressee of a decision or judgement of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data falling 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 where:

   (a) the third-country system requires the reasons and proportionality of such a decision or judgement to be set out and requires such a decision or judgement 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 third-country court or tribunal; and

   (c) the competent third-country court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of

that third 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 national body or authority competent for international cooperation in legal matters, in order to determine whether these conditions are met, notably when it considers that the decision may relate to trade secrets and other commercially sensitive data as well as to content protected by intellectual property rights or the transfer may lead to re-identification. The relevant national body may consult the Commission. If the addressee considers that the decision may impinge on national security or defence interests of the Union or its Member States, it shall ask the opinion of the national competent bodies or authorities with the relevant competence, in order to determine whether the data requested concerns national security or defence interests of the Union or its Member States. If the addressee has not received a reply within a month, or if the opinion of the competent authorities concludes that the conditions are not met, the addressee may deny the request for transfer or access on those grounds.

The European Data Innovation Board established under Regulation (EU) 2022/868 (Data Governance Act)[16] and referred to in Article [XX] of this Regulation shall advise and assist the Commission in developing guidelines on the assessment of whether these conditions are met.

4. If the conditions laid down 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 the provider's, the relevant competent body's or the relevant competent authority's reasonable interpretation of the request.

5. The provider of data processing services shall inform the data holder about the existence of a request of a third-country administrative authority to access its data before complying with that request, except 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

[16] OJ L 152, 3.6.2022, p. 1

Article 28

Essential requirements regarding interoperability of data spaces

1. Participants of data spaces that offer data or data services to other participants, shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services as well as of 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:

   (a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in machine-readable format, 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 where that is technically feasible and does not hamper the good functioning of the product;

   (d) where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements, such as smart contracts.

   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 of this Regulation to supplement this Regulation by further specifying the essential requirements referred to in paragraph 1 of this Article, in relation to those requirements that, by their nature, cannot produce the intended effect unless they are further specified in binding legal acts of the Union and in order to properly reflect technological and market

developments, taking into account the views of the European Data Innovation Board in accordance with Article 30, point (f) of Regulation (EU) 2022/868.

3. The participants of data spaces that offer data or data services to other participants of data spaces that meet the harmonised standards or parts thereof the reference of which have been 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 in so far as those standards or parts thereof cover those requirements.

4. The Commission shall, 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.

5. The Commission may, by way of implementing acts, adopt common specifications covering any or all of the essential requirements set out in paragraph 1 where the following conditions have been fulfilled:

(a) the Commission has requested, pursuant to Article 10(1) of Regulation 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the essential requirements set out in paragraph 1 and the request has not been accepted or the European standardisation deliverables addressing that request are not delivered within the deadline set in accordance with article 10(1) of Regulation 1025/2012 or the European standardisation deliverables standard do not comply with the request; and

(b) no reference to harmonised standards covering the relevant essential requirements set out in paragraph 1 is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

5a. Before preparing a draft implementing act in accordance with paragraph 5, the Commission shall inform the committee referred to in Article 22 of Regulation EU (No) 1025/2012 that it considers that the conditions in paragraph 5 are fulfilled.

5b. When preparing the draft implementing act establishing the common specifications in accordance with paragraph 5, the Commission shall take into account the views of the European Data Innovation Board and other relevant bodies or expert groups and shall duly consult all relevant stakeholders.

5c. The participants of data spaces that offer data or data services to other participants of data spaces that meet the common specifications established by one or more implementing acts referred to in paragraph 5 or parts thereof shall be presumed to be in conformity with the essential requirements set out in paragraph 1 covered by those common specifications or parts thereof.

5d. Where a harmonised standard is adopted by an European standardisation organisation and proposed to the Commission for the publication of its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal implementing acts referred to in paragraph 5, or parts thereof which cover the same essential requirements set out in paragraph 1.

5e. When a Member State considers that a common specification does not entirely satisfy the essential requirements set out in paragraph 1, it shall inform the Commission thereof with a detailed explanation. The Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification in question.

6. The Commission may adopt guidelines taking into account the proposal of the European Data Innovation Board in accordance with Article 30, point (h), of Regulation (EU) 868/2022 laying down interoperability specifications for the functioning of common European data spaces.

Article 28a

Interoperability for the purposes of in-parallel use of data processing services

1. The requirements set out in Article 23(1), Article 23a, Article 24(1)(a)(ii), (1)(a)(iii), (1)(b), 1(ba) and 1(e) and Article 26(2), (3), (3a) and (4) shall also be applied mutatis

mutandis to providers of data processing services to facilitate interoperability for the purposes of in-parallel use of data processing services.

2. Article 25 shall also apply mutatis mutandis in relation to data egress charges to facilitate interoperability for the purposes of in-parallel use of data processing services. Data egress charges shall not exceed the costs incurred by the provider of data processing services.

Article 29

Interoperability for data processing services

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

(a) where technically feasible, achieve interoperability 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) facilitate, where technically feasible, functional equivalence between different data processing services referred to in paragraph 1 of Article 26 that cover the same service type;

(ca) shall not adversely impact the security and integrity of services and data;

(cb) be designed in a way to allow for technical advances and inclusion of new functions and innovation in data processing services.

2. Open interoperability specifications and harmonised 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 Annex II of Regulation (EU) No 1025/2012.

4. After taking into account relevant international and European standards and self-regulating initiatives, 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 paragraphs 1 and 2.

4a. The Commission may, by way of implementing acts, adopt common specifications on the basis of open interoperability specifications covering all of the essential requirements set out in paragraphs 1 and 2.

4b. When a Member State considers that a common specification does not entirely satisfy the essential requirements set out in paragraphs 1 and 2, it shall inform the Commission thereof with a detailed explanation. The Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification in question.

5. For the purpose of Article 26(3) , the Commission shall, by way of implementing acts, publish the reference of harmonised standards and common specifications for the interoperability of data processing services in a central Union standards repository for the interoperability of data processing services.

5a. When preparing the draft implementing act establishing the common specifications in accordance with paragraph 4a , the Commission shall take into account the views of the national competent authorities referred to in Article 31(3)(h) and other relevant bodies or expert groups and shall duly consult all relevant stakeholders.

5b. The implementing acts referred to in this Article shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 30

Essential requirements regarding smart contracts for executing data sharing agreements

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 executing an agreement or part of it, to make data available shall ensure that the smart contracts comply with the following essential requirements:

(a) robustness and access control: ensure that the smart contract has been designed to offer access control mechanisms and 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.

(da) consistency with the terms of the data sharing agreement that the smart contract executes.

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 and the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements under paragraph 1 in so far as those standards or parts thereof cover those requirements.

5. The Commission shall, 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.

6. The Commission may, by way of implementing acts, adopt common specifications covering any or all of the essential requirements set out in paragraph 1 where the following conditions have been fulfilled:

(a) the Commission has requested, pursuant to Article 10(1) of Regulation 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the essential requirements set out in paragraph 1 and the request has not been accepted or the European standardisation deliverables addressing that request is not delivered within the deadline set in accordance with article 10(1) of Regulation 1025/2012 or the European standardisation deliverables standard does not comply with the request; and

(b) no reference to harmonised standards covering the relevant essential requirements set out in paragraph 1 is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

6a. Before preparing a draft implementing act in accordance with paragraph 6, the Commission shall inform the committee referred to in Article 22 of Regulation EU (No) 1025/2012 that it considers that the conditions in paragraph 6 are fulfilled.

6b. When preparing the draft implementing act establishing the common specifications in accordance with paragraph 6, the Commission shall take into account the views of the European Data Innovation Board and other relevant bodies or expert groups and shall duly consult all relevant stakeholders.

6c. 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 that meet the common specifications established by one or more implementing acts referred to in paragraph 5 or parts thereof shall be presumed to be in conformity with the essential requirements set out in paragraph 1 covered by those common specifications or parts thereof.

6d Where a harmonised standard is adopted by an European standardisation organisation and proposed to the Commission for the publication of its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal implementing acts referred to in paragraph 5, or parts thereof which cover the same essential requirements set out in paragraph 1.

6e. When a Member State considers that a common specification does not entirely satisfy the essential requirements set out in paragraph 1, it shall inform the Commission thereof with a detailed explanation. The Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification in question.

## CHAPTER IX

## IMPLEMENTATION AND ENFORCEMENT

### Article 31

### Competent authorities and data coordinators

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.

1a. Where a Member State designates more than one competent authority, it shall designate a data coordinator from among them to facilitate cooperation between the competent authorities and to assist the entities in scope of this Regulation on all matters related to its enforcement and implementation. 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.

1b. 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 European Data Protection Supervisor shall be responsible for monitoring the application of this Regulation insofar as it concerns the Commission, the European Central Bank or Union bodies. Where relevant, Article 62 of Regulation (EU) 2018/1725 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to the processing of personal data.

2. Without prejudice to paragraph 1 of this Article:

(b) for specific sectoral data access and use 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 and Article 29 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 data literacy and awareness among users and entities falling within the scope of this Regulation of the rights and obligations under this Regulation;

(b) handling complaints arising from alleged infringements of this Regulation, including in relation to trade secrets, and investigating, to the extent appropriate, the subject matter of the complaint and regularly informing the complainant, where relevant 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 effective, proportionate and 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 and relevant commercial developments of relevance for the making available and use of data;

(f) cooperating with *competent authorities* of other Member States and, where relevant, with the Commission or the European Data Innovation Board, to ensure the consistent and efficient application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay, including with respect to Article 31(7a). Where designated, the data coordinator shall facilitate such cooperation and assist the competent authorities upon their request.

(fa) cooperating with the relevant competent authorities responsible for the implementation of other Union or national legal acts, including with authorities competent in the field of data and electronic communication services, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 or with sectoral authorities to ensure that this Regulation is enforced coherently with other Union and national law. Where designated, the data coordinator shall facilitate such cooperation and assist the competent authorities upon their request.

(h) cooperating with all relevant competent authorities to ensure that the obligations of Chapter VI and Article 29 are enforced consistently with other Union legislation and

self-regulation applicable to providers of data processing services. Where designated, the data coordinator shall facilitate such cooperation and assist the competent authorities upon their request.

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

(ia) examining the requests for data made pursuant to Chapter V.

4. The data coordinator, where such authority has been designated, shall:

(a) ensure the online public availability of requests for access to data made by public sector bodies in the case of public emergencies under Chapter V and promote voluntary data sharing agreements between public sector bodies and data holders;

(b) act as the single point of contact for all issues related to the implementation of this Regulation;

(c) inform the Commission, on an annual basis, of the refusals notified under Article [4(3)(b)] and Article [5(8)(b)].

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 data coordinator 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 impartial and free from any external influence, whether direct or indirect, and shall neither seek nor take instructions for individual cases from any other public authority or any private party.

7. Member States shall ensure that the designated competent authorities are provided with sufficient human and technical resources and relevant expertise to effectively carry out their tasks in accordance with this Regulation.

7a. Entities falling within the scope of this Regulation shall be subject to the competence 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 competence 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.

7b. Any entity falling in scope of this Regulation that offers products or services in the Union, and which is not established in the Union, shall designate a legal representative in one of the Member States.

7c. For the purpose of ensuring compliance with this Regulation, the legal representative shall be mandated by the entity falling in scope of this Regulation that offers products or services in the Union, to be addressed in addition to or instead of it by competent authorities, with regard to all issues related to the entity falling in scope of this Regulation that offers products or services in the Union. The legal representative shall cooperate with and comprehensively demonstrate to the competent authorities, upon request, the actions taken and provisions put in place by the entity falling in scope of this Regulation that offers products or services in the Union, to ensure compliance with this Regulation.

7d. The entity falling in scope of this Regulation that offers products or services in the Union, shall be deemed to be under the jurisdiction of the Member State in which the legal representative is located. The designation of a legal representative by an entity falling in scope of this Regulation that offers products or services in the Union, shall be without prejudice to any legal actions which could be initiated against the entity. Until the entity designates a legal representative in accordance with this Article, it shall be under the competence 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, including by imposing effective, proportionate and dissuasive penalties, provided that the entity is not subject to enforcement proceedings under this Regulation for the same facts by another competent authority.

7f. Competent authorities shall have the power to request from users, data holders, or data recipients, or their legal representatives falling under the competence of their Member State, all the information that is necessary to verify compliance with the requirements of this Regulation. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

7i. Competent authorities under this Article 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 necessary information by electronic means, without undue delay, in particular to carry out the tasks referred to in paragraph (3), points (b), (c) and (d).

7j. 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.

7k. 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.

Article 32

Right to lodge a complaint

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. The data coordinator shall upon request, provide all the necessary information to natural and legal persons for lodging their complaints to the appropriate competent authority.

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 effectively and in a timely manner, 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 32b

Right to an effective judicial remedy

1. Notwithstanding any administrative or other non-judicial remedies, any affected natural and legal persons shall have the right to an effective judicial remedy with regard to legally binding decisions taken by competent authorities.

2. Where a competent authority fails to act on a complaint, any affected natural and legal persons shall, in accordance with national law, either have the right to an effective judicial remedy or access to review by an impartial body with the appropriate expertise.

3. Proceedings pursuant to this Article shall be brought before the courts or tribunals of the Member State of the competent authority against which the judicial remedy is sought individually or, where relevant, collectively by the representatives of one or more natural or legal persons.

4. Where proceedings are brought against a decision of a competent authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

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 recommendations of the European Data Innovation Board and the following non-exhaustive criteria for the imposition of penalties for infringements of this Regulation:

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

(b) any action taken by the infringing party to mitigate or remedy the damage caused by the infringement;

(c) any previous infringements by the infringing party;

(d) the financial benefits gained or losses avoided by the infringing party due to the infringement, insofar as such benefits or losses can be reliably established;

(e) any other aggravating or mitigating factors applicable to the circumstances of the case;

(f) the infringer's annual turnover of the preceeding financial year in the Union.

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. The Commission shall regularly update and maintain an easily accessible public register of those measures.

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, before [date of application of the Regulation], shall recommend non-binding model contractual terms on data access and use, including reasonable compensation and the protection of trade secrets, and non-binding standard contractual clauses for cloud computing contracts to assist parties in drafting and negotiating contracts with fair, reasonable and non-discriminatory 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, in which competent authorities shall be represented, 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:

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

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

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

(iv) 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 96/9/EC

Article 35

Databases containing certain data

The *sui generis* right provided for in Article 7 of Directive 96/9/EC shall not apply when data is obtained from or generated by a product or related service falling within the scope of this Regulation, in particular in relation to Articles 4 and 5.



## 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 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) and 28(2) 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) and 28(2) 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) and 28(2) 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 [ 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.

2a. This Regulation, with the exception of Chapter V, is without prejudice to Union and national law providing for access to and authorising the use of data for scientific research purposes.

Article 41

Evaluation and review

1. 1. By [three 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) Situations to be deemed as exceptional needs for the purpose of Article 15 and the application of Chapter V in practice, in particular the experience in the application of Chapter V by public sector bodies, Union Institutions, agencies and bodies; the number and outcome of the proceedings brought to the competent authority/data coordinator under Art 18(6) on the application of Chapter V, as reported by the competent authorities/data coordinator; the impact of other obligations laid down in Union or national law for the purposes of complying with access to information requests; the impact of voluntary data-sharing mechanisms, such as data altruism organisations recognised under Regulation (EU) 2022/868, on meeting the objectives of Chapter V, and the role of

personal data in the context of Article 15, including the evolution of privacy-enhancing technologies;

(-aa) the impact of this Regulation on the use of data in the economy, including on data innovation, data monetisation practices and data intermediation services, as well as on data sharing within the common European data spaces;

(a) the accessibility and use of different categories and types of data;

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

(ba) the absence of impact on intellectual property rights;

(bb) the impact on trade secrets, including on the protection against their unlawful acquisition, use and disclosure, as well as the impact of the mechanism allowing the data holder to reject the user's request under Article [4 (3b)] and Article [5 (8b)]. This assessment shall, to the possible extent, take into account the revision of Directive (EU) 2016/943.

(bc) whether the list of unfair contractual terms referred to in Article 13 is up-to-date in light of new business practices, given the rapidity of market innovations;

(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.

(ea) the interplay of this Regulation with other Union legal acts of relevance for the data economy.

(ed) the prevention of unlawful governmental access to non-personal data;

(eh) the efficacy of the enforcement regime required under Article 31;

(ej) impacts on micro, small and medium sized enterprises, on their capacity to innovate, on the burden of complying with the new obligations and on the availability of data processing services for European users.

3. Member States shall provide the Commission with the information necessary for the preparation of those reports.

2. By [date of application + 3 years 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 the impact of the provisions outlined in Chapter VI, Article 28a and Article 29, particularly with respect to pricing and diversity of data processing services offered within the Union, with a special focus on SMEs providers.

4. On the basis of those reports, the Commission may, where appropriate, submit a legislative proposal to the Parliament and the Council to amend this Regulation.

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 20 months after [the date of entry into force of this Regulation].

The obligation resulting from Article 3(1) shall apply to products and those services related to them 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. The provisions of Chapter IV shall apply from 2 years from the date of application of this Regulation to contracts concluded on or before the date of application of this Regulation provided that they are:

- of indefinite duration; or

- due to expire at least 10 years after the date of entry into force of this Regulation.

Done at Brussels,

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