C/2023/419

23.11.2023

P9_TA(2023)0069

Data Act

Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (COM(2022)0068 — C9-0051/2022 — 2022/0047(COD)) [1]

(Ordinary legislative procedure: first reading)

Amendment 1

(C/2023/419)

AMENDMENTS BY THE EUROPEAN PARLIAMENT (*)

to the Commission proposal

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

(Data Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

Acting in accordance with the ordinary legislative procedure,

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.

---

[1] The matter was referred back for interinstitutional negotiations to the committee responsible, pursuant to Rule 59(4), fourth subparagraph (A9-0031/2023).

(*) Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol ▌.

[1] OJ C 365, 23.9.2022, p. 18.

[2] OJ C 375, 30.9.2022, p. 112,

(2) ***In a context where the European Union holds a global competitive position in manufacturing and is leader in industrial software and robotics,*** 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, ***the economic value of data sets, the*** costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, bottlenecks impeding data access, a lack of common data sharing practices and abuse of contractual imbalances with regards to data access and use.

(3) In sectors characterised by the presence of micro, small and medium-sized enterprises ***(SMEs)***, 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***, avoid the fragmentation of the internal market that could emerge from national legislation*** 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 accessible data collected, obtained or otherwise*** generated by ***connected*** products or related services, under which conditions and on what basis. Accordingly, Member States should not adopt or maintain additional national requirements on those matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of this Regulation.

(5) This Regulation ensures that ***manufacturers of connected products and providers of related services must design the products and services in a way that*** users of a ***connected*** product or related service in the Union can access, in a timely manner, the data ***accessible from the product or*** generated ***during the provision of a*** 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 ***data recipients*** nominated by the users [redacted] . 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 [redacted] . This Regulation also ensures that data holders make ***data*** available to public sector bodies of the Member States and to Union institutions, agencies or bodies, where there is an exceptional need [redacted] . In addition, this Regulation seeks to facilitate switching between data processing services and to enhance the interoperability of data and data sharing mechanisms and services in the Union. This Regulation should not be interpreted as recognising or creating any legal basis for ***data holders*** to hold, have access to or process data, or as conferring any new right on ***a*** data holder to use data ***accessed from a connected product or*** generated ***during the provision of a*** related service. Instead, it ***recognises that users may agree to grant access and use permissions over data accessed from connected products or generated during the provision of related services to data holders, which may often be manufacturers, and which may contractually agree with the user to perform one or more*** related services.

(6) Data generation is ***a function of the manufacturer's design of a connected product, in particular the inclusion of sensors and processing software within the device,*** of the actions of ***the user and, depending on the operating modalities, of the provision of one or more related service. Many connected products, for example in the civil infrastructure, energy generation or transport sectors, are recording data about their environment or interaction with other elements of that infrastructure without any actions by the user or any third party. Such data may often be non-personal in nature and valuable for*** the user ***or third parties, which may use it to improve their operations, the overall functioning of a network or system or by making it available to others. This*** gives rise to

questions of fairness in the digital economy, because the data ***accessed from connected*** products or ***generated during the provision of*** related services are an important input for aftermarket, ancillary and other services. In order to realise the important economic benefits of data ▌ for the economy and society, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use. ***However, it is also important that data sharing based on voluntary agreements continues to develop in order to facilitate the development of data-driven value growth of European companies.***

(7) The fundamental right to the protection of personal data is safeguarded in particular under ***Regulations*** (EU) 2016/679 ([3]) and ▌ (EU) 2018/1725 ([4]) ***of the European Parliament and of the Council***. Directive 2002/58/EC ***of the European Parliament and of the Council*** ([5]) 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. ***This Regulation should not be read as creating a new legal basis for the processing of personal data for any of the regulated activities, or as amending the information requirements laid down in Regulation (EU) 2016/679. In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data should prevail.***

(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) 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 ([6]), Directive 2011/83/EU of the European Parliament and of the Council ([7]) and Directive 93/13/EEC of the European Parliament and of the Council ([8]).

([3]) ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).***

([4]) ***Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).***

([5]) ***Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).***

([6]) 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).

([7]) 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.

([8]) 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.

(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], the [Proposal for] a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, as well as international cooperation in this context in particular on the basis of the Council of Europe 2001 Convention on Cybercrime ('Budapest Convention'). This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence and national security in accordance with Union law, and activities from customs on risk management and in general, verification of compliance with the Customs Code by economic operators.

(11) Union law setting physical design and data requirements for products to be placed on the Union market should not be affected ***beyond the obligations of Article 3(1) of*** this Regulation.

(12) This Regulation complements and is without prejudice to Union law aiming at setting accessibility requirements on certain products and services, in particular Directive 2019/882 ([9]).

(13) This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence and national security in accordance with Union law, and activities from customs on risk management and in general, verification of compliance with the Customs Code by economic operators.

(13a) This Regulation also aims at strengthening the position and business models of third parties, for example suppliers, through a horizontal approach. To account for the specific situation and complexity of the respective sector, this Regulation should be followed by sectoral legislation, for example the mobility data space. That legislation could set out further rules for the right for suppliers to improved or direct access to data from their own smart components for issues such as quality monitoring, product development or safety improvements and clarifies the role of providers of components in relation to connected products.

(13b) This Regulation is without prejudice to Union and national legal acts providing for the protection of intellectual property rights, including Directives 2001/29/EC ([10]), 2004/48/EC ([11]), and (EU) 2019/790 ([12]) of the European Parliament and of the Council.

(14) Physical products that obtain, generate or collect, by means of their components, 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*** (often referred to as the Internet of Things) should be covered by this Regulation ***with the exception of prototypes***. Electronic communications services include 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, ***ships, aircraft,*** home equipment and consumer goods, medical and health devices or agricultural and industrial machinery ***or energy production and transmission facilities. Data obtained, generated or collected by a connected product that is accessible to any data holders or data recipients*** should ***always*** be accessible to the ***owner of the product, or a third party to whom the owner of the product has transferred certain rights to the product based on a rental or lease contract. The owner or such third party should be referred to as the user for the purpose*** of this

([9]) 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, p. 70).

([10]) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10).

([11]) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004, p. 45).

([12]) Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92).

Regulation. ***Those access rights should in no way alter or interfere with the fundamental rights of data subjects, who may be interacting with connected product, to personal data generated by the product. Manufacturers' design choices, the users' demands and, where relevant, sectoral legislation to address sector-specific needs and objectives, or antitrust decisions, should determine which data a connected product is capable of making accessible to any data holders or data recipients at the point of sale. This Regulation applies to products placed on the market in the Union and thus does not apply to*** products in ***development stage such as prototypes***.

(15) In contrast, ***content, or data obtained, generated or accessed from the connected product or transmitted to it*** for the ***purpose of storage or processing on behalf of third parties, such as in the case of*** servers ***or cloud infrastructure, amongst others for the use by an online service should not be covered by this Regulation***.

(16) It is ***also*** necessary to lay down rules applying to ***related services that are incorporated*** or are interconnected with a ***connected product*** in such a way that the absence of the service would prevent the product from performing ***one or more of*** its functions***, and which involve the transfer of data between the connected product and the provider of the related*** services ***Where a provider of a related service accesses data from a connected product or has access to data generated during the provision*** of the ***related service and has the right to use non-personal data, in accordance with Article 4(6), it should be considered a data holder for the data it accessed from the product or generated during the provision*** of the ***related service. Such related services can be part of the sale***. These related services may themselves generate data of value to the user independently of the data collection capabilities of the ***connected*** product with which they are interconnected. ***Such data may represent the digitalisation of user actions and events and should accordingly be accessible to the user. 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 particular through facilitating the maintenance and repair of the products in question or the development of products or services. Information derived or inferred from non-personal data by a data holder or a data recipient after it has been accessed from the connected product, other than in those generated during the provision of a related service, should not be considered to fall within scope of this Regulation.*** This Regulation should also apply to a related service that is not supplied by the seller, renter or lessor itself, but is supplied, under the sales, rental or lease contract, by a third party. In the event of doubt as to whether the ***provision of a related service is necessary to maintain the functional operation of the connected product,*** supply of service forms 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.***

(17) Data ***accessed from a connected product or*** generated ***during the provision of a*** related service include data recorded intentionally by the user. Such data include also data generated as a by-product of the user's action, such as diagnostics data, and without any action by the user, such as ***data about the connected product's environment or interactions, including*** when the product is in 'standby mode', and data recorded during periods when the product is switched off. Such data should include data in the form and format in which they are ***accessed from*** the product, ***and be compiled in a comprehensible, structured, commonly used and machine-readable format and including the relevant metadata,*** but not pertain to data resulting from ***value-add via a*** software process that calculates derivative data ***where*** such software process ***is*** be subject to ***trade secrets and*** intellectual property rights. ***Where data is accessed in an encrypted format, the user should be provided with all necessary means to decrypt such data and make it accessible.***

(17a) Further efforts must be made to consolidate the data economy and data governance. In particular, increasing and supporting data literacy is essential so that users and businesses are aware and motivated to offer and provide access to their data in compliance with the relevant legal rules. This is on the basis of a sustainable data society. The spread of data literacy measures would imply the reduction of digital inequalities, contribute to improving working conditions, and ultimately sustain the consolidation and the innovation path of the data economy in the Union. In order to deliver high-quality job opportunities, the acquisition and development of data literacy skills, enabling the acquisition of digital competences by citizens and workers, should be ensured especially in the case of employees from start-ups and SMEs.

(18) The user of a ***connected*** product should be understood as the legal or natural person, such as a business***, consumer or public sector body*** which has ***acquired the connected product or receives related services, or to whom the owner of the connected*** product ***has transferred,*** on the ***basis of a rental or lease agreement, temporary rights to use the connected product or receive related services.*** Such a user bears the risks and enjoys the benefits of using the connected product and should ▌ therefore be entitled to derive benefit from data ***accessed from the connected*** product and ***generated during the provision of*** any related service.

(18a) 'Data literacy' refers to skills, knowledge and understanding that allows users, consumers and businesses, in particular medium, small and micro companies, to gain awareness on the potential value of the data they generated, produce and share, in the context of their rights and obligations set out in this Regulation and in other Union data related Regulations. Data literacy should go beyond learning about tools and technologies and aiming to equip citizens and businesses with the ability to benefit from a fair data market. It is therefore necessary that the Commission and the Member States, in cooperation with all relevant stakeholders, promote the development of data literacy, in all sectors of society, for citizens of all ages, including women and girls. Consequently, the Union and its Member states should allocate more investments in education and training to spread data literacy, and that progress in that regard is closely followed Accordingly businesses should also promote tools and take measures to ensure data literacy skills of their staff dealing with data access and use and data transfers, and where applicable, of other persons processing data on their behalf, taking into account their technical knowledge, experience, education and training and considering the users or groups of users from which data is produced or generated.

(19) In practice, not all data generated by ***connected*** 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 often able to determine, through their control of the technical design of the product or related services, what data are generated and how they can be accessed, even though they have no legal right to the data. It is therefore necessary to ensure that ***connected*** products are designed and manufactured and related services are provided in such a manner that data generated by their use are always easily accessible to the user***, free of charge in a comprehensive, structured, commonly used and machine-readable format, including for the purpose of retrieving, using or sharing the data. Unless specified otherwise by Union or Member State law or relevant antitrust rulings, such data should be accessible at the level of processing, including by means of software contained in the connected product, which the manufacturer's design choice permit ahead of the sale to the user. Data should be available in the form in which they are accessible from the product with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data. This requires the removal of technical barriers to ensure that users, where it is technically possible, will have direct real-time access to their data without extensive individual verification procedures. In order to facilitate third-party access to the required data, cost-efficient access to software tools is also necessary. 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 should be communicated to the user in the context of the update or alteration. This Regulation does not set an obligation to store data additionally on the central computing unit of a product where this would be disproportionate in relation to the expected use. This does not prevent a manufacturer or data holder to voluntarily agree with the user on making such adaptation***.

(20) In ***cases of co-ownership of the connected product and related services provided, where*** several persons or entities own a product or are party to a lease or rent agreement ▌ the design of the ***connected*** product or related service or the relevant interface ***should enable*** all persons ***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. ***For identification and authentication purposes, manufacturers and providers of related services should enable users to use European Digital Identity Wallets issued pursuant to Regulation (EU) 910/2014*** ([13]). 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. Access should be granted to the user upon simple request mechanisms granting automatic execution, not requiring examination or clearance by ***a*** 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. ***User accounts should enable users to revoke consent for processing and data sharing, as well as request deletion of the data generated through the use of the connected product, particularly in cases when the users of the product intend to transfer the ownership of the product to another party.***

(21) Products may be designed to make certain data directly available 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***. 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***. They may be designed to permit the user or a third party to process the data on the product or on a computing instance of the manufacturer.

(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 physical objects 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 home services. Such virtual assistants should be covered by the data access right provided for in this Regulation also regarding data recorded before the virtual assistant's activation by the wake word and data generated when a user interacts with a ***connected*** product via a virtual assistant provided by an entity other than the manufacturer of the ***connected*** product ▌.

(23) Before concluding a contract for the purchase ***of a connected product, clear and sufficient information should be provided by the manufacturer, or where relevant the vendor, to the user with regard to the data which is accessible from the connected*** product***, including the type, format, sampling frequency and the estimated volume of accessible data. This should include information on data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, as well as information*** on how the data ▌ may be ***stored, retrieved or*** accessed***, including the provision of software development kits or application programming interfaces, along with their terms of use and quality of service descriptions***. This obligation provides transparency over the ***accessible*** data generated and enhances the easy access for the user***. The transparency obligation could be fulfilled by a data holder for example by, maintaining a stable uniform resource locator (URL) on the web, which can be distributed as a web link or QR code, pointing to the relevant information. Such URL could be provided by the manufacturer or where relevant seller, to the user before concluding the contract for the purchase, of a***

([13]) ***Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).***

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. 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.

(23a) Related services should be provided in such a manner that data generated during their provision, which represent the digitalisation of user actions or events, are, by default, easily, securely and, where relevant and technically feasible, directly accessible to the user free of charge, in a structured, commonly used and machine-readable format, along with the relevant metadata necessary to interpret and use it. Information derived or inferred from this data by means of complex proprietary algorithms, in particular where it combines the output of multiple sensors in the connected product, should not be considered within the scope of a data holder's obligation to share data with users or data recipients, unless agreed differently. Before concluding an agreement with a user on the provision of a related service, which involves the provider's access to data from the connected product, in line with Article 4(6) of this Regulation, the provider should agree with the user on the nature, volume, collection frequency and format of data accessed by the provider of related services from the connected product, as well as the nature and estimated volume of data generated during the provision of the related service and, where relevant, the modalities for the user to access or retrieve such data, including the period during which it should be stored.

(24) This Regulation imposes the obligation on data holders to make data available in certain circumstances. Insofar as personal data are processed, ***a*** data holder should be a controller under Regulation (EU) 2016/679. Where users are data subjects, data holders should be obliged to provide them access to their data and to make the data available to third parties of the user's choice in accordance with this Regulation. However, this Regulation does not create a legal basis under Regulation (EU) 2016/679 for ***data holders*** to provide access to personal data or make it available to a third party when requested by a user that is not a data subject and should not be understood as conferring any new right on ***data holders*** to use data ***accessed from the connected product or*** generated ***during the provision of a*** related service. This applies in particular where the manufacturer is ***a*** data holder. In that case, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user. This agreement may be part of the sale ***agreement relating to the connected product. The user should be given a reasonable opportunity to reject this*** agreement***. If a user choses to reject the contractual terms and conditions, this should not prevent the user from using the relevant*** product ***of the service, unless the product of the service cannot function without the user's acceptance of the contractual terms***. Any contractual term in the agreement stipulating that ***a*** data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which ***a*** data holder intends to use the data. This Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by ***a*** 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 ***a*** data holder on well-defined public policy grounds.

(24a) 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 ([14]). 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

([14]) Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1).

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. In order to protect the incentives for users to monetise non-personal data from connected products they own, data holders should only be able to monetise aggregated data sets from multiple users and should not make available non-personal data accessed by them from the connected product to third parties for commercial or non-commercial purposes, other than the fulfilment of their contractual obligations to the user. At the same time, where data holders have contractually agreed with users the right to use such data, they should be free to use it for a wide range of purposes, including improving the functioning of the connected product or related services, developing new products or services or enriching or manipulating it or aggregating it with other data, including with the aim of making available the resulting data set with third parties, as long as such derived data set does not allow the identification of the specific data items accessed by the data holder from the connected product, or allow a third party to derive those data items from the data set without a significant effort.

(24b) Where products generate data, that is derived or inferred from other data generated by the connected product by means of proprietary, complex algorithms, including those that are a part of proprietary software, within the meaning of Directive 2009/24/EC of the European Parliament and of the Council ([15]), such data should be considered to fall outside 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 should include in particular information derived by means of sensor fusion, inferring or deriving data from multiple sensors, collected in the connected product, using complex, proprietary algorithms. However, data inferred or derived from processing of raw 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, pH, liquid level, position, acceleration or speed, should be included in the obligation for data holders to make data available to users and data recipients. Sectorial legislation should further define accessible data based on the specificities of the sector.

(24c) In principle, 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. Ahead of sharing data, a user should be able to share data with a high degree of certainty that they will not face adverse legal consequence after the data has been shared. Therefore, where data is excluded from a data holder's obligation to make it available to users or data recipients, the scope of such data should be specified in the contractual agreement between the user and the data holder for the provision of a related service in a comprehensible and clear format, in a way that users can easily determine which data is available for them for sharing with data recipients or third parties without further obligations to protect such data.

(24d) There are many reasons why certain data generated by the use of a product remain inaccessible to a data holder and consequently would not fall under the sharing obligations of chapter II. Data may be highly volatile (values recorded at high frequency) and either instantly or quickly overwritten. They may be collected only for activating a very specific function, such as the activity of windshield wipers or headlights, and there is currently no use case and the design of the product does not foresee such data to be stored in the product in light of the cost related to

([15]) Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (OJ L 111, 5.5.2009, p. 16).

storage of such data, to connecting the data-capturing sensor to a central computing component from which data could be exported and the costs of connectivity for transmitting the data when volumes are considerable. In this regard, sector-specific regulations should further specify relevancy of accessible data according to their specificities in order to ensure the availability of at least data, which is essential for the repairing or servicing of the connected products and related services.

(25) In sectors characterised by the concentration of a small number of manufacturers ***or providers of related services*** supplying end users, ***the ability of users to bargain for access to data transferred by the connected product or generated during the provision of related services is limited due to the bargaining power of the manufacturer or provider of related service***. In such circumstances, contractual agreements may be insufficient to achieve the objective of user empowerment. The data tends to remain under the control of the manufacturers ***or providers of related services***, making it difficult for users to obtain value from the data generated by the equipment they ***own***. 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***, security concerns*** and objectives. Furthermore, ***data holders*** should not use any data ***accessed by them from the connected product or generated during the provision of*** related ***services*** 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 ***connected products*** or related service generating data, ***EU consumer law applies, Directive 2005/29/EC, which applies against unfair commercial practices, 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 ▌ 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 ***data recipient*** 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 also be valid regardless of whether the request is put forward by the user or an authorised third party acting on user's behalf, such as authorised data intermediation service in the meaning of the Regulation (EU) 2022/868. Data holders*** should ensure that the data made available to ***a data recipient*** 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 trade secrets or intellectual property rights should be ***fully*** 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 in this context include reverse engineering, when allowed pursuant to Directive (EU) 2016/943 of the European Parliament and of the Council [16] as a lawful means of independent discovery of know-how or information, provided that it does not lead to unfair competition and it is without prejudice of the obligation not to develop a competing product using the data received under this Regulation. This may be the case for the purposes of repairing, prolonging the lifetime of a product or providing aftermarket services to connected products when the manufacturer or provider of related services has ended their production or provision.***

(28a) ***This Regulation should be interpreted in a manner to preserve the protection awarded to trade secrets under Directive (EU) 2016/943. To that end, 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. Trade secrets should be identified prior to the disclosure. However, data holders cannot undermine the right of the users to request access and use of data in accordance with this Regulation on the basis of certain data being considered as trade secrets by the data holder. The data holder, or the trade secret holder where it is not the data holder, 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 cases where 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 suspend the sharing of data identified as trade secrets, pending review by the data coordinator of the Member State. In such cases, the data holder should immediately notify the data coordinator of the Member State in which the data holder is established, pursuant to Article 31 of this Regulation, that it has suspended the sharing of data and identify which measures have not been implemented or which trade secrets have had their confidentiality undermined. Where the user, or a third party of the user's choice, wishes to challenge the data holder's decision to suspend the sharing of data, the data coordinator should decide, within a reasonable period of time, whether the data sharing should be resumed or not and if yes, indicate under which conditions. The Commission, assisted by the European Data Innovation Board, should develop model contractual terms, and should be able to develop technical standards. The Commission, assisted by the European Innovation Board, could also encourage the establishment of codes of conduct in relation with the respect of trade secrets or intellectual property rights in handling the data, in order to help achieving the aim of this Regulation.***

(29) A ***data recipient*** to whom data is made available may be ***a natural or legal person,*** enterprise, a research organisation or a not-for-profit organisation ***or an intermediary, including data intermediation services or data altruism organisations as defined in Regulation (EU) 2022/868***. In making the data available to ***a data recipient, data holders*** should not abuse ***their*** position to seek a competitive advantage in markets where ***a*** data holder and ***data recipient*** may be in direct competition. ***Data holders*** should not therefore use any data ***accessed from the connected product or generated during the provision of a*** related service in order to derive insights about the economic situation of the third party or its assets or production methods or the use in any other way that could undermine the commercial position of the third party on the markets it is active on. ***The user should have the right 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, data recipients should be able to transfer the data access rights granted by the user to third parties, including in exchange for compensation. Data intermediation services [as regulated by Regulation (EU) 2022/868] may support users or data recipients in establishing a commercial relation for any lawful purpose on the basis of data 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.***

---

[16] ***Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).***

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

(31) Data ***accessed from a connected product or*** generated ***during the provision of a*** related service should only be made available to a third party at the request of the user. This Regulation accordingly complements the right provided under Article 20 of Regulation (EU) 2016/679. That Article provides for a right of data subjects to receive personal data concerning them in a structured, commonly used and machine-readable format, and to port those data to other controllers, where those data are processed on the basis of Article 6(1), point (a), or Article 9(2), point (a), or of a contract pursuant to Article 6(1), point (b). Data subjects also have the right to have the personal data transmitted directly from one controller to another, but only where technically feasible. Article 20 specifies that it pertains to data provided by the data subject but does not specify whether this necessitates active behaviour on the side of the data subject or whether it also applies to situations where a product or related service by its design observes the behaviour of a data subject or other information in relation to a data subject in a passive manner. The right under this Regulation complements the right to receive and port personal data under Article 20 of Regulation (EU) 2016/679 in several ways. It grants users the right to access and make available to a ***data recipient*** to any data ***accessed from the connected product or*** generated ***during the provision of a*** related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike the technical obligations provided for in Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of data coming within its scope, whether personal or non-personal. It also allows ***data holders*** to set reasonable compensation to be met by ***data recipients***, but not by the user, for any cost incurred in providing direct access to the data generated by the user's product. If a data holder and third party are unable to agree terms for such direct access, the data subject should be in no way prevented from exercising the rights contained in Regulation (EU) 2016/679, including the right to data portability, by seeking remedies in accordance with that Regulation. It is to be understood in this context that, in accordance with Regulation (EU) 2016/679, a contractual agreement does not allow for the processing of special categories of personal data by ***data holders or data recipient***.

(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

([17]) OJ L 303, 28.11.2018, p. 59.

the transmission of a communication). Directive 2002/58/EC ('ePrivacy Directive') (and the proposed ePrivacy Regulation) protect the integrity of the user's terminal equipment as regards the use of processing and storage capabilities and the collection of information. Internet of Things equipment is considered terminal equipment if it is directly or indirectly connected to a public communications network.

(33) In order to prevent the exploitation of users, ***data recipients*** 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 ***not*** share it with another third party ***without unequivocally informing the user in a timely manner and having its explicit agreement to such sharing***.

(34) ***Data recipients*** should only access additional information that is necessary for the provision of the service requested by the user. Having received access to data, the ***data recipient*** should process it exclusively for the purposes agreed with the user, without interference from the data holder. It should be as easy for the user to refuse or discontinue access by the ***data recipient*** to the data as it is for the user to authorise access. ***A data recipient or data holder*** 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, ***or*** by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface ***or a part thereof, including its structure, design, function or manner of operation*** 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, ***including*** the requirements set out in Directive 2005/29/EC, Directive 2011/83/EU, Directive 2000/31/EC and Directive 98/6/EC.

(35) ***Data holders and data recipients*** should also refrain from using the data to profile individuals unless these processing activities are strictly necessary to provide the service requested by the user. The requirement to delete ***personal*** data when no longer required for the purpose agreed with the user complements the right to erasure of the data subject pursuant to Article 17 of Regulation ***(EU)*** 2016/679. Where ***a data recipient*** 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, ***SMEs*** and companies from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This Regulation aims to facilitate access to data for these entities, while ensuring that the corresponding obligations are scoped as proportionately as possible to avoid overreach. At the same time, a small number of very large companies have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. These companies include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and whom existing or new market operators are unable to challenge or contest. The ***Regulation (EU) 2022/1925 of the European Parliament and of the Council*** ***([18])*** aims to redress these inefficiencies and imbalances by allowing the Commission to designate a provider as a 'gatekeeper', and imposes a number of obligations on such designated gatekeepers, including a prohibition to combine certain data without consent, and an obligation to ensure effective rights to data portability under Article 20 of Regulation (EU) 2016/679. Consistent with the ▌ Regulation ***(EU) 2022/1925***, and given the unrivalled ability of these companies to acquire data, it would

([18]) ***Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). (OJ L 265, 12.10.2022, p. 1)***

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. This means that an undertaking providing core platform services that has been designated as a gatekeeper cannot request or be granted access to users' data generated by the use of a product or related service or by a virtual assistant based on the provisions of Chapter II of this Regulation. An undertaking providing core platform services designated as a gatekeeper pursuant to ***Regulation (EU) 2022/1925*** should be understood to include all legal entities of a group of companies where one legal entity provides a core platform service. Furthermore, third parties to whom data are made available at the request of the user may not make the data available to a designated gatekeeper. For instance, the third party may not sub-contract the service provision to a gatekeeper. However, this does not prevent third parties from using data processing services offered by a designated gatekeeper. This exclusion of designated gatekeepers from the scope of the access right under this Regulation does not prevent these companies from obtaining data through other lawful means.

(37) ***Micro and small enterprises should be excluded from the*** obligations ***of Chapter II***. 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 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.

(38) This Regulation contains ▌ rules, 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.

(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.

(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 for making the data available should not discriminate 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. ***The Commission, while involving all affected stakeholders, should establish practical guidelines on what constitutes non-discriminatory terms.*** 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, this Regulation contains the principle that ***data holders*** may request reasonable compensation when legally obliged to make data available to the data recipient ***in business- to business relations***. These provisions should not be understood as paying for the data itself, but ***to allow data holders to be reasonably compensated for making data available or,*** in the case of ***micro, small or medium-sized enterprises and of research organisations using the data on a not-for-profit basis***, for the ***direct*** costs incurred and investment required for making the data available. ***The Commission should develop guidance detailing what qualifies as a reasonable compensation in the data economy.***

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

(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 compensation for making data available to be paid by them should not exceed the direct cost of making the data available and be non-discriminatory. ***The same regime should apply to those research organisations that use the data on a not-for-profit basis.***

(45) Direct costs for making data available are the costs necessary for data reproduction, dissemination via electronic means and storage but not of data collection or production. Direct costs for making data available should be limited to the share attributable to the individual requests, taking into account that the necessary technical interfaces or related software and connectivity will have to be set up permanently by the data holder. Long-term arrangements between data holders and data recipients, for instance via a subscription model, could reduce the costs linked to making the data available in regular or repetitive transactions in a business relationship. ***The data holder, if not an SME, should actively provide the calculation showing that his price is a cost-based, when he knows, or should have known, that his counterparty is an SME. In any case, he should state that he is obliged to make the data available to an SME at cost price and that he is obliged to make detailed information available when requested.***

(46) It is not necessary to intervene in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company. In such cases, the companies are considered capable of negotiating any compensation if it is reasonable, taking into account factors such as the volume, format, nature, or supply of and demand for the data as well as the costs for collecting and making the data available to the data recipient. ***In the case of misuse or disclosure of data, the data recipient should be liable for the damages to the party suffering from it and should comply without undue delay with the requests of the data holder.***

(47) Transparency is an important principle to ensure that the compensation requested by ***a*** data holder is reasonable, or, ***if*** the data recipient is ***an SME***, 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.

(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.

(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.***

(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 enterprises*** without a meaningful ability to negotiate the conditions for access to data, who may have no other choice than to accept 'take-it-or-leave-it' contractual terms. Therefore, unfair contract terms regulating the access to and use of data or the liability and remedies for the breach or the termination of data related obligations should not be binding on micro, small or medium-sized enterprises when they have been unilaterally imposed on them.

(52) Rules on contractual terms should take into account the principle of contractual freedom as an essential concept in business-to-business relationships. ▌. 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. ***All contractual agreements should be in line with Fair, Reasonable and Non-Discriminatory (FRAND) principles.***

(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 ▌ continue to apply.

(55) 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.

(56) In situations of exceptional need, it may be necessary for public sector bodies or Union institutions, agencies or bodies to use data held by an enterprise ***or that it is currently collecting or has previously obtained, collected or otherwise generated and which it retains at the time of the request,*** to respond to public emergencies or in other

exceptional cases. Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law. To limit the burden on businesses, micro and small enterprises should be exempted from the obligation to provide public sector bodies and Union institutions, agencies or bodies data in situations of exceptional need.

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

(58) An exceptional need may also ***stem from non-emergency situations*** when a public sector body can demonstrate that the data are necessary ***for the fulfilment of*** a specific task in the public interest that has been explicitly provided ***and defined by national law, such as preventing or assisting the recovery from a public emergency. Such a request can be made only*** when the ▌ public sector body or the Union institution, agency or body ***has identified specific data which is unavailable and only if it has exhausted all of the following three*** alternative means ***to obtain data: requesting*** the data ***through voluntary agreements; purchasing the data on the market or by relying on existing*** obligations ***to make data available***.

(59) This Regulation should not apply to, nor pre-empt, voluntary arrangements for the exchange of ***non-personal*** data between private and public entities. ▌ 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.

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

(61) A proportionate, limited and predictable framework at Union level is necessary 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 ***based on Union or national law, 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 ***and an appropriate coordination***, data requests made by public sector bodies and by Union institutions, agencies or bodies should be ***communicated*** without undue delay by the entity requesting the data ***to the data coordinator of that Member State that will ensure that those request are to be included in an*** online public ***available list*** of all requests justified by ***an exceptional need***.

(62) The objective of the obligation to provide the data is to ensure that public sector bodies and Union institutions, agencies or bodies have the necessary knowledge to respond to, prevent or recover from public emergencies or to maintain the capacity to fulfil specific tasks explicitly provided by law. The data obtained by those entities may be commercially sensitive. Therefore, ***Regulation (EU) 2022/868, as well as*** Directive (EU) 2019/1024 of the European Parliament and of the Council ([19]) should not apply to data made available under this Regulation and should not be considered as open data available for reuse by third parties. This however should not affect the applicability of Directive (EU) 2019/1024 to the reuse of official statistics for the production of which data obtained pursuant to this Regulation was used, provided the reuse does not include the underlying data. In addition, it should not affect the possibility of sharing the data for conducting research or for the compilation of official statistics, provided the conditions laid down in this Regulation are met. ***Where allowed by Union or national law, public*** sector bodies should also be allowed to exchange data obtained pursuant to this Regulation with other public sector bodies to address the exceptional needs for which the data has been requested. ***provided that the data holder is informed in a timely manner and all bodies respect the same rules on transparency as the original requester of the data and protection of trade secrets and intellectual property rights is ensured.***

(63) Data holders should have the possibility to either ask for a modification of the request made by a public sector body or Union institution, agency and body or its cancellation in a period of 5 or 15 working days depending on the nature of the exceptional need invoked in the request. In case of requests motivated by a public emergency, justified reason not to make the data available should exist if it can be shown that the request is similar or identical to a previously submitted request for the same purpose by another public sector body or by another Union institution, agency or body ***or if the data holder is not currently collecting or has not previously collected, obtained or otherwise generated the requested data and does not retain it at the time of the request***. 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 ([20]) apply in relation to the requested datasets, data holders should exercise their rights in a way that does not prevent the public sector body and Union institutions, agencies or bodies from obtaining the data, or from sharing it, in accordance with this Regulation.

▌

(65) Data made available to public sector bodies and to Union institutions, agencies and bodies on the basis of exceptional need should only be used for the purpose for which they were requested ▌. The data should be destroyed once it is no longer necessary for the purpose stated in the request, unless agreed otherwise, and the data holder should be informed thereof. ***Public sector bodies and to Union institutions, agencies and bodies should ensure, including through the application of proportionate security measures, where applicable in accordance with Union and national law, that any protected nature of data is preserved and unauthorised access is avoided.***

(66) When reusing data provided by data holders, public sector bodies and Union institutions, agencies or bodies should respect both existing applicable legislation and contractual obligations to which the data holder is subject. Where the disclosure of trade secrets of the data holder to public sector bodies or to Union institutions, agencies or bodies is strictly necessary to fulfil the purpose for which the data has been requested, confidentiality of such disclosure should be ensured ***in advance*** to the data holder ***or the trade secret holder, including as appropriate, by the use of model contractual clauses, technical standards and the application of codes of conduct. In cases where the public sector body or the Union institutions, agency or body or the third parties that received the data to perform the task that have been outsourced to it, fail to implement those measures or undermine the confidentiality of trade secrets, the data holder should be able to suspend the sharing of data identified as trade secrets. Such a decision to***

([19]) 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).

([20]) 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).

suspend the sharing of data might be challenged by the public sector body or the Union institutions, agency or body or the third parties to which data were transmitted and subject to review by the data coordinator of the Member State.

(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 ***provided that the request is limited in time and scope, proportionate to the state of the public emergency***. Public emergencies are rare events and not all such emergencies require the use of data held by enterprises. The business activities of the data holders are therefore not likely to be negatively affected as a consequence of the public sector bodies or Union institutions, agencies or bodies having recourse to this Regulation. However, as cases of an exceptional need other than responding to a public emergency might be more frequent, including cases of prevention of or recovery from a public emergency, data holders should in such cases be entitled to a reasonable compensation***. This Regulation*** should not ***affect existing Union or national arrangements in which data is shared free of charge, or prevent*** public sector ***bodies,*** Union ***institutions, agencies or bodies, and data holders from entering into voluntary data sharing agreements free of charge***.

(68) The public sector body or Union institution, agency or body may share the data it has obtained pursuant to the request with other entities or persons when this is needed to carry out scientific research activities or analytical activities it cannot perform itself ***provided that those activities are strictly necessary to respond to the emergency need. 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 compilation 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 ***or public*** undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, which could result in preferential access to the results of the research, should not be considered research organisations for the purposes of this Regulation.

(69) The ability for customers of data processing services, including cloud and edge services, to switch from one data processing service to another, while ***avoiding downtime of services, or to use the services of several providers simultaneously without undue data transfer costs***, is a key condition for a more competitive market with lower entry barriers for new service providers***, and for ensuring further resilience for the users of those services. Guarantees for effective switching should also include customers benefiting from large-scale free-tier offerings, so that does not result in a lock-in situation for customers. 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)***.

(69a) Switching charges are charges imposed by providers of cloud computing 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 that wishes to switch. Examples of common switching charges are costs related to the transfer of data from one provider to the other or to an on-premise system ('egress fees') or the costs incurred for specific support actions during the switching process. Unnecessarily high egress fees and other unjustified charges unrelated to actual switching costs, inhibit customers' 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. As a result of the new obligations foreseen in this Regulation, the source provider of data processing services might outsource certain tasks and renumerate third party entities in order to comply with those obligations. The customer should not bare 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. Nothing in the Data Act prevents a customer to remunerate third party entities for support in the migration process. Egress fees are charged to customers by providers of source data processing services when the customers are willing to take their data out

from a cloud provider's network to an external location, especially when switching from one provider to one or several providers of destination, to relocate their data from one location to another while using the same cloud service provider. Therefore, in order to foster competition, the gradual withdrawal of the charges associated with switching data processing services should specifically include withdrawing egress fees charged by the data processing service to a customer.

(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 contractual, ***commercial, organisational,*** economic and technical barriers***, which are not limited*** to ***an impeded 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 ***deployment models of data processing services should include private and public cloud. Such services and deployment models should be the same as defined by international standards. 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. ***Digital services considered as an online platform as defined in point (i) of Article 3 of [the Digital Services Act] and an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128 of the European Parliament and of the Council ([21]) should not be considered as 'data processing services' within the meaning of this Regulation.***

(71a) 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. Three base cloud delivery models are further completed by emerging variations, each

([21]) Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market (OJ L 168, 30.6.2017, p. 1).

comprised of a distinct combination of IT resources, such as Storage-as-a-Service and Database-as-a-Service. For the purpose of this Regulation, data processing services can be categorised in more granular and a non-exhaustive multiplicity of different 'equivalent services', 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 operational characteristics. In an example two databases might appear to share the same primary objective, but after considering their data processing model, distribution model and targeted use-case, such databases should fall into a more granular subcategory of equivalent services. Equivalent services may have different and competing characteristics such as performance, security, resilience, and quality of service.

(71b) Extracting the data that belongs to the customer from the source provider of data processing services remains one of the challenges that impedes restoration of the service functionalities in the destination provider infrastructure. In order to properly plan the exit strategy, avoid unnecessary and burdensome tasks and to ensure that the customer does not lose any of its data as a consequence of the switching process, the source provider of data processing services should include in the contract the mandatory information on the scope of the data that can be exported by the customer once he or she decides to switch to a different service, other provider of data processing services or move to on-premise ICT infrastructure. The scope of exportable data should include at a minimum input and output data, including relevant data formats, data structures and metadata directly or indirectly generated or co-generated by the customer's use of the data processing service, and that can be clearly assigned to the customer. The exportable data should exclude any data processing service, or third party's assets or data protected by intellectual property rights or constituting a trade secret or confidential information, such as data related to the integrity and security of the service provided by the data processing service, and should also exclude data used by the provider to operate, maintain and improve the service.

(72) This Regulation aims to facilitate switching between data processing services, which encompasses all ***relevant*** conditions and actions that are necessary for a customer to terminate a contractual agreement of a data processing service, to conclude one or multiple new contracts with different providers of data processing services, to port all its digital assets, including data, to the concerned other providers and to continue to use them in the new environment ***and benefit*** from functional equivalence. ***It should be noted that the data processing services in scope are those where the data processing service, as defined under this Regulation, forms part of the core business of a provider.*** Digital assets refer to elements in digital format for which the customer has the right of use, including data, applications, virtual machines and other manifestations of virtualisation technologies, such as containers. ***Switching is a customer-driven operation consisting in three main steps, namely (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 right 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 cloud computing 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 to extract 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. Obstacles to switching are of a different nature, depending on which step of the switching process is referred to.*** Functional equivalence means the ***possibility to re-establish, on the basis of the customer's data,*** 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 comparable outcome in response to the same input for shared functionality supplied to the customer under the contractual agreement. Different*** services ***may only achieve functional equivalence for the shared core functionalities, where both the source and destination service providers independently offer*** the same ***core functionalities. This Regulation does not instance an obligation of facilitating functional equivalence for data processing*** service ***delivery models of the PaaS or SaaS. Relevant*** meta-data, generated by the customer's use of a service, should also be portable pursuant to this Regulation's

provisions on switching ***and falls within the definition of exportable data. 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***.

(72a) An ambitious and innovation inspiring regulatory approach to interoperability is needed, in order to overcome vendor lock-in, which undermines competition and the development of new services. Interoperability between equivalent 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 ***not to impose and to remove all relevant obstacles and*** to offer all assistance and support ***within their capacity and proportional to their respective obligations*** that is required to make the switching process successful***, safe*** and effective***. 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 has no access and insights into the environment of the destination provider of data processing services and should not be obliged to rebuilt customer's service, according to functional equivalence requirements, 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. The information to be provided by providers of data processing services to the customer should*** support ***the development of the customer's exit strategy and should include procedures for initiating switching from the cloud computing service, the machine-readable data formats that the user's data can be exported to, the tools, including at least one open standard data portability interface, 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. The written contract setting out the rights of the customer and the obligations of the provider of cloud computing services should only cover information which is available to the provider of data processing services at the time of the formation of the contract***. 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 ([22]) should not be affected. ***Any mandatory period under this Regulation should not affect compliance with other timelines specified under sectoral legislation. 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.***

(75) To facilitate switching between data processing services, providers of data processing services should consider the use of implementation and/or compliance tools, notably those published by the Commission in the form of a Rulebook relating to cloud services. In particular, standard contractual clauses are beneficial to increase confidence in data processing services, to create a more balanced relationship between users and ***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 developed by relevant bodies or expert groups established under Union law.

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

(75a) In order to facilitate switching between cloud computing 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.

(75b) Data processing services which concern services that are substantially altered to facilitate a specific customer's need (custom built), or data processing services that operate on a trial basis or only supply a testing and evaluation service for business product offerings, should be exempted from some of the obligations applicable to data processing service switching.

(75c) Without prejudice to their right to take action before a court, customers should have access to certified dispute settlement bodies to settle disputes related to switching between providers of data processing services.

(76) Open interoperability ***and portability*** specifications and standards developed in accordance with paragraph 3 and 4 of Annex II ***to*** Regulation (EU) 1025/2012 ***of the European Parliament and of the Council ([23])*** in the field of interoperability and portability enable a ▌ multi-vendor cloud environment, which is a key requirement for open innovation in the European data economy. As market-driven processes have not demonstrated the capacity to establish technical specifications or standards that facilitate effective cloud interoperability ***and portability*** at the PaaS ▌ and SaaS ▌ levels, the Commission should be able, ***where technically feasible,*** 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 equivalent 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 ***and portability*** specifications. ***Following consultation with stakeholders and taking into account relevant international and European standards and self-regulatory initiatives,*** the Commission, by way of delegated acts, can mandate the use of European standards for interoperability ***and portability*** or open interoperability ***and portability*** specifications for specific ***equivalent services*** 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 for interoperability and portability specifications, taking into account the nature, security and integrity of the data they host.*** European standards ***for the interoperability and portability 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.

(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

([23]) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

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 ***consumer*** whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality.

(78) To foster further trust in the data, it is important that safeguards in relation to Union citizens, the public sector and businesses are implemented to the extent possible to ensure control over their data. In addition, Union law, values and standards should be upheld in terms of (but not limited to) security, data protection and privacy, and consumer protection. In order to prevent unlawful access to non-personal data, 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***, semantic and syntactic*** interoperability should play a key role to provide technical solutions to ***enable portability and*** interoperability. In order to facilitate the conformity with the requirements for interoperability ***within the common European data spaces which are purpose- or sector-specific or cross-sectoral, interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives should be developed. This Regulation lays down certain essential requirements for interoperability. Participants within the data spaces, which are entities facilitating or engaging in data sharing within the common European data spaces, including data holders, should comply with those requirements. Compliance with those rules can occur by adhering to the requirements laid down in this Regulation, or by adapting to already existing standards via a presumption of conformity. In order to facilitate the conformity with the requirements for interoperability***, it is necessary to provide for a presumption of conformity for interoperability solutions that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 ***. Standards should be developed in open, technology neutral and inclusive way line with Chapter II of the Regulation (EU) No 1025/2012. Taking into account, where relevant, positions adopted by the European Data Innovation Board according to Article 30, point (f), of Regulation (EU) 2022/868,*** the Commission should adopt common specifications in areas where no harmonised standards exist or where they are insufficient in order to further enhance interoperability for the common European data spaces, application programming interfaces, cloud switching as well as smart contracts. Additionally, common specifications in the different sectors could remain to be adopted, in accordance with Union or national sectoral law, based on the specific needs of those sectors. Reusable data structures and models (in form of core vocabularies), ontologies, metadata application profile, reference data in the form of core vocabulary, taxonomies, code lists, authority tables, thesauri ***could*** also be part of the technical specifications for semantic interoperability. Furthermore, ***following consultation with stakeholders and taking into account relevant international and European standards and self-regulating initiatives, where relevant, positions adopted by the European Data Innovation Board, as referred to in Article 30, point (f), of Regulation (EU) 2022/868,*** the Commission should be enabled to ***adopt common specifications in areas where no harmonised standards exist and to*** mandate the development of harmonised standards for the ***portability and*** interoperability of data processing services. ***The European Data Innovation Board should build on existing European and global initiatives for cross-sectoral interoperability of data. In particular, the European Data Innovation Board should study the potential of the digital identity of objects framework as established by the Regulation (EU) 910/2014 and systems for the identification of legal entities such as the GLEIF for that purpose.***

(79a) In order to further enhance coordination in the enforcement of this Regulation, the European Data Innovation Board should foster the mutual exchange of information amongst competent authorities as well as advise and assist the Commission in matters falling under this Regulation that fall within the competences of Article 30 of Regulation (EU) 2022/868. A subgroup for stakeholder involvement referred to in Article 29(2), point (c), of that Regulation should participate in the consultation on a continual basis.

(80) To promote the interoperability of smart contracts in data sharing applications, it ***may be*** necessary to lay down essential requirements for smart contracts for professionals who create smart contracts for others or integrate such smart contracts in applications that support the implementation of agreements for sharing data. ***For example,*** smart contracts ***should guarantee that conditions for data sharing are respected. Specific training programmes on*** smart contracts ***for businesses, in particular SMEs, should be promoted***.

(81) In order to ensure the efficient implementation of this Regulation, Member States should designate one or more competent authorities ***and assign to them sufficient resources***. If a Member State designates more than one competent authority, it should also designate a coordinating competent authority. Competent authorities should cooperate with each other ***effectively and in a timely manner, in line with the principles of good administration and mutual assistance to ensure the effective implementation and enforcement of 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. ***Competent authorities should cooperate upon request of the authorities within the European Data Protection Board and the European Data Innovation Board.***

(81a) In order to further enhance coordination in the enforcement of this Regulation, the European Data Innovation Board should foster the mutual exchange of information amongst competent authorities as well as advise and assist the Commission in matters falling under this Regulation with a focus on the matters falling under the competences of the Board in line with Article 30 of Regulation (EU) No 2022/868.

(82) In order to enforce their rights under this Regulation, natural and legal persons should be entitled to seek redress for the infringements of their rights under this Regulation by lodging complaints with ***the data coordinator, other relevant*** competent authorities ***and before the Courts***. 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 ([24]) and Directive (EU) 2020/1828 of the European Parliament and of the Council ([25]).

(83) Member States competent authorities should ensure that infringements of the obligations laid down in this Regulation are sanctioned by penalties. 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 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.

([24]) 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).

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

(84) In order to eliminate the risk that holders of ***databases containing data*** obtained or generated by means of physical components, such as sensors, of a connected product and a related service***, namely machine-generated data,*** claim the sui generis right under Article 7 of Directive 96/9/EC***, this Regulation clarifies that*** the sui generis right ***does not apply to such databases as the requirements for protection of a substantial investment in either the obtaining, verification or presentation of the data as provided for in Article 7(1) of Directive 96/9/EC would not be fulfilled. 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 and to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 ([26]). 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 ([27]).

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

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

([26]) OJ L 123, 12.5.2016, p. 1.
([27]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(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 ***18 months*** after entry into force of the Regulation. ***Only where the data holder and the manufacturer are the same entity the obligations related to the provision of related services provided for the connected products already placed in the market within the last five years from the entry into force of this Regulation should apply retroactively. Such obligations should be fulfilled, only when the provider of related services is able to remotely deploy mechanisms to ensure the fulfilment of the requirements pursuant to Article 1 and only when the deployment of such mechanisms would not place a disproportionate burden on the manufacturer.***

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

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Regulation lays down harmonised rules on:

(a) the design of connected products to allow access to data generated by a connected product or generated during the provision of related services to the user of that product;

(b) data holders making available data they accessed from a connected product or generated during the provision of a related service to data subjects, users or to data recipients, at the request of the user or data subject;

(c) fair contractual terms for data sharing agreements;

(d) the making available of data to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need in the public interest;

(e) facilitating switching between data processing services;

(f) introducing safeguards against unlawful international governmental access to non-personal data; and

(g) providing for the development of interoperability standards and common specifications for data to be 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 accessible data obtained, collected or otherwise generated by connected products or generated during the provision of related services;

(b) Chapter III applies to any private sector data subject to statutory data sharing obligations;

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

(d) Chapter V applies to any private sector 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 and*** users of such ***connected*** products or ***related*** services ***or in the case of personal data, identified or identifiable natural persons the data obtained, collected, or generated by the use, relates to***;

(b) ***users of connected products or related services in the Union and*** data holders***, irrespective of their place of establishment,*** that make data available to data recipients in the Union ***or in the case of personal data, identified or identifiable natural persons the data obtained, collected, or generated by the use, relates to***;

(c) data recipients in the Union to whom data are made available;

(d) public sector bodies ***of a Member State*** and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a ***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,*** offering such services to customers in the Union.

3. Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to ***any*** personal data processed in connection with the rights and obligations laid down in this Regulation. ***The obtaining, collection, or generation of personal data through the use of a product or related service shall require a legal basis pursuant to applicable data protection law.*** This Regulation ***does not constitute a legal basis for the processing of personal data. This Regulation is without prejudice to*** Union law on the protection of personal data ***and privacy***, in particular Regulation (EU) 2016/679***, Regulation (EU) 2018/1725,*** and Directive 2002/58/EC, including the ***rules concerning the*** powers and competences of supervisory authorities. ***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.*** Insofar as the rights laid down in Chapter II of this Regulation are concerned, and where users are the data subjects of personal data, subject to the rights and obligations under that Chapter, the provisions of this Regulation shall complement ***and particularise*** the right of data portability under Article 20 of Regulation (EU) 2016/679. ***No provision of this Regulation shall 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.***

4. 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 ***or administrative*** offences or the execution of criminal ***or administrative*** penalties, including Regulation (EU) 2021/784 of the European Parliament and of the Council ([28]) and the [e-evidence proposals [COM(2018) 225 and 226] once adopted, and international cooperation in that area. This Regulation shall not affect the collection, sharing, access to and use of data under Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing and Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying the transfer of funds. This Regulation shall not affect the competences of the Member States regarding activities concerning public security, defence, national security, customs and tax administration and the ***public*** health and ***the*** safety of citizens in accordance with Union law. ***This Regulation shall not apply to data collected or generated in the context of defence-related activities or by defence products or services or by products or services deployed and used for defence purposes.***

4a. 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.

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

4b. Data holders shall not be obliged to provide access to data to any natural or legal person, entity or body outside the Union, unless requested by the user or otherwise provided by the Union law or national law implementing the Union law.

4c. The obligations set out in the Regulation shall not preclude voluntary lawful reciprocal non personal data sharing between users, data holders and data recipients, agreed in contracts.

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording; ***content, or data obtained, generated or collected by the connected product or transmitted to it on behalf of others for the purpose of storage or processing, shall not be covered by this Regulation.***

(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 defined in Article 4, point (1), of Regulation (EU) 2016/679;

(1e) 'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and has a right to use that data for commercial or non-commercial purposes;

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

(3) 'related service' means a digital service, including software ***, but excluding electronic communication services which is*** inter-connected with a product in such a way that its absence would prevent the product from performing one ***or more*** of its functions***, and which involves accessing data from the connected product by the provider or the service***;

(4) 'virtual assistants' means software that can process demands, tasks or questions including ***those*** based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access ***to other*** services or control ***the functions of products***;

(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 receives a related service or to whom the owner of a connected product has transferred, on the basis of a rental or leasing agreement, temporary rights to use a connected*** product or ***receive related*** services ***and, where the connected product or related service involves the processing of personal data, the data subject***;

(6) 'data holder' means a legal or natural person, who has ***accessed data from the connected product or has generated data during the provision of a related service and who has the contractually agreed right to use such data, and the obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law*** to make available certain data ***to the user or a data recipient***;

(7) 'data recipient' means a legal or natural person ▌ other than the user of a ***connected*** product or related service, to whom ***a*** data holder makes ***available data accessed from a connected product or generated during the provision of a related service*** following ***an explicit*** request by the user ▌ 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 and officially declared according to the relevant procedures under Union or national law***;

(10a) 'official statistics' means 'European statistics' within the meaning of Regulation (EC) No 223/2009 ([29]);

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

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

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

(14) 'functional equivalence' means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract;

(15) 'open ***standards', mean*** technical specifications, ▌ which are performance oriented towards achieving interoperability between data processing services ***and which are adopted through an inclusive, collaborative, consensus-based and transparent process from which materially affected and interested parties cannot be excluded***;

▌

(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;

([29]) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

(19) 'interoperability' means the ability of two or more ***data-based serviced, including*** data spaces or communication networks, systems, products, applications or components to ***process,*** exchange and use data in order to perform their functions ***in an accurate, effective and consistent manner***;

(19a) 'portability' means the ability of a customer to move imported or directly generated data that can be clearly assigned to the customer between their own system and cloud services, and between cloud services of different cloud service providers;

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

(20a) 'common European data spaces' means purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives;

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

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

(20d) 'data altruism' means the voluntary sharing of data as defined in Article 2(16)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' should be understood as per Article 2, point (2) of Directive (EU) 2016/943.

CHAPTER II

BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING

Article 3

Obligation to make data ***accessed from connected products or*** generated ***during the provision of*** related services accessible ***to the user.***

1. ***Connected*** products shall be designed and manufactured ***in such a manner that data they collect, generate or otherwise obtain, which are accessible to data holders or data recipients*** are, by default ***free of charge to the user, and*** easily, securely and, where relevant and ***technically feasible***, directly accessible to ***it, in a comprehensive, structured, commonly used and machine-readable format. Data shall be available in the form in which they have been collected, obtained or generated by the connected product, along with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data. Information derived or inferred from this data by means of complex proprietary algorithms, in particular where it combines the output of multiple sensors in the connected product, shall not be considered within the scope of a data holder's obligation to share data with users or data recipients unless agreed differently between*** the user ***and the data holder. In case that user is a data subject, connected products shall offer possibilities to directly exercise the data subjects' rights, where technically feasible. Connected products shall be designed and manufactured in such a way that a data subject, irrespective of their legal title over the connected product, is offered the possibility to use the products covered by this Regulation in the least privacy-invasive way possible. The requirements set out in the first subparagraph shall be met without inhibiting the functionality of the connected product and related services and in accordance with data security requirements as laid down by Union law***.

1a. Data holders may reject a request for data if access to the data is prohibited by Union or national law.

2. Before concluding a contract for the purchase ***of a connected product, the manufacturer, or where relevant the vendor, shall provide*** at least the following information ▌ to the user, in a ***simple manner and in a*** clear and comprehensible format:

(a) the ***type of data, format, sampling frequency, the in-device storage capacity, and the estimated*** volume of ***accessible data which the connected product is capable of collecting, generating or otherwise obtaining***;

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

(ba) whether data will be stored on-device or on a remote server, including the period during which it shall be stored;

(c) how the user may access ***free of charge, and, where relevant, retrieve and request the deletion of*** those data;

(ca) The technical means to access the data, such as Software Development Kits or application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable the development of such means of access;

(cb) Whether a data holder is the holder of trade secrets or other intellectual property rights contained in the data likely to be accessed from the connected product or generated during the provision of related service, and, if not, the identity of the trade secret holder, such as its trading name and the geographical address at which it is established.

▌

2a. Related services shall be provided in such a manner that data generated during their provision, which represent the digitalisation of user actions or events, are free of charge to the user and, by default, easily, securely and, where relevant and technically feasible, directly accessible to the user in a structured, commonly used and machine-readable format, along with the relevant metadata necessary to interpret and use it.

2b. Before the user concludes an agreement with a provider of related services, which involves the provider's access to data from the connected product during the provision of such services, in line with Article 4(6) of this Regulation, the agreement shall address:

(a) the nature, volume, collection frequency and format of data accessed by the provider of related services from the connected product and, where relevant, the modalities for the user to access or retrieve such data, including the period during which it shall be stored;

(b) the nature and estimated volume of data generated during the provision of the related service, as well as modalities for the user to access or retrieve such data;

(c) granular, meaningful consent options for data processing, within the meaning of Article 4(11) of Regulation (EU) 2016/679;

(d) whether the service provider providing the related service, in its role as data holder, intends to use the data accessed from the connected product itself or allow one or more third parties to use the data for purposes agreed upon with the user;

(e) the trading name of the provider of the related service, its legal entity identifier, contact details and the geographical address at which it is established; and where applicable, other data processing parties;

(f) where relevant, the means of communication which enable the user to contact the provider quickly and communicate with its staff efficiently;

(g) how the user may request that the data are shared with a data recipient, and, where relevant, withdraw the consent for data sharing;

(h) Whether a data holder is the holder of trade secrets or other intellectual property rights contained in the data likely to be accessed from the connected product or generated during the provision of related service, and, if not, the identity of the trade secret holder, such as its trading name, legal identity identifier and the geographical address at which it is established;

(i) how the user is able to manage permissions to allow the use of data, where possible with granular permission options, and including the option to withdraw permissions to a data holder for the use of the user's data, to the third parties nominated by a data holder, or to exclude geographical addresses;

(j) the duration of the agreement between the user and the provider of the related service, as well as the modalities to terminate such an agreement prematurely; as well as the minimal period for which the related service is guaranteed to receive security and functionality updates;

(k) the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the data coordinator referred to in Article 31.

Article 3a

Data Literacy

1. When implementing this Regulation, the Union and the Member States shall promote measures and tools for the development of data literacy, across sectors and taking into account the different needs of groups of users, consumers and businesses, including through education and training, skilling and reskilling programmes and while ensuring a proper gender and age balance, in view of allowing a fair data society and market.

Article 4

The ***rights and obligations*** of users ***and data holders*** to access***, use and make available data accessed from connected products or*** generated ***during the provision of*** related services

1. Where data cannot be directly accessed by the user from the product, ***data holders*** shall make available to the user ***any data accessed by them from a connected*** product or ***generated during the provision of a*** related service without undue delay, ***easily, securely, in a comprehensive, structured, commonly used and machine-readable format,*** free of charge and, where ***relevant and technically feasible***, continuously and in real-time***, including making any personal data derived from such data available to a data subject pursuant to Article 15 of Regulation (EU) 2016/679, accompanied with relevant metadata. Data shall be provided in the form in which they have been accessed from the connected product or generated by the related service, with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data. Information derived or inferred from this data by means of complex proprietary algorithms, in particular where it combines the output of multiple sensors in the connected product,*** shall ***not be considered within the scope of a data holder's obligation to share data with users or data recipients, unless agreed differently between the user and the data holder. Any data access request to a data holder should*** be done on the basis of a simple request through electronic means where technically feasible ***and, where appropriate, indicate the type, nature or scope of data requested***.

1a. Data holders may reject a request for data if access to the data is prohibited by Union or national law;

1b. Users and data holders may agree contractually on restricting or prohibiting the access, use of or further sharing of data, which could undermine security of the product as laid down by law. Each party may refer the case to the data coordinator, to assess whether such restriction is justified, in particular in light of serious adverse effect on the health, safety or security of human beings. Sectoral competent authorities will be given the possibility to provide technical expertise in this context.

1c. Where in compliance with all the provisions established within this Regulation, and the terms and conditions agreed in the contractual agreement between the parties, a data holder shall not be liable towards the user for any damage arising from data made available, provided that the data holder has processed the data lawfully in accordance with Union and national law and has complied with relevant cybersecurity requirements and where applicable, with the technical and organisational measures to preserve the confidentiality of the shared data. When complying with this

Regulation, a user, who lawfully makes available data accessed from the connected product or received following a request under Article 4 paragraph 1 to a third party, or a data recipient, who is lawfully sharing data made available to it by a data holder, to a third party, shall not be liable for damage arising from sharing such data, provided that the user or data recipient have processed the data in accordance with Union and national laws and have complied with relevant cybersecurity requirement and where applicable, with the technical and organisational measures to preserve the confidentiality of the shared data.

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

2. ***Data holders*** shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. ***Data holders*** shall not keep any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure. ***Where identification is legally requires, data holders shall enable the possibility for users to identify and authenticate through the European Digital Identity Wallets, pursuant to Regulation (EU) No 910/2014.***

3. Trade secrets shall ***be preserved and shall*** only be disclosed provided that all specific necessary measures ***pursuant to Directive (EU) 2016/943*** are taken ***in advance*** to preserve ***their*** confidentiality, in particular with respect to third parties. The data holder ***or the trade secret holder if it is not simultaneously the data holder, shall identify the data which are protected as trade secrets and*** can agree ***with the user any technical and organisational*** measures to preserve the confidentiality of the shared data, in particular in relation to third parties***, as well as on liability provisions. Such technical and organisational measures include, as appropriate, model contractual terms, confidential agreements, strict access protocols, technical standards and the application of codes of conduct. In cases where the user fails to implement those measures or undermines the confidentiality of trade secrets, the data holder shall be able to suspend the sharing of data identified as trade secrets. In such cases, the data holder must immediately notify the data coordinator of the Member State in which the data holder is established, pursuant to Article 31 of this Regulation, that it has suspended the sharing of data and identify which measures have not been implemented or which trade secrets have had their confidentiality undermined. Where the user wishes to challenge the data holder's decision to suspend the sharing of data, the data coordinator shall decide, within a reasonable period of time, whether the data sharing shall be resumed or not and if yes, indicate under which conditions***.

4. The user shall not use ▌ data obtained pursuant to a request referred to in paragraph 1 to develop a product that ***directly*** competes with the product, from which the data originate ***and shall not use such data to derive insights about the economic situation, assets and production methods of the manufacturer***.

4a. The user 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.

4b. Users have the right to either directly share, through a data holder or through providers of data intermediation services as set in the Regulation (EU) 2022/868, non-personal data accessed from the connected product or obtained pursuant to a request referred in paragraph 1 to any data recipient for commercial or non-commercial purposes. The data sharing between a user and a data recipient shall be carried out by means of contractual agreements; the provisions of Chapter IV on fair, reasonable and non-discriminatory terms shall apply mutatis mutandis to the contractual agreements between users and data recipients.

5. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where ***all conditions and rules provided by the applicable data protection law are complied with, in particular where*** there is a valid legal basis under Article ***6*** of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 ***and Article 5(3) of Directive 2002/58/EC*** are fulfilled.

6. ***Data holders*** shall only use any non-personal data ***accessed from a connected product or*** generated ***during the provision of a*** related service on the basis of a contractual agreement with the user. The data holder shall not ***make the use of the product or related service dependent on the user allowing it to process data not required for the functionality of the product or provision of the related service. The data holder shall delete the data when they are no longer necessary for the purpose contractually agreed. Data holders and the users shall not*** use such data ***obtained, collected or*** generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use ***of the product or related service*** by the ***other party*** that could undermine the commercial position of the ***other party*** in the markets in which the user is active.

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

6b. Where the contractual agreement between the user and a data holder allows for the use of non personal data accessed by them from the connected product, referred to in point (a) of Article 3(2a), the data holder shall be able to use that data for any of the following purposes:

(a) improving the functioning of the connected product or related services;

(b) developing new products or services;

(c) enriching or manipulating it or aggregating it with other data, including with the aim of making available the resulting data set to third parties, as long as such derived data set does not allow the identification of the specific data items transmitted to the data holder from the connected product, or allow a third party to derive those data items from the data set.

6c. Users, in business-to- business relations, have the right to make data available to data recipients or data holders under any lawful contractual condition, including by agreeing to limit or restrict further sharing of such data, and to be compensated proportionately in exchange for foregoing their right to use or share such data lawfully. Data recipients or data holders shall not make the offer of a related service, or its commercial terms, including pricing, contingent on such agreement by the user, or coerce, deceive or manipulate in any other way the user to make available data under such contractual conditions.

Article 5

Right ***of the user*** to share data with third parties

1. Upon request by a user, or by a party acting on behalf of a user, ***such as an authorised data intermediation service in the meaning of the Regulation (EU) 2022/868, data holders*** shall make available the data ***accessed by them from a connected*** product or ***generated during the provision of a*** related service to a third party, without undue delay, ***easily, securely, in a comprehensive, structured, commonly used and machine-readable format,*** free of charge to the user, of the same quality as is available to the data holder and, where ***relevant and technically feasible*** continuously and in real-time. ***Where the user is a data subject, personal data shall be processed for purposes specified by the data subject, such as the following:***

(a) the provision of after-market services, such as the maintenance and repair of the product, including after-market services in competition with a connected product or service provided by a data holder;

(b) enabling the user to update the software of the connected product or related services in particular to fix security and usability problems;

(c) specific data intermediation services recognised in the Union or specific services provided by data altruism organisations recognised in the Union under the conditions and requirements of Chapters III and IV of Regulation (EU) 2022/868.

Data shall be provided in the form in which they have accessed from the product, with only the minimal adaptations necessary to make them useable by a third party, including related metadata necessary to interpret and use the data. Information derived or inferred from this data by means of complex proprietary algorithms, in particular where it combines the output of multiple sensors in the connected product, shall not be considered within the scope of a data holder's obligation to share data with users or data recipients, unless agreed differently between the user and the data holder.

1a. The right under paragraph 1 shall not apply to data resulting from the use of a product or related service in the context of testing of other new products, substances or processes that are not yet placed on the market unless use by a third party is permitted by the agreement with the enterprise with whom the user agreed to use one of its products for testing of other new products, substances or processes.

2. Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper, pursuant to Article […] of ▌ Regulation ***(EU) 2022/1925***, shall not be an eligible ***data recipient*** under this Article and therefore shall not:

(a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1);

(b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;

(c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).

3. The user or ***the data recipient*** shall not be required to provide any information beyond what is necessary to verify the quality as user or as ***data recipient*** pursuant to paragraph 1. ***Data holders*** shall not keep any information on the ***data recipient***'s access to the data requested beyond what is necessary for the sound execution of the ***data recipient***'s access request and for the security and the maintenance of the data infrastructure.

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

5. The data holder shall not use any non-personal data ***obtained, collected or*** generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has ***expressly*** consented to such use and has the technical possibility to ***easily*** withdraw that consent at any time.

6. ***In the case of*** a data subject ***who is not the user requesting access***, any personal data ***obtained, collected, or*** generated by ***their*** use of a product or related service***, and data derived and inferred from that use,*** shall only be made available ***by the data holder to the third party*** where there is a valid legal basis under Article ***6*** of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 ***and Article 5(3) of Directive 2002/58/EC*** are fulfilled.

7. Any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation.

8. Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose ***of the request*** agreed between the user and the third party and all specific necessary measures agreed between the data holder***, or between the trade secrets holder if it is not simultaneously the data holder,*** and the third party are taken ***prior to the disclosure*** by the third party to preserve the confidentiality of the trade secret. In such a case, the ***data holder or the trade secret holder, shall identify*** the data ***which are protected*** as trade secrets and the ***technical and organisational***

measures for preserving ***their*** confidentiality***, as well as on liability provisions. Such technical and organisational measures*** shall be specified in the agreement between the data ***or trade secret*** holder and the third party***, including, as appropriate through model contractual terms, strict access protocols, confidential agreements, technical standards and the application of codes of conduct. In cases where the third party fails to implement those measures or undermines the confidentiality of trade secrets, the data holder shall be able to suspend the sharing of data identified as trade secrets. In such cases, the data holder must immediately notify the data coordinator of the Member State in which the data holder is established, pursuant to Article 31, that it has suspended the sharing of data and identify which measures have not been implemented or which trade secrets have had their confidentiality undermined. Where the third party wishes to challenge the data holder's decision to suspend the sharing of data, the data coordinator shall decide, within a reasonable period of time, whether the data sharing shall be resumed or not and if yes, indicate under which conditions***.

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

Article 6

Obligations of ***data recipients*** receiving data at the request of the user

1. A ***data recipient*** shall process ▌ data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and ***where all conditions and rules provided by the applicable data protection law are complied with, notably where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 and Article 5(3) of Directive 2002/58/EC are fulfilled, and*** subject to the rights of the data subject insofar as personal data are concerned***. The data recipient*** shall delete the data when they are no longer necessary for the agreed purpose***, unless otherwise agreed with the user***.

2. The ***data recipient*** shall not:

(a) ***make the exercise of the rights or choices of users unduly difficult including by offering choices to the users in a non-neutral manner, or*** coerce, deceive or manipulate the user in any way, ***or*** by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user ***or a part thereof, including its structure, design, function or manner of operation***;

(b) use the data it receives for the profiling of natural persons within the meaning of Article ***4, point (4),*** of Regulation (EU) 2016/679, ***other than in accordance with that Regulation***;

(c) make the data ▌ it receives ***available*** to another third party ***without making the user aware in a clear and easily accessible way and seeking its the explicit contractual permission*** by the user;

(d) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article ***3 of [Regulation (EU) 2022/1925*** (Digital Markets Act)];

(e) use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose; ***data recipients shall also not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the data holder that could undermine the commercial position of the data holder on the markets in which the data holder is active;***

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

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

(ec) use the data to disrupt sensitive critical infrastructure protection information within the meaning of Article 2(d) of Directive 2008/114/EC.

▌

2a. The third party shall bear the responsibility to ensure the security and protection of the data it receives from a data holder.

Article 7

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

1. The obligations of this Chapter shall not apply to ▌ 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***.

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

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 a*** data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing 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 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 data sharing*** 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 ***holds reasonable doubt that*** 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 with the evidence demonstrating*** that there has been no discrimination.

▌

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

5a. Data holders and data recipients shall take all necessary legal, organisational and technical measures to ensure the security and integrity of the data transfers.

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

Article 9

Compensation for making data available

1. Any compensation agreed between a data holder and a data recipient for making data available ***in business- to-business relations*** shall be ***non — discriminatory and*** reasonable. ***A data holder, a data recipient or a third party shall not directly or indirectly charge consumers or data subjects a fee, compensation or costs for sharing data or accessing it.***

2. Where the data recipient is a ***non- profit research organisation or a SME***, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, ***provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC and do not qualify as an SME,*** any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly. ***In case of an SME, the data holder shall actively inform of the obligation to provide the data preferably on the basis of a cost-based model.***

2a. The Commission shall develop guidelines to determine criteria for categories of costs related to making data available, which shall be the basis for awarding compensation pursuant to paragraph 1.

3. This Article shall not preclude other Union law or national legislation implementing Union law from excluding compensation for making data available or providing for lower compensation.

4. The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can verify that the requirements of paragraph 1 and, where applicable, paragraph 2 are met.

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 ***fulfilment of the data holder's obligation to make data available to the data recipient, upon the request of the user,*** the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available in accordance with Articles 8***, 9 and 13***.

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

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

(b) it has the necessary expertise in relation to the determination of fair, reasonable and non-discriminatory terms 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 ***Member State where the body is established.***

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

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

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

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

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

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

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

(a) the number of disputes received;

(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. The data holder may apply appropriate technical protection measures, including smart contracts ***and encryption***, to prevent unauthorised ***disclosure of and*** access to the data***, including metadata,*** and to ensure compliance with Articles ***4, 5, 6, 8,*** 9 and 10, 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). ***Where a user or data holder provides tangible relevant evidence for unlawful use or unauthorised disclosure to a third party by the data recipient, the data recipient shall, upon request of the user or data holder, provide information on how the data has been used, or with whom it has been shared.***

2. ***Where*** a data recipient that has, for the purposes of obtaining data, provided ▌ false information to the data holder, deployed deceptive or coercive means or abused evident gaps in the technical infrastructure of the data holder designed to protect the data, has used the data made available for unauthorised purposes***, including the development of a competing product within the meaning of Article 6 (2) (e)*** or has ***unlawfully*** disclosed ▌ data to another party, the data ***recipient shall be liable for the damages to the party suffering from the misuse or disclosure of such data and*** shall ***comply*** without undue delay ***with the requests of*** the data holder or the ***trade secret holder when they are not the same legal person to***:

(a) ***erase*** the data made available ▌ and any copies thereof;

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

(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.

(bb) notify the data holder about the disclosure of such data.

2a. The user shall enjoy the same prerogatives as the data holder, and the data recipient, the same obligation as those stated in paragraph 2 when the data recipient has infringed Article 6 (2) (a) and (b).

▌

Article 12

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

1. This Chapter shall apply where a data holder is obliged under Article 5, or under Union law or national legislation implementing 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 ***be void.***

2a. Any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects, undermines the application of their rights to privacy and data protection, derogates from it, or varies its effect, shall be void.

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

CHAPTER IV

UNFAIR TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES

Article 13

Unfair contractual terms unilaterally imposed on a ▌ 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***, the data recipient or user respectively,*** if it is unfair.

1a. A contractual term is not to be considered unfair where it arises from applicable Union law.

2. A contractual term is unfair if it is of such a nature that ***objectively impairs the ability of the party upon whom the term has been unilaterally imposed to protect its legitimate commercial interest in the data in question or*** its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing. ***or creates a significant imbalance between the rights and the obligations of the parties in the contract.***

3. A contractual term is unfair for the purposes of this Article 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 this Article 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;

(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***, including when such data contains commercially sensitive data or are protected by trade secrets or by intellectual property rights, without the prior consent of the relevant parties***;

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

(ca) impose the unilateral choice of the competent jurisdiction or the payment of the cost related to the procedure;

(cb) prevent the party upon whom the term has been unilaterally imposed for 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 substantially vary the upfront price payable under the contract, or any other substantial condition on the data to be shared, without the right of the other party to terminate the contract, or*** enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so.

5. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied 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 contractual term bears the burden of proving that that term has not been unilaterally imposed.

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

6a. The party that supplied the contested term may not argue that the term is an unfair term.

7. This Article does not apply to contractual terms defining the main subject matter of the contract ***and shall not affect the parties' ability to negotiate*** the price to be paid.

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.

8a. This Article shall apply to all new contracts entered into after … [date of entry into force of this Regulation. Businesses shall be given three-years following that date to review existing contractual obligations that are subject to this Regulation.

8b. Given the rapidity in which innovations occur in the markets, the list of unfair contractual terms within Article 13 shall be reviewed regularly by the Commission and be updated to new business practices if necessary.

CHAPTER V

MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES AND UNION INSTITUTIONS, AGENCIES OR BODIES BASED ON EXCEPTIONAL NEED

Article 14

Obligation to make data available based on exceptional need

1. Upon ***a specified duly justified*** request ***limited in time and scope***, a data holder ***that is a legal person*** shall make ***non-personal data which are available at the time of the request, including metadata*** available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.

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

2a. This Chapter shall not preclude voluntary arrangements between businesses and public sector bodies and union institutions, agencies or bodies for the sharing of data for purpose of delivering public services, including for exceptional needs if stipulated in their contracts.

Article 15

Exceptional need to use data ▌

An exceptional need to use ***non-personal*** data within the meaning of this Chapter shall be ***limited in time and scope and shall be*** deemed to exist in ▌ the following circumstances:

(a) where the data requested is necessary to respond to ▌ public emergency;

(b) ***in non-emergency situations,*** where the ***public sector body or Union institution, agency or body is acting on the basis of Union or national law and has identified specific data, which is unavailable to it and which is*** necessary to ***fulfil, a specific task in the*** public ***interest that has been explicitly provided by law such as the prevention or*** recovery from a public emergency ***and which the public sector body or Union institution, agency or body has been unable to obtain by any of the following means: voluntary agreement***; ***by purchasing the data on the market or by relying on existing obligations to make data available.***

▌

Article 15a

Single point to handle public sector bodies' request

1. The data coordinator designated pursuant to Article 31 shall be responsible for coordinating the requests pursuant Article 14(1) from the sector bodies of the Member State concerned, in order to ensure that the requests meet the requirement laid down in this Chapter and shall transmit them to the data holder. It shall avoid multiple requests by different public sector bodies within their territory to the same data holder.

2. Member States shall regularly inform the Commission about requests pursuant to Article 14(1).

3. Where public sector bodies or Union institutions, agencies or bodies requires data from the same data holder in more than one Member State on the basis of an exceptional need pursuant Article 14(1), the competent authorities of the Member States shall cooperate in accordance with Article 22 to coordinate their requests where it is necessary to minimise the administrative burden on the data holders.

4. The Commission shall develop a model template for requests pursuant to Article 17.

Article 16

Relationship with other obligations to make data available to public sector bodies and Union institutions, agencies and bodies ▌

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

2. ▌ This Chapter shall not ***apply to*** public sector bodies and Union institutions, agencies and bodies ***that*** carry 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.

2a. Enterprises that fall within the scope of this Chapter shall inform their users of the possibility that data may be shared in the case of exceptional circumstances.

Article 17

Requests for data to be made available

1. ***In a request for*** data pursuant to Article 14(1), a public sector body or a Union institution, agency or body shall:

(a) ***request data within their remit and*** specify what ***datasets*** are required;

(b) demonstrate the exceptional need for which the data are requested ***and compliance with the conditions mentioned in Article 15***;

(c) explain the purpose of the request, the intended use of the data requested, and the duration of that use;

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

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

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

(cd) disclose the identity of the third party referred to in paragraph 4 of this Article, and in Article 21 of this Regulation;

(ce) apply all relevant ICT security measures concerning the transfer and storage of data;

(d) state the legal basis for requesting the data;

(da) specify the geographical limits that apply to the request for data;

(e) specify the deadline by which the data are to be made available ***and*** within which the data holder may request the public sector body, Union institution, agency or body to modify or withdraw the request;

(ea) submit a declaration on the lawful and secure handling of the data requested, including the confidentiality of trade secrets;

(eb) ensure that making the data available does not put the data holder in a situation that violates Union or national law or confer liability on the data holder for any infringement or damage resulting from the data access that a public sector body or a Union institution, agency or body has requested.

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

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

(aa) be submitted through the competent authority;

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

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

(c) respect the legitimate aims of the data holder, taking into account the protection of trade secrets and the cost and effort required to make the data available***. Where applicable, specify the measures to be taken pursuant to Article 19 (2) to preserve the confidentiality of trade secrets, including, as appropriate, through the use of model contractual terms, technical standards and codes of conduct***;

(d) concern ***only*** non-personal data;

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

(f) ***be transmitted to the data coordinator referred to in Article 31, who shall make the request*** publicly available online without undue delay; ***the data coordinator may inform the public sector body or Union institution, agency or body if the data holder already provided the requested data in response to previously submitted request for the same purpose by another public sector body or Union institution agency or body.***

3. A public sector body or a Union institution, agency or body shall not make data obtained pursuant to this Chapter available for reuse within the meaning of Directive (EU) 2019/1024 ***and Regulation (EU) 2022/868***. Directive (EU) 2019/1024 ***and Regulation (EU) 2022/868*** shall not apply to the data held by public sector bodies obtained pursuant to this Chapter.

4. Paragraph 3 does not preclude a public sector body or a Union institution, agency or body to exchange data obtained pursuant to this Chapter with another public sector body, Union institution, agency or body, ***for the purpose*** of completing the tasks in Article 15 ***which was included the request in accordance with paragraph 1(cc),*** or to make the data available to a third party in cases where it has outsourced, by means of a publicly available agreement, technical inspections or other functions to this third party. ***It shall bind the third party contractually not to use the data for any other purposes and not to share is with any other third parties, Where a public sector body or a Union institution, agency or body transmits or makes data available under this paragraph, it shall notify the data holder from whom the data was received without undue delay. Within five working days of that notification, the data holder shall have the right to submit a reasoned objection to such transmission or making available of data. In the case of a rejection of the reasoned objection by the public sector body or a Union institution, agency or body, the data holder may bring the matter to the data coordinator referred to in Article 31. The receiving*** public sector bodies, Union institutions, agencies or bodies ***and third parties shall be bound by the obligations laid down in*** Article 19 ▌ .

Data obtained pursuant this chapter shall be used only for the purpose specified in the request. Public sector bodies, Union institutions, agencies or bodies shall bind contractually third parties with whom they agreed to share data pursuant paragraph 4 not to use the data for any other purpose and not to share it with other parties.

Article 18

Compliance with requests for data

1. A data holder receiving a request for access to data under this Chapter shall make the data available to the requesting public sector body or a Union institution, agency or body without undue delay***, taking into account provision of time and necessary technical, organisational and legal measures***.

2. Without prejudice to specific needs regarding the availability of data defined in sectoral legislation, the data holder may decline or seek the modification of the request within ***five*** working days following the receipt of a request for the data necessary to respond to a public emergency and within ***30*** working days in other cases of exceptional need, on either of the following grounds:

(a) the data is ***not available to the data holder at the time of the request***;

(aa) provided security measures concerning transfer, storing and maintaining confidentiality are insufficient;

(ab) a similar request for the same purpose has been previously submitted by another public sector body or Union institution, agency or body and the data holder has not been notified of the destruction of the data pursuant to Article 19(1) point (c);

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

▌

4. If the data holder decides to decline the request or to seek its modification in accordance with paragraph 3, it shall indicate the identity of the public sector body or Union institution agency or body that previously submitted a request for the same purpose.

5. Where compliance with the request to make data available to a public sector body or a Union institution, agency or body requires the disclosure of personal data, the data holder shall ▌ pseudonymise the ***personal*** data ***to be made available***.

6. Where the public sector body or the Union institution, agency or body wishes to challenge a data holder's refusal to provide the data requested, or to seek modification of the request, or where the data holder wishes to challenge the request, the matter shall be brought to the ***data coordinator*** referred to in Article 31***, without prejudice to the right to submit a dispute to a civil or administrative court, in accordance with Union or national law***.

Article 19

Obligations of public sector bodies and Union institutions, agencies and bodies

1. A public sector body or a Union institution, agency or body having received data pursuant to a request made under Article 14 ***and statistical or research organisations receiving data pursuant to a request made under Article 21(1)*** shall:

▌

(b) implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects ***and guarantee a high level of security and prevent the unauthorised disclosure of data***;

(ba) implement the necessary technical and organisational measures to manage cyber risk that could affect the confidentiality, integrity or availability of the requested data;

(bb) notify the data holder from whom has received the data of any cybersecurity incident affecting the confidentiality, integrity, or availability of the received data as soon as possible but not later than 72 hours after having determined that the incident has occurred without prejudice to the reporting obligations under Regulation(EU) XXX/XXXX (EUIBAL) and Directive (EU) 2022/2555. Those entities shall be liable by damages due to a cybersecurity breach if they have not had the measures in place pursuant to paragraph 1, point (ba);

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

1a. A public sector body, Union institution, agency, body, or a third party receiving data under this Chapter shall not:

(a) use the data to develop a product or a service that competes with the product or service or enhance an existing product or service from which the accessed data originates;

(b) derive insights about the economic situation, assets and production or operation methods of the data holder, or share the data with another third party for that purpose; or

(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 a Union institution, agency or body shall only be required to the extent that it is strictly necessary to achieve the purpose of ***a*** request ***under Article 15***. In such a case, the ***data holder shall identify the data which are protected as trade secrets. The*** public sector body or the Union institution, agency or body shall take ***in advance all the necessary and*** appropriate ***technical and organisational*** measures ***agreed with the data holder or with the trade secrets holder if it is not simultaneously the same legal person,*** to preserve the confidentiality of those trade secrets ***including as appropriate through the use of model contractual terms, technical standards and the application of codes of conduct***.

2a. Where a public sector body or a Union institution, agency or body transmits or makes data available to third parties to perform the tasks that have been outsourced to it as a result of the outsourcing of technical inspections or other functions pursuant to Article 17(4), trade secrets as identified by the data holder, shall only be disclosed to the extent that they are strictly necessary for the third party to perform the tasks that have been outsourced and provided that all specific necessary measures agreed between the data holder and the third party are taken in advance, including technical and organisational measures to preserve the confidentiality of those trade secrets, including as appropriate through the use of model contractual terms, technical standards and the application of codes of conduct.

2b. In cases where the public sector body or a Union institution, agency or body that submitted the request for data or the third party to which data were made available pursuant to Article 17(4) fails to implement those measures or undermines the confidentiality of trade secrets, the data holder shall be able to suspend the sharing of data identified as trade secrets. In such cases, the data holder shall immediately notify the data coordinator of the Member State in which the data holder is established, pursuant to Article 31, that it has suspended the sharing of data and identify which measures have not been implemented or which trade secrets have had their confidentiality undermined. Where the public sector body or Union institution, agency or body or the third party wishes to challenge the data holder's decision to suspend the sharing of data, the data coordinator shall decide within a reasonable period of time, whether the data sharing shall be resumed or not and if yes, indicate under which conditions.

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

2d. A public sector body or a Union institution, agency or body shall notify the data holder in the event of a security breach as soon as possible, but within 48 hours at the latest.

Article 20

Compensation in cases of exceptional need

1. ***Unless specified otherwise in Union or national law,*** data made available to respond to a public emergency pursuant to Article 15, point (a), shall be provided free of charge. ***The public sector body or the Union institution, agency or body that has received data shall provide public recognition to the data holder if requested by the data holder.***

2. ▌The data holder ***shall be entitled to fair remuneration*** for making data available in compliance with a request made pursuant to Article 15, ***point (b)***, such compensation shall ***at least cover*** the technical and organisational costs incurred to comply with the request including, where ***applicable***, the costs of anonymisation and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the Union institution, agency or body requesting the data, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.

2a. Where the public-sector body or the Union institution, agency or body wishes to challenge the level of remuneration requested by the data holder, the matter shall be brought to the attention of the data coordinator referred to in Article 31 of the Member State where the data holder is established.

Article 21

Contribution of research organisations or statistical bodies in the context of exceptional needs

1. A public sector body or a Union institution, agency or body shall be entitled to share data received under this Chapter with individuals or organisations in view of carrying out scientific research or analytics ***necessary to fulfil*** the purpose for which the data was requested, or to national statistical institutes***, the members of the European System of Central Banks*** and Eurostat for the compilation of official statistics.

2. Individuals or organisations receiving the data pursuant to paragraph 1 shall act ***exclusively*** 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 could result in preferential access to the results of the research.

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

4. Where a public sector body or a Union institution, agency or body ***intends to transmit or make*** data available under paragraph 1, it shall notify the data holder from whom the data was received. ***That notification shall include the identity and the contact details of individuals or organisations receiving the data, the purpose of the transmission or making available of the data and the period for which the data will be used by the receiving entity. Within five working days of the notification referred to in the first subparagraph of this paragraph, the data holder shall have the right to submit a reasoned objection to such transmission or making available of data. In the case of a rejection of the objection by the public sector body, Union institution, agency or body, the data holder may bring the reasoned objection to the data coordinator referred to in Article 31.***

Article 22

Mutual assistance and cross-border cooperation

1. Public sector bodies and Union institutions, agencies and bodies shall cooperate and assist one another, to implement this Chapter in a consistent manner.

2. Any data exchanged in the context of assistance requested and provided pursuant to paragraph 1 shall not be used in a manner incompatible with the purpose for which they were requested.

3. Where a public sector body intends to request data from a data holder established in another Member State, it shall first notify the ***data coordinator*** of that Member State as referred to in Article 31, of that intention. This requirement shall also apply to requests by Union institutions, agencies and bodies. ***The request shall be evaluated by the competent authority of the Member State where the data holder is established.***

4. After having been notified in accordance with paragraph 3, the ***data coordinator*** shall advise the requesting public sector body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request. The requesting public sector body shall take the advice of the ***data coordinator*** into account.

CHAPTER VI

SWITCHING BETWEEN DATA PROCESSING SERVICES

Article 22a

Definitions

For the purposes of this Chapter, the following definitions apply:

1. ***'data processing service' means a digital service enabling ubiquitous, and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature, provided to a customer, that can be rapidly provisioned and released with minimal management effort or service provider interaction;***

2. ***'on-premise' means an ICT infrastructure and computing resources leased or owned by the customer, located in its own data centre and operated by the customer or by a third-party;***

3. ***'equivalent service' means a set of data processing services that share the same primary objective and data processing service model;***

4. ***'data processing service data portability' means the ability of the cloud service to move and adapt its exportable data between the customer's data processing services, including in different deployment models;***

5. ***'switching' means the process where a data processing service customer changes from using one data processing service to using a second equivalent or other service offered by a different provider of data processing services, including through extracting, transforming and uploading the data, involving the source provider of data processing services, the customer and the destination provider of data processing services;***

6. 'exportable data' means the input and output data, including metadata, directly or indirectly generated, or cogenerated, by the customer's use of the data processing service, excluding any data processing service provider's or third party's assets or data protected by intellectual property rights or constituting a trade secret or confidential information;

7. 'functional equivalence' means the possibility to re-establish on the basis of the customer's data a minimum level of functionality in the environment of a new data processing service after the switching process, where the destination service delivers comparable outcome in response to the same input for shared functionality supplied to the customer under the contractual agreement;

8. 'egress fees' refers to data transfer fees charged to the customers of a provider of data processing services for extracting their data through the network from the ICT infrastructure of a provider of data processing services.

Article 23

Removing obstacles to effective switching between providers of data processing services

1. Providers of a data processing service shall***, within their capacity,*** take the measures provided for in Articles 24, ***24a, 24b,*** 25 and 26 to ***enable*** customers ***to*** switch to another data processing service, covering the ***equivalent*** service ▌, which is provided by a different ***provider of data processing services or, where relevant, to use several providers of data processing services at the same time***. In particular, providers of ***a*** data processing service ***shall not impose and*** shall remove commercial, technical, contractual and organisational obstacles, which inhibit customers from:

(a) terminating, after a maximum notice period of ***60*** calendar days, the contractual agreement of the service***, unless an alternative notice period is mutually and explicitly agreed between the customer and the provider where both parties are able equally to influence the content of the contractual agreement***;

(b) concluding new contractual agreements with a different provider of data processing services covering the ***equivalent*** service ▌;

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

(d) ***achieving*** functional equivalence ***in the use*** of the ***new*** service in the IT-environment of the different provider or providers of data processing services covering the ***equivalent*** service ▌, in accordance with Article 26.

2. Paragraph 1 shall only apply to obstacles that are related to the services, contractual agreements or commercial practices provided by the ***source*** provider ***of data processing services***.

Article 24

Contractual terms concerning switching between providers of data processing services

1. The rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services ***or, where applicable, to an on-premise ICT infrastructure*** shall be clearly set out in a written contract ***which is made available to the customer in a user-friendly manner prior to signing the contract***. Without prejudice to Directive (EU) 2019/770, ***the provider of a data processing service*** shall ***ensure that that contract includes*** at least the following:

(a) clauses allowing the customer, upon request, to switch to a data processing service offered by another provider of data processing ***services*** or to port all ***exportable*** data ▌ applications and digital assets ***to an on-premise ICT infrastructure, without undue delay and in any event no longer than*** mandatory maximum transition period of ***90*** calendar days, during which the ***provider of*** data processing ***services*** shall:

(i) ***reasonably assist through and facilitate*** the switching process;

(ii) ***act with due care to maintain business continuity and a high level of security of the service and, taking into account the advancement in the switching process,*** ensure***, to the greatest extent possible,*** continuity in the provision of the ***relevant*** functions or services ***within the capacity of the source provider of data processing services and in accordance with contractual obligations***.

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

(aa) a list of additional services that customers can obtain facilitating the switching process, such as the test of the switching process;

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

(b) ***a detailed*** specification of all data and application categories ***that can be ported*** during the switching process, including, at ***a*** minimum, all ***exportable data***;

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

(ca) an obligation on the provider of data processing services to delete all of the former customer's exportable data after the expiration of the period set out in paragraph 1, point (c), of this Article;

2. Where the mandatory transition period as defined in paragraph 1, points (a) and (c) of this Article is technically unfeasible, the provider of data processing services shall notify the customer within ***14*** working days after the switching request has been made, ***and shall duly motivate*** the technical unfeasibility ***and indicate*** an alternative transition period, which may not exceed ***9*** months. In accordance with paragraph 1 of this Article, ▌ service continuity shall be ensured throughout the alternative transition period against reduced charges, referred to in Article 25(2). ***The customer shall retain the right to extend that period, if needed, prior to or during the switching process.***

Article 24a

Information obligation of providers of destination data processing services

The provider of destination data processing services shall provide the customer with information on available procedures for switching and porting to the data processing service when it is a porting destination, including information on available porting methods and formats as well as restrictions and technical limitations which are known to the provider of destination data processing services.

Article 24b

Good faith obligation

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

Article 25

Gradual withdrawal of switching charges

1. From [***the date of entry into force of this Regulation***] onwards, providers of data processing services shall not impose any charges on ***customers who are consumers*** for the switching process.

2. From [date X, the date of entry into force of ***this Regulation***] until [date X+3yrs], providers of data processing services may impose reduced charges on ***customers in the context of business-to-business relations*** for the switching process***, with particular reference to egress fees***.

2a. From [3 years after the date of entry into force of this Regulation] onwards, providers of data processing services shall not impose any charges for the switching process.

3. The charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned ***and shall be linked to the mandatory operations that providers of data processing services must perform as part of the switching process***.

3a. Standard subscription or service fees and charges for professional transition services work undertaken by the provider of data processing services at the customer's request for support in the switching process shall not be considered switching charges for the purposes of this Article.

3b. Before entering into a contractual agreement with a customer, the provider of data processing services shall provide the customer with clear information describing the charges imposed on the customer for the switching process in accordance with paragraph 2, as well as the fees and charges referred to in paragraph 3a, and, where relevant, shall provide information on services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, application or service architecture. Where applicable, the provider of data processing services shall make this information publicly available to customers via a dedicated section of their website or in any other easily accessible way.

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

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 ***take reasonable measures within their power to facilitate*** that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, ***achieves*** functional equivalence in the use of the new service***, provided that the functional equivalence is established by the destination provider of data processing services. 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 ▌, ***including*** providers of ***destination*** data processing services, shall make open interfaces publicly available and free of charge ***in order to facilitate switching between those services and data portability and interoperability. In accordance with paragraph 1 of this Article, those services shall also make it possible that a specific service, where there are no major obstacles, can be unbundled from the contract and made available for switching in an interoperable manner***.

3. ▌Providers of data processing services shall ensure compatibility with open interoperability ***and portability*** specifications or European standards for interoperability that are identified in accordance with Article 29(5) ▌.

3a. Providers of data processing services for which a new open interoperability and portability specification or European standard was published in the repository referred to in Article 29(5) shall have the right to a one-year transition for compliance with the obligation referred to in paragraph 3 of this Article.

4. Where the open interoperability ***and portability*** specifications or European standards referred to in paragraph 3 ***of this Article*** do not exist for the ***equivalent*** service ▌ concerned, the provider of data processing services shall, at the request of the customer, ***where technically feasible,*** export all ***exportable data in a structured, commonly used and machine-readable format as indicated to the customer in accordance with the exit strategy referred to in Article 24(1), point (ab), unless another format is accepted by the customer***.

4a. Providers of data processing services shall not be required to develop new technologies or services, disclose or transfer proprietary or confidential data or technology 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

Exemptions for certain data processing services

1. The obligations set out in Article 23(1), point (d), and Articles 25 and 26 shall not apply to data processing services which have been custom-built to.

2. The obligations set out in this Chapter shall not apply to data processing services provisioned free of charge, that operate on a trial basis or only supply a testing and evaluation service for business product offerings.

Article 26b

Dispute settlement

1. Customers shall have access to dispute settlement bodies, certified in accordance with Article 10(2), to settle disputes in relation to breaches of the rights of customers and the obligations of providers of data processing services in relation to switching between providers of such services. The customer shall have the right to allow a third party to pursue its legal claims on its behalf.

2. Article 10(3) to (9) shall apply to the settlement of disputes between customers and providers of data processing service in relation to switching between providers of such services.

CHAPTER VII

INTERNATIONAL CONTEXTS NON-PERSONAL DATA SAFEGUARDS

Article 27

International access and transfer

1. Providers of data processing services shall take all ▌ technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer ***and third-country*** governmental access to ***such*** non-personal data held in the Union where such transfer or access would ***be in contravention of*** Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.

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

3. In the absence of such an international agreement, where a provider of data processing services is the addressee of a decision of a court or a tribunal or a decision of an administrative authority of a third country to transfer from or give access to non-personal data ***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 ***following a review by the relevant competent bodies or authorities, pursuant to this Regulation to assess if, in addition to complying with the provisions of any relevant Union or national o law, the following conditions have been met***:

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

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

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

The addressee of the decision may ask the opinion of the ***Commission, the data coordinator*** pursuant to this Regulation ***or relevant competent bodies or authorities***, 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 may impinge on 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 shall deny the request for transfer or access on those grounds.***

The European Data Innovation Board established under Regulation ***(EU) 2022/868 and referred to in Article 31a 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 in paragraph 2 or 3 are met, the provider of data processing services shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation thereof ***by the relevant competent body or authority***.

4a. Where the provider of data processing services has reason to believe that the transfer of or access to non-personal data may lead to the risk of re-identification of non-personal, or anonymised data, the provider shall request the relevant bodies or authorities competent pursuant to applicable data protection legislation for authorisation before transferring or giving access to data.

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

CHAPTER VIII

INTEROPERABILITY

Article 28

Essential requirements regarding interoperability ***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:

(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described ***in a 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 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 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) the means to enable the interoperability of ▌ contracts ***for data sharing*** within their services and activities shall be provided.

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

2. The Commission is empowered to adopt delegated acts, ***after consulting the European Data Innovation Board pursuant to Article 29 and Article 30, points (f) and (h), of Regulation (EU) 2022/868 and*** 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***.

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 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 ▌, to the extent those standards cover those requirements.

3a. Participants within a particular data space shall agree on the rules by which the accountabilities regarding those requirements are defined between the participants.

4. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements under paragraph 1 of this Article***,developed in an open, transparent, technology-neutral, industry-led and inclusive manner, in accordance with Chapter II of Regulation (EU) No 1025/2012, taking into account, where relevant, existing international standards, good practices, norms, technical specifications and relevant open source norms as well as the needs of SMEs.***

5. The Commission ***may***, by way of implementing acts, adopt common specifications, where harmonised standards referred to in paragraph 4 of this Article do not exist or ***if*** it considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article, where necessary***. Prior to adopting those implementing acts the Commission shall seek advice from and take into account relevant positions adopted by the European Data Innovation Board, as referred to in*** Article ***30, point (f), of Regulation (EU) 2022/868 and*** be adopted in accordance with the examination procedure referred to in Article 39(2).

6. The Commission may adopt guidelines ***proposed by the European Data Innovation Board in accordance with Article 30, point (h), of Regulation (EU) 2022/868*** laying down interoperability specifications for the functioning of common European data spaces, such as architectural models and technical standards implementing legal rules and arrangements between parties that foster data sharing, such as regarding rights to access and technical translation of consent or permission.

Article 29

Interoperability ***and portability*** for data processing services

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

(a) ***where technically feasible,*** be performance oriented towards achieving interoperability ***and portability*** between different data processing services that cover ***equivalent services***;

(b) enhance portability of digital assets between different data processing services that cover ***equivalent services***;

(c) ***facilitate***, where technically feasible, functional equivalence between different data processing services ***referred to in paragraph 1 of Article 26 that cover equivalent services;***

(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 ***and portability*** specifications and European standards for the interoperability ***and portability*** of data processing services shall 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 ***and portability*** specifications shall comply with paragraph 3 and 4 of Annex II ***to*** Regulation (EU) No 1025/2012.

3a. Open interoperability and portability specifications and European standards shall not distort the data processing services market or limit the development of any new competing and innovative technologies or solutions or any technologies or solutions that are based on them.

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 European standards applicable to ***equivalent services*** of data processing services. ***The standardisation shall take into account the needs of SMEs.***

5. For the purposes of Article 26(3) of this Regulation, the Commission***, after consulting the European Data Innovation Board pursuant to Article 29 and Article 30, points (f) and (h), of Regulation (EU) 2022/868,*** shall be empowered to adopt delegated acts, ***supplementing this Regulation,*** in accordance with Article 38 ***of this Regulation***, to publish the reference of open ▌ standards for the interoperability ***and portability*** of data processing services in central Union standards repository for the interoperability ***and portability*** of data processing services ***developed by relevant standardisation organisations or organisations referred to in paragraph 3 of Annex II to Regulation (EU) No 1025/2012,***, where these satisfy the criteria specified in paragraph 1 and 2 of this Article.

Article 30

Essential requirements regarding smart contracts for data sharing

▌The ***party offering*** smart contracts ▌ in the context of an agreement to make data available shall comply with the following essential requirements:

(a) robustness ***and access control***: ensure that the smart contract has been designed to offer ***rigorous 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; ***in this regard, the conditions under which a smart contract could be reset or instructed to stop or interrupted, should be clearly and transparently defined. Especially, it should be assessed under which conditions non-consensual termination or interruption should be permissible;***

(ba) equivalence;: a smart contract shall afford the same level of protection and legal certainty as any other contracts generated through different means.

(bb) protection of confidentiality of trade secrets: ensure that a smart contract has been designed to ensure the confidentiality of trade secrets, in accordance with this Regulation.

▌

CHAPTER IX

IMPLEMENTATION AND ENFORCEMENT

Article 31

Data coordinator

1. Each Member State shall designate ***an independent competent coordinating authority ('data coordinator')*** as responsible for the application and enforcement of this Regulation***, for coordinating the activities entrusted to that*** Member ***State, for acting as the single contact point towards the Commission, with regard to the implementation of this Regulation and for representing the Member State at the European Data Innovation Board, as referred to in Article 31a***
.

1a. 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 Union institutions, bodies, offices and agencies. 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***, the data coordinator shall ensure cooperation among the national competent authorities that are responsible for the monitoring of other Union or national legal acts in the field of data and electronic communication services, namely***:

▌

(b) for specific sectoral data ***access*** issues related to the implementation of this Regulation, the competence of sectoral authorities shall be respected ***without prejudice to the rules on conflicts of competences;***

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

3. Member States shall ensure that the respective tasks and powers of the ***data coordinator*** are clearly defined and include:

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

(b) handling ***and deciding on*** complaints arising from alleged violations of this Regulation, and investigating, to the extent appropriate, the subject matter of the complaint and ***regularly*** informing the complainant 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 commercial*** developments of relevance for the making available and use of data ***with a view of better enforcing this Regulation***;

(f) cooperating with ***the data coordinators*** of other Member States to ensure the consistent***, swift and effective*** application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay;

(fa) cooperating with all relevant competent authorities pursuant to other Union law, and with the European Data Protection Board and the European Data Innovation Board to ensure that the obligations of this Regulation are enforced coherently with other Union law;

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

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

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

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

5. Member States shall communicate the name of ***data coordinators*** and their respective tasks and powers and, where applicable, the name of the coordinating competent authority to the Commission ***and Data Innovation Board***. 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, ***data coordinators*** shall ***in an independent and impartial manner and*** remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party.

7. Member States shall ensure that the ***data coordinator is*** provided with ***sufficient human and technical*** resources***, expertise, premises and infrastructure necessary for the effective performance*** to adequately carry out their tasks in accordance with this Regulation.

7a. Entities falling within the scope of this Regulation shall be subject to the jurisdiction of the Member State where the entity is established.

7b. A user, data holder or data recipient that is a legal person and is not established in the Union, but which is subject to obligations under this Regulation, shall designate a legal representative in one of the Member States in which its relevant counterparties are established.

7c. The competent authorities under this Regulation shall have the power to request from users, data holders or data recipients, that are legal persons, or their legal representatives 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.

7d. Where a user, data holder or data recipient, that is a legal person and not established in the Union fails to designate a legal representative or the legal representative fails, upon request of the competent authority, to provide the necessary information that comprehensively demonstrates compliance with this Regulation, the competent authority shall have the power to postpone the commencement of or to suspend the provision of related services by data holders or requests for data access from data holders by users or data recipients, that are legal persons, until the legal representative is designated or the necessary information is provided.

Article 31a

Mutual assistance

1. Data coordinators and the Commission shall cooperate closely and provide each other mutual assistance in order to apply this Regulation in a consistent and efficient manner. Mutual assistance shall include, in particular, exchange of all information in accordance with this Article by electronic means and the duty of the Data Coordinator of the concerned Member State to inform all competent authorities and the Commission about the opening of an investigation.

2. For the purpose of an investigation, the Data coordinator of establishment may request other Data coordinators to provide specific information in their possession or to exercise their investigative powers with regard to specific information located in their Member State. Where appropriate, the data coordinator receiving the request may involve other competent authorities or other public authorities of the Member State in question.

3. The Data coordinator receiving the request pursuant to paragraph 2 shall comply with such request and inform the competent authority of the concerned Member State about the action taken, without undue delay.

4. The European Data Innovation Board shall foster the mutual exchange of information amongst competent authorities as well as advise and assist the Commission in all matters falling under this Regulation., falling under the competence of the Board in accordance with Article 30 of the Regulation (EU) No 2022/868. The data coordinators shall represent the Member States at the European Data Innovation Board established under Regulation (EU) 2022/868.

Article 32

Right to lodge a complaint with a ***data coordinator***

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or ▌ collectively, with the ***data coordinator*** 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. ***Such complaint may arise from the suspension of sharing of data identified as trade secrets, after receiving the notification by the data holder pursuant to Articles 4(3), 5(8) or 19 (2b).***

2. The ***data coordinator*** 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 ***from the beginning of the process*** to handle and resolve complaints ***effectively and in a timely manner***, including ***by setting reasonable deadlines for adopting formal decisions, ensuring equality of the parties, ensuring the right to be heard from complainants and access to the file throughout the process, and*** 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.

Article 32a

Representation

1. Without prejudice to Directive (EU) 2020/1828 or to any other type of representation under national law, users, data holders and data recipients shall at least have the right to mandate a body, organisation or association to exercise the rights conferred by this Regulation on their behalf, provided the body, organisation or association meets all of the following conditions:

(a) it operates on a not-for-profit basis;

(b) it has been properly constituted in accordance with the law of a Member State;

(c) its statutory objectives include a legitimate interest in ensuring that this Regulation is complied with.

Article 32b

Right to an effective judicial remedy against a competent authority

1. Without prejudice to any other administrative or non-judicial remedy, each user, data holder and data recipient shall have the right to an effective judicial remedy against a legally binding decision of a competent authority concerning them.

2. Without prejudice to any other administrative or non judicial remedy, each user shall have the right to an effective judicial remedy where the competent authority does not handle a complaint swiftly or does not inform the user, data holder and data recipient within three months on the progress or outcome of the complaint lodged pursuant to Article 32.

3. Proceedings against a competent authority shall be brought before the courts of the Member State of the habitual residence, place of work or establishment of the user or their representative organisation.

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 32c

Right to an effective judicial remedy

1. Without prejudice to any available administrative or non-judicial remedy, including under Directive (EU) 2020/1828 and the right to lodge a complaint with a competent authority pursuant to Article 32b, user, data holder and data recipient shall have the right to an effective judicial remedy where they consider that their rights under this Regulation have been infringed as a result of the non-compliance with this Regulation.

2. Proceedings against a data holder, third party or data recipient shall be brought before the courts of the Member State where the user has their habitual residence, place or work or establishment.

Article 33

Penalties

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

1a. Member States shall take into account the following non-exhaustive 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.

2. Member States shall by [date of application of the Regulation] notify the Commission***, the European Data Protection Board and the European Data Innovation Board*** of those rules and measures and shall notify ***them*** 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

The Commission shall develop and recommend non-binding model contractual terms on data access and use ***and standard contractual clauses for cloud computing contracts, based on Fair, Reasonable and Non-Discriminatory (FRAND) principles,*** to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations. ***Such model contractual terms shall address at least the following elements:***

(a) right to early termination of the contract and conditions for compensation in the case of early termination;

(b) data retention and storage policies;

(c) readability of the data for the user, including information on metadata and decryption;

(d) the protection and preservation of the confidentiality of trade secrets, in accordance with this Regulation.

The model contractual terms referred to in the first subparagraph shall be published and shall be available free of charge in easily usable electronic format.

CHAPTER X

INAPPLICABILITY OF THE SUI GENERIS RIGHT UNDER DIRECTIVE ***96/9/EC TO DATABASES CONTAINING CERTAIN DATA***

Article 35

Databases containing certain data

The sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service ***falling within the scope of this Regulation***.

CHAPTER XI

FINAL PROVISIONS

Article 36

Amendment to Regulation (EU) No 2017/2394

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

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

Article 37

Amendment to Directive (EU) 2020/1828

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

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

Article 38

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Articles 25(4), 28(2) and 29(5) shall be conferred on the Commission for an indeterminate period of time from […].

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

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

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

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

Article 39

Committee procedure

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

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

Article 40

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

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

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

(a) technical aspects of data access;

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

(c) aspects going beyond data access and use.

Article 41

Evaluation and review

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

(-a) the use of data by users, data holders, data recipients and third parties, the development of monetisation practices in the European data economy as well as the development of the arrangements for data sharing, including competitive dynamics in data spaces and data intermediation services;

(-aa) the effects of technical and administrative obligations to comply with this Regulation, in particular with Chapter II thereof on industry participants, also in view of the SME exemptions;

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

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

(ba) whether the provisions of this Regulation related to trade secrets ensure respect for trade secrets while not hampering the access to and sharing of data; in particular, the evaluation shall assess whether and how the confidentiality of trade secrets is ensured in practice despite their disclosure both in the context of data sharing with third parties and in the business-to-government context. This assessment shall be carried out in close relationship with the evaluation report on Directive (EU) 2016/943 expected by 9 June 2026 pursuant to Article 18(3) of the directive thereof;

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

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

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

(ea) the interaction between the this Regulation and other relevant Union law to assess possible conflicting regulation, overregulation or legislative gaps;

(eb) the contribution of this Regulation to ensuring the economic attractiveness of the collection and use of high quality data sets by Union companies;

(ec) the contribution of this Regulation to innovation and to promoting the development of high-tech start-ups and SMEs, as well as to enabling access for European users to state-of-the-art computing services;

(ed) the application and functioning of Article 27 on the international access and transfer of data.

1a On the basis of that report, the Commission shall, 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 ***18*** months after the date of entry into force of this Regulation ▌ .

The obligations resulting from Article 4(1) shall apply to related services placed on the market within five years prior to the entry into force of this Regulation and only where the provider of a related service is able to remotely deploy mechanisms to ensure the fulfilment of the requirements pursuant to Article 4(1) and where the deployment of such mechanisms would not place a disproportionate burden on the manufacturer or provider of related services.

Done at,

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