Official Journal
of the European Union

EN
Series L

2023/2854 22.12.2023

# REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## of 13 December 2023

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

**(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Central Bank ([1]),

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

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

Acting in accordance with the ordinary legislative procedure ([4]),

Whereas:

(1) In recent years, data-driven technologies have had transformative effects on all sectors of the economy. The proliferation of 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 data may be used and reused for a variety of purposes and to an unlimited degree, without any loss of quality or quantity.

(2) Barriers to data sharing prevent an optimal allocation of data for the benefit of society. Those 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 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 the abuse of contractual imbalances with regard to data access and use.

(3) In sectors characterised by the presence of microenterprises, small enterprises and medium-sized enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC ([5]) (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 them in the system or due to a lack of interoperability between data, between data services or across borders.

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

(5) This Regulation ensures that users of a connected product or related service in the Union can access, in a timely manner, the data generated by the use of that connected product or related service and that those users can use the data, including by sharing them with third parties of their choice. It imposes the obligation on data holders to make data available to users and third parties of the user's choice in certain circumstances. It also ensures that data holders make data available to data recipients in the Union under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner. Private law rules are key in the overall framework for data sharing. Therefore, this Regulation adapts rules of contract law and prevents the exploitation of contractual imbalances that hinder fair access to and use of data. This Regulation also ensures that data holders make available to public sector bodies, the Commission, the European Central Bank or Union bodies, where there is an exceptional need, the data that are necessary for the performance of a specific task carried out in the public interest. In addition, this Regulation seeks to facilitate switching between data processing services and to enhance the interoperability of data and of data sharing mechanisms and services in the Union. This Regulation should not be interpreted as recognising or conferring any new right on data holders to use data generated by the use of a connected product or related service.

(6) Data generation is the result of the actions of at least two actors, in particular the designer or manufacturer of a connected product, who may in many cases also be a provider of related services, and the user of the connected product or related service. It gives rise to questions of fairness in the digital economy as the data recorded by connected products or related services are an important input for aftermarket, ancillary and other services. In order to realise the important economic benefits of data, including by way of data sharing on the basis of voluntary agreements and the development of data-driven value creation by Union enterprises, a general approach to assigning rights regarding access to and the use of data is preferable to awarding exclusive rights of access and use. This Regulation provides for horizontal rules which could be followed by Union or national law that addresses the specific situations of the relevant sectors.

(7) The fundamental right to the protection of personal data is safeguarded, in particular, by Regulations (EU) 2016/679 ([6]) and (EU) 2018/1725 ([7]) of the European Parliament and of the Council. Directive 2002/58/EC of the European Parliament and of the Council ([8]) additionally protects private life and the confidentiality of communications, including by way of conditions on any personal and non-personal data storing in, and access from, terminal equipment. Those Union legislative acts 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 the protection of personal data and privacy, in particular Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive 2002/58/EC. No provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right

to privacy and confidentiality of communications. Any processing of personal data pursuant to this Regulation should comply with Union data protection law, including the requirement of a valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC. This Regulation does not constitute a legal basis for the collection or generation of personal data by the data holder. This Regulation imposes an obligation on data holders to make personal data available to users or third parties of a user's choice upon that user's request. Such access should be provided to personal data that are processed by the data holder on the basis of any of the legal bases referred to in Article 6 of Regulation (EU) 2016/679. Where the user is not the data subject, this Regulation does not create a legal basis for providing access to personal data or for making personal data available to a third party and should not be understood as conferring any new right on the data holder to use personal data generated by the use of a connected product or related service. In those cases, it could be in the interest of the user to facilitate meeting the requirements of Article 6 of Regulation (EU) 2016/679. As this Regulation should not adversely affect the data protection rights of data subjects, the data holder can comply with requests in those cases, inter alia, by anonymising personal data or, where the readily available data contains personal data of several data subjects, transmitting only personal data relating to the user.

(8) The principles of data minimisation and data protection by design and by default are essential when processing involves significant risks to the fundamental rights of individuals. Taking into account the state of the art, all parties to data sharing, including data sharing falling within scope of this Regulation, should implement technical and organisational measures to protect those 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) Unless otherwise provided for in this Regulation, it does not affect national contract law, including rules on the formation, validity or effect of contracts, or the consequences of the termination of a contract. This Regulation complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection, and to protect their health, safety and economic interests, in particular Council Directive 93/13/EEC ([9]) and Directives 2005/29/EC ([10]) and 2011/83/EU ([11]) of the European Parliament and of the Council.

(10) This Regulation is without prejudice to Union and national legal acts providing for the sharing of, access to and the use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for 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 (TFEU) on which such Union legal acts were adopted, as well as to international cooperation in that area, in particular on the basis of the Council of Europe Convention on Cybercrime, (ETS No 185), done at Budapest on 23 November 2001. Such acts include Regulations (EU) 2021/784 ([12]), (EU) 2022/2065 ([13]) and (EU) 2023/1543 ([14]) of the European Parliament and of the Council and Directive (EU) 2023/1544 of the European Parliament and of the Council ([15]). This Regulation does not apply to the collection or sharing of, access to or the use of data under Regulation (EU) 2015/847 of the European Parliament and of the Council ([16]) and Directive (EU) 2015/849 of the European Parliament and of the Council ([17]). This Regulation does not apply to areas that fall outside the scope of Union law and in any event does not affect the competences of the Member States concerning

public security, defence or national security, customs and tax administration or the health and safety of citizens, regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences.

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

(12) This Regulation complements and is without prejudice to Union law aiming to establish accessibility requirements on certain products and services, in particular Directive (EU) 2019/882 of the European Parliament and of the Council ([18]).

(13) This Regulation is without prejudice to Union and national legal acts providing for the protection of intellectual property rights, including Directives 2001/29/EC ([19]), 2004/48/EC ([20]) and (EU) 2019/790 ([21]) of the European Parliament and of the Council.

(14) Connected products that obtain, generate or collect, by means of their components or operating systems, data concerning their performance, use or environment and that are able to communicate those data via an electronic communications service, a physical connection, or on-device access, often referred to as the Internet of Things, should fall within the scope of this Regulation, with the exception of prototypes. Examples of such electronic communications services include, in particular, land-based telephone networks, television cable networks, satellite-based networks and near-field communication networks. Connected products are found in all aspects of the economy and society, including in private, civil or commercial infrastructure, vehicles, health and lifestyle equipment, ships, aircraft, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery. Manufacturers' design choices, and, where relevant, Union or national law that addresses sector-specific needs and objectives or relevant decisions of competent authorities, should determine which data a connected product is capable of making available.

(15) The data represent the digitisation of user actions and events and should accordingly be accessible to the user. The rules for access to and the use of data from connected products and related services under this Regulation address both product data and related service data. Product data refers to data generated by the use of a connected product that the manufacturer designed to be retrievable from the connected product by a user, data holder or a third party, including, where relevant, the manufacturer. Related service data refers to data, which also represent the digitisation of user actions or events related to the connected product which are generated during the provision of a related service by the provider. Data generated by the use of a connected product or related service should be understood to cover data recorded intentionally or data which result indirectly from the user's action, such as data about the connected product's environment or interactions. This should include data on the use of a connected product generated by a user interface or via a related service, and should not be limited to the information that such use took place, but should include all data that the connected product generates as a result of such use, such as data generated automatically by sensors and data recorded by embedded applications, including applications indicating hardware status and malfunctions. This should also include data generated by the connected product or related service during times of inaction by the user, such as when the user chooses not to use a connected product for a given period of time and instead to keep it in stand-by mode or even switched off, as the status of a connected product or its components, for example its batteries, can vary when the connected product is in stand-by mode or switched off. Data which are not substantially modified, meaning data in raw form, also known as source or primary data which refer to data points that are automatically generated without any further

form of processing, as well as data which have been pre-processed for the purpose of making them understandable and useable prior to subsequent processing and analysis fall within the scope of this Regulation. Such data includes data collected from a single sensor or a connected group of sensors for the purpose of making the collected data comprehensible for wider use-cases by determining a physical quantity or quality or the change in a physical quantity, such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed. The term ‘pre-processed data’ should not be interpreted in such a manner as to impose an obligation on the data holder to make substantial investments in cleaning and transforming the data. The data to be made available should include the relevant metadata, including its basic context and timestamp, to make the data usable, combined with other data, such as data sorted and classified with other data points relating to them, or re-formatted into a commonly used format. Such data are potentially valuable to the user and support innovation and the development of digital and other services to protect the environment, health and the circular economy, including through facilitating the maintenance and repair of the connected products in question. By contrast, information inferred or derived from such data, which is the outcome of additional investments into assigning values or insights from the data, in particular by means of proprietary, complex algorithms, including those that are a part of proprietary software, should not be considered to fall within the scope of this Regulation and consequently should not be subject to the obligation of a data holder to make it available to a user or a data recipient, unless otherwise agreed between the user and the data holder. Such data could include, in particular, information derived by means of sensor fusion, which infers or derives data from multiple sensors, collected in the connected product, using proprietary, complex algorithms and which could be subject to intellectual property rights.

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

(17) It is necessary to lay down rules regarding products that are connected to a related service at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to or adapt the functionality of the connected product. Such related services involve the exchange of data between the connected product and the service provider and should be understood to be explicitly linked to the operation of the connected product’s functions, such as services that, where applicable, transmit commands to the connected product that are able to have an impact on its action or behaviour. Services which do not have an impact on the operation of the connected product and which do not involve the transmitting of data or commands to the connected product by the service provider should not be considered to be related services. Such services could

include, for example, auxiliary consulting, analytics or financial services, or regular repair and maintenance. Related services can be offered as part of the purchase, rent or lease contract. Related services could also be provided for products of the same type and users could reasonably expect them to be provided taking into account the nature of the connected product and any public statement made by or on behalf of the seller, rentor, lessor or other persons in previous links of the chain of transactions, including the manufacturer. Those 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. This Regulation should also apply to a related service that is not supplied by the seller, rentor or lessor itself, but which is provided by a third party. In the event of doubt as to whether the service is provided as part of the purchase, rent or lease contract, this Regulation should apply. Neither the power supply, nor the supply of the connectivity are to be interpreted as related services under this Regulation.

(18) The user of a connected product should be understood to be a natural or legal person, such as a business, a consumer or a public sector body, that owns a connected product, has received certain temporary rights, for example by means of a rental or lease agreement, to access or use data obtained from the connected product, or receives related services for the connected product. Those access rights should in no way alter or interfere with the rights of data subjects who may be interacting with a connected product or a related service regarding personal data generated by the connected product or during the provision of the related service. The user bears the risks and enjoys the benefits of using the connected product and should also enjoy access to the data it generates. The user should therefore be entitled to derive benefit from data generated by that connected product and any related service. An owner, renter or lessee should also be considered to be a user, including where several entities can be considered to be users. In the context of multiple users, each user may contribute in a different manner to the data generation and have an interest in several forms of use, such as fleet management for a leasing enterprise, or mobility solutions for individuals using a car sharing service.

(19) Data literacy refers to the skills, knowledge and understanding that allows users, consumers and businesses, in particular SMEs falling within the scope of this Regulation, to gain awareness of the potential value of the data they generate, produce and share and that they are motivated to offer and provide access to in accordance with relevant legal rules. Data literacy should go beyond learning about tools and technologies and aim to equip and empower citizens and businesses with the ability to benefit from an inclusive and fair data market. The spread of data literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions and ultimately sustain the consolidation, and innovation path of, the data economy in the Union. Competent authorities should promote tools and adopt measures to advance data literacy among users and entities falling within the scope of this Regulation and an awareness of their rights and obligations thereunder.

(20) In practice, not all data generated by connected products or related services are easily accessible to their users and there are often limited possibilities regarding the portability of data generated by products connected to the internet. Users are unable to obtain the data necessary to make use of providers of repair and other services and businesses are unable to launch innovative, convenient and more efficient services. In many sectors, manufacturers are able to determine, through their control of the technical design of the connected products or related services, what data are generated and how they can be accessed, despite having no legal right to those data. It is therefore necessary to ensure that connected products are designed and manufactured, and related services are designed and provided, in

such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, including for the purpose of retrieving, using or sharing them, are always easily and securely accessible to a user, free of charge, in a comprehensive, structured, commonly used and machine-readable format. Product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, such as by means of the connected product design, the data holder's contract with the user for the provision of related services, and its technical means of data access, without disproportionate effort, are referred to as 'readily available data'. Readily available data does not include data generated by the use of a connected product where the design of the connected product does not provide for such data being stored or transmitted outside the component in which they are generated or the connected product as a whole. This Regulation should therefore not be understood to impose an obligation to store data on the central computing unit of a connected product. The absence of such an obligation should not prevent the manufacturer or data holder from voluntarily agreeing with the user on the making of such adaptations. The design obligations in this Regulation are also without prejudice to the data minimisation principle laid down in Article 5(1), point (c), of Regulation (EU) 2016/679 and should not be understood as imposing an obligation to design connected products and related services in such a way that they store or otherwise process any personal data other than the personal data necessary in relation to the purposes for which they are processed. Union or national law could be introduced to outline further specificities, such as the product data that should be accessible from connected products or related services, given that such data may be essential for the efficient operation, repair or maintenance of those connected products or related services. Where subsequent updates or alterations to a connected product or a related service, 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.

(21) Where several persons or entities are considered to be users, for example in the case of co-ownership or where an owner, renter or lessee shares rights of data access or use, the design of the connected product or related service, or the relevant interface, should enable each user to have access to the data they generate. Use of connected products that generate data typically requires a user account to be set up. Such an account allows the user to be identified by the data holder, which may be the manufacturer. It can also be used as a means of communication and to submit and process data access requests. Where several manufacturers or related services providers have sold, rented or leased connected products or provided related services, integrated together, to the same user, the user should turn to each of the parties with which it has a contract. Manufacturers or designers of a connected product that is typically used by several persons should put in place the necessary mechanisms to allow separate user accounts for individual persons, where relevant, or for the possibility of several persons using the same user account. Account solutions should allow users to delete their accounts and erase the data related to them and could allow users to terminate data access, use or sharing, or submit requests to terminate, in particular taking into account situations in which the ownership or usage of the connected product changes. Access should be granted to the user on the basis of simple request mechanism granting automatic execution and not requiring examination or clearance by the manufacturer or data holder. This means that the data should be made available only when the user actually wants access. Where automated execution of the data access request is not possible, for example via a user account or accompanying mobile application provided with the connected product or related service, the manufacturer should inform the user as to how the data may be accessed.

(22) Connected products may be designed to make certain data directly accessible from on-device data storage or from a remote server to which the data are communicated. Access to on-device data storage may be enabled via cable-based or wireless local area networks connected to a publicly available electronic communications service or mobile network. The server may be the manufacturer's own local server capacity or that of a third party or a cloud service provider. Processors as defined in Article 4, point (8), of Regulation (EU) 2016/679 are not considered to act as data holders. However, they can be specifically tasked with making data available by the controller as defined in Article 4, point (7), of Regulation (EU) 2016/679. Connected products may be designed to permit the user or a third party to process the data on the connected product, on a computing instance of the manufacturer or within an information and communications technology (ICT) environment chosen by the user or the third party.

(23) Virtual assistants play an increasing role in digitising consumer and professional environments and serve as an easy-to-use interface to play content, obtain information, or activate products connected to the internet. Virtual assistants can act as a single gateway in, for example, a smart home environment and record significant amounts of relevant data on how users interact with products connected to the internet, including those manufactured by other parties, and can replace the use of manufacturer-provided interfaces such as touch screens or smartphone apps. The user may wish to make available such data to third party manufacturers and enable novel smart services. Virtual assistants should be covered by the data access rights provided for in this Regulation. 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 should also be covered by the data access rights provided for in this Regulation. However, only the data arising from the interaction between the user and a connected product or related service through the virtual assistant should be covered by this Regulation. Data produced by the virtual assistant which are unrelated to the use of a connected product or related service are not covered by this Regulation.

(24) Before concluding a contract for the purchase, rent, or lease of a connected product, the seller, rentor or lessor, which may be the manufacturer, should provide to the user information regarding the product data which the connected product is capable of generating, including the type, format and the estimated volume of such data, in a clear and comprehensible manner. This could include information on data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, as well as clear and sufficient information relevant for the exercise of the user's rights on how the data may be stored, retrieved or accessed, including the terms of use and quality of service of application programming interfaces or, where applicable, the provision of software development kits. That obligation provides transparency over the product data generated and enhances easy access for the user. The information obligation could be fulfilled, for example by maintaining a stable uniform resource locator (URL) on the web, which can be distributed as a web link or QR code, pointing to the relevant information, which could be provided by the seller, rentor or lessor, which may be the manufacturer, to the user before concluding the contract for the purchase, rent or lease of a connected product. It is, in any case, necessary that the user is able to store the information in a way that is accessible for future reference and that allows the unchanged reproduction of the information stored. The data holder cannot be expected to store the data indefinitely in view of the needs of the user of the connected product, but should implement a reasonable data retention policy, where applicable, in line with storage limitation principle pursuant Article 5(1), point (e), of Regulation (EU) 2016/679, that allows for the effective application of the data access rights provided for in this Regulation. The obligation to provide information does not affect the obligation of the controller to provide information

to the data subject pursuant to Articles 12, 13 and 14 of Regulation (EU) 2016/679. The obligation to provide information before concluding a contract for the provision of a related service should lie with the prospective data holder, independently of whether the data holder concludes a contract for the purchase, rent or lease of a connected product. Where information changes during the lifetime of the connected product or the contract period for the related service, including where the purpose for which those data are to be used changes from the originally specified purpose, it should also be provided to the user.

(25) This Regulation should not be understood to confer any new right on data holders to use product data or related service data. Where the manufacturer of a connected product is a data holder, the basis for the manufacturer to use non-personal data should be a contract between the manufacturer and the user. Such a contract could be part of an agreement for the provision of the related service, which could be concluded together with the purchase, rent or lease agreement relating to the connected product. Any contractual term stipulating that the data holder may use product data or related service data should be transparent to the user, including regarding the purposes for which the data holder intends to use the data. Such purposes could include improving the functioning of the connected product or related services, developing new products or services, or aggregating data with the aim of making available the resulting derived data to third parties, provided that such derived data do not allow the identification of specific data transmitted to the data holder from the connected product, or allow a third party to derive those data from the dataset. Any change of the contract should depend on the informed agreement of the user. This Regulation does not prevent parties from agreeing on contractual terms the effect of which is to exclude or limit the use of non-personal data, or certain categories of non-personal data, by a data holder. Neither does it prevent parties from agreeing to make product data or related service data available to third parties, directly or indirectly, including, where applicable, via another data holder. Moreover, this Regulation does not prevent sector-specific regulatory requirements under Union law, or national law compatible with Union law, which would exclude or limit the use of certain such data by the data holder on well-defined public policy grounds. This Regulation does not prevent users, in the case of business-to-business relations, from making data available to third parties or data holders under any lawful contractual term, including by agreeing to limit or restrict further sharing of such data, or from being compensated proportionately, for example in exchange for waiving their right to use or share such data. While the notion of ‘data holder’ generally does not include public sector bodies, it may include public undertakings.

(26) To foster the emergence of liquid, fair and efficient markets for non-personal data, users of connected products should be able to share data with others, including for commercial purposes, with minimal legal and technical effort. It is currently often difficult for businesses to justify the personnel or computing costs that are necessary for preparing non-personal datasets or data products and to offer them to potential counterparties via data intermediation services, including data marketplaces. A substantial hurdle to the sharing of non-personal data by businesses therefore results from the lack of predictability of economic returns from investing in the curation and making available of datasets or data products. In order to allow for the emergence of liquid, fair and efficient markets for non-personal data in the Union, the party that has the right to offer such data on a market must be clarified. Users should therefore have the right to share non-personal data with data recipients for commercial and non-commercial purposes. Such data sharing could be performed directly by the user, upon the request of the user via a data holder, or through data intermediation services. Data intermediation services, as regulated by Regulation (EU) 2022/868 of the European Parliament and of the Council ([22]) 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 anonymisation of personal data or aggregation of access to data from multiple individual users. Where data are excluded from a data holder's obligation to make them available to users or third parties, the scope of such data could be specified in the contract between the user and the data holder for the provision of a related service so that users can easily determine which data are available to them for sharing with data recipients or third parties. Data holders should not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user, without prejudice to legal requirements pursuant to Union or national law for a data holder to make data available. Where relevant, data holders should contractually bind third parties not to further share data received from them.

(27) In sectors characterised by the concentration of a small number of manufacturers supplying connected products to end users, there may only be limited options available to users for the access to and the use and sharing of data. In such circumstances, contracts may be insufficient to achieve the objective of user empowerment, making it difficult for users to obtain value from the data generated by the connected product they purchase, rent or lease. Consequently, there is limited potential for innovative smaller businesses to offer data-based solutions in a competitive manner and for a diverse data economy in the Union. This Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contract. Union or national law may be adopted to address sector-specific needs and objectives. Furthermore, data holders should not use any readily available data that is non-personal data in order to derive insights about the economic situation of the user or its assets or production methods or about such use by the user in any other manner that could undermine the commercial position of that user on the markets in which it is active. This could include using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on the potential acquisition of the user's products or agricultural produce to the user's detriment, or using such information to feed into larger databases on certain markets in the aggregate, for example 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 such permissions.

(28) In contracts between a data holder and a consumer as user of a connected product or related service generating data, Union consumer law, in particular Directives 93/13/EEC and 2005/29/EC, applies to ensure that a consumer is not subject to unfair contractual terms. For the purposes of this Regulation, unfair contractual terms unilaterally imposed on an enterprise should not be binding on that enterprise.

(29) Data holders may require appropriate user identification to verify a 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.

(30) The user should be free to use the data for any lawful purpose. This includes providing the data the user has received while exercising its rights under this Regulation to a third party offering an aftermarket service that may be in competition with a service provided by a data holder, or to instruct the data holder to do so. The request should be submitted by the user or by an authorised third party acting on a user's behalf, including a provider of a data intermediation service. Data holders should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date as the data the data holder itself may be able or entitled to access from the use of the connected product or related service. Any intellectual property rights should be respected in the handling of the

data. It is important to preserve incentives to invest in products with functionalities based on the use of data from sensors built into those products.

(31) Directive (EU) 2016/943 of the European Parliament and of the Council ([23]) provides that the acquisition, use or disclosure of a trade secret shall be considered to be lawful, inter alia, where such acquisition, use or disclosure is required or allowed by Union or national law. While this Regulation requires data holders to disclose certain data to users, or third parties of a user's choice, even when such data qualify for protection as trade secrets, it should be interpreted in such a manner as to preserve the protection afforded to trade secrets under Directive (EU) 2016/943. In this context, data holders should be able to require users, or third parties of a user's choice, to preserve the confidentiality of data considered to be trade secrets. To that end, data holders should identify trade secrets prior to the disclosure, and should have the possibility to agree with users, or third parties of a user's choice, on necessary measures to preserve their confidentiality, including by the use of model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct. In addition to the use of model contractual terms to be developed and recommended by the Commission, the establishment of codes of conduct and technical standards related to the protection of trade secrets in handling the data could help achieve the aim of this Regulation and should be encouraged. Where there is no agreement on the necessary measures or where a user, or third parties of the user's choice, fail to implement agreed measures or undermine the confidentiality of the trade secrets, the data holder should be able to withhold or suspend the sharing of data identified as trade secrets. In such cases, the data holder should provide the decision in writing to the user or to the third party without undue delay and notify the competent authority of the Member State in which the data holder is established that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined. Data holders cannot, in principle, refuse a data access request under this Regulation solely on the basis that certain data is considered to be a trade secret, as this would subvert the intended effects of this Regulation. However, in exceptional circumstances, a data holder who is a trade secret holder should be able, on a case-by-case basis, to refuse a request for the specific data in question if it is able to demonstrate to the user or to the third party that, despite the technical and organisational measures taken by the user or by the third party, serious economic damage is highly likely to result from the disclosure of that trade secret. Serious economic damage implies serious and irreparable economic loss. The data holder should duly substantiate its refusal in writing without undue delay to the user or to the third party and notify the competent authority. Such a substantiation should be based on objective elements, demonstrating the concrete risk of serious economic damage expected to result from a specific data disclosure and the reasons why the measures taken to safeguard the requested data are not considered to be sufficient. A possible negative impact on cybersecurity can be taken into account in that context. Without prejudice to the right to seek redress before a court or tribunal of a Member State, where the user or a third party wishes to challenge the data holder's decision to refuse or to withhold or suspend data sharing, the user or the third party can lodge a complaint with the competent authority, which should, without undue delay, decide whether and under which conditions data sharing should start or resume, or can agree with the data holder to refer the matter to a dispute settlement body. The exceptions to data access rights in this Regulation should not in any case limit the right of access and right to data portability of data subjects under Regulation (EU) 2016/679.

(32) The aim of this Regulation is not only to foster the development of new, innovative connected products or related services, stimulate innovation on aftermarkets, but also to stimulate the development of

entirely novel services making use of the data concerned, including based on data from a variety of connected products or related services. At the same time, this Regulations aims to avoid undermining the investment incentives for the type of connected product from which the data are obtained, for instance, by the use of data to develop a competing connected product which is considered to be interchangeable or substitutable by users, in particular on the basis of the connected product's characteristics, its price and intended use. This Regulation provides for no prohibition on the development of a related service using data obtained under this Regulation as this would have an undesirable discouraging effect on innovation. Prohibiting the use of data accessed under this Regulation for developing a competing connected product protects data holders' innovation efforts. Whether a connected product competes with the connected product from which the data originates depends on whether the two connected products are in competition on the same product market. This is to be determined on the basis of the established principles of Union competition law for defining the relevant product market. However, lawful purposes for the use of the data could include reverse engineering, provided that it complies with the requirements laid down in this Regulation and in Union or national law. This may be the case for the purposes of repairing or prolonging the lifetime of a connected product or for the provision of aftermarket services to connected products.

(33) A third party to whom data is made available may be a natural or legal person, such as a consumer, an enterprise, a research organisation, a not-for-profit organisation or an entity acting in a professional capacity. In making the data available to the third party, a data holder should not abuse its position to seek a competitive advantage in markets where the data holder and the third party may be in direct competition. The data holder should not therefore use any readily available data in order to derive insights about the economic situation, assets or production methods of, or the use by, the third party in any other manner that could undermine the commercial position of the third party on the markets in which the third party is active. The user should be able to share non-personal data with third parties for commercial purposes. Upon the agreement with the user, and subject to the provisions of this Regulation, third parties should be able to transfer the data access rights granted by the user to other third parties, including in exchange for compensation. Business-to-business data intermediaries and personal information management systems (PIMS), referred to as data intermediation services in Regulation (EU) 2022/868, may support users or third parties in establishing commercial relations with an undetermined number of potential counterparties for any lawful purpose falling within the scope of this Regulation. They could play an instrumental role in aggregating access to data so that big data analyses or machine learning can be facilitated, provided that users remain in full control of whether to provide their data to such aggregation and the commercial terms under which their data are to be used.

(34) The use of a connected product or related service may, in particular when the user is a natural person, generate data that relates to 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 dataset are inextricably linked. 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 that user 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 use of a connected product, whether personal or 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 connected product, the user is considered to be a controller. Accordingly, such a user who as controller intends to request personal data generated by the use of a connected product or related service is required to have a legal basis for processing the data as

required by Article 6(1) of Regulation (EU) 2016/679, such as the consent of the data subject or the performance of a contract to which the data subject is a party. Such user should ensure that the data subject is appropriately informed of the specified, explicit and legitimate purposes for processing those data, and of how the data subject may exercise their rights effectively. 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 that user meets the criteria under this Regulation and thus becomes subject to the obligations to make data available under this Regulation.

(35) Product data or related service data should only be made available to a third party at the request of the user. This Regulation complements accordingly the right, provided for in Article 20 of Regulation (EU) 2016/679, of data subjects to receive personal data concerning them in a structured, commonly used and machine-readable format, as well as to port those data to another controller, where those data are processed by automated means on the basis of Article 6(1), point (a), or Article 9(2), point (a), or of a contract pursuant to Article 6(1), point (b) of that Regulation. Data subjects also have the right to have the personal data transmitted directly from one controller to another, but only where that is technically feasible. Article 20 of Regulation (EU) 2016/679 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 connected 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 rights provided for under this Regulation complement the right to receive and port personal data under Article 20 of Regulation (EU) 2016/679 in a number of ways. This Regulation grants users the right to access and make available to a third party any product data or related service data, irrespective of their nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of data falling within its scope, whether personal or non-personal, thereby ensuring that technical obstacles no longer hinder or prevent access to such data. It also allows data holders to set reasonable compensation to be met by third parties, but not by the user, for costs incurred in providing direct access to the data generated by the user’s connected product. If a data holder and a third party are unable to agree on terms for such direct access, the data subject should in no way be prevented from exercising the rights laid down 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 contract does not allow for the processing of special categories of personal data by the data holder or the third party.

(36) 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 by the subscriber or for the sole purpose of the transmission of a communication. Directive 2002/58/EC protects the integrity of a user’s terminal equipment regarding the use of processing and storage capabilities and the collection of information. Internet of Things equipment is considered to be terminal equipment if it is directly or indirectly connected to a public communications network.

(37) In order to prevent the exploitation of users, third parties to whom data has been made available at the request of the user should process those data only for the purposes agreed with the user and share them with another third party only with the agreement of the user to such data sharing.

(38) In line with the data minimisation principle, third parties should access only information that is necessary for the provision of the service requested by the user. Having received access to data, the third party should process it for the purposes agreed with the user without interference from the data holder. It should be as easy for the user to refuse or discontinue access by the third party to the data as it is for the user to authorise access. Neither third parties nor data holders should make the exercise of choices or rights by the user unduly difficult, including by offering choices to the user in a non-neutral manner, or by coercing, deceiving or manipulating the user, or by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a user digital interface or a part thereof. In that 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. Those manipulative techniques can be used to persuade users, in particular vulnerable consumers, to engage in unwanted behaviour, 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 such a way as to subvert or impair their autonomy, decision-making and choice. Common and legitimate commercial practices that comply with Union law should not in themselves be regarded as constituting dark patterns. Third parties and data holders should comply with their obligations under relevant Union law, in particular the requirements laid down in Directives 98/6/EC ([24]) and 2000/31/EC ([25]) of the European Parliament and of the Council and in Directives 2005/29/EC and 2011/83/EU.

(39) Third parties should also refrain from using data falling within the scope of this Regulation to profile individuals unless such processing activities are strictly necessary to provide the service requested by the user, including in the context of automated decision-making. The requirement to erase data when no longer required for the purpose agreed with the user, unless otherwise agreed in relation to non-personal data, complements the data subject's right to erasure pursuant to Article 17 of Regulation (EU) 2016/679. Where a third party is a provider of a data intermediation service, the safeguards for the data subject provided for by Regulation (EU) 2022/868 apply. The third party may use the data to develop a new and innovative connected product or related service but not to develop a competing connected product.

(40) Start-ups, small enterprises, enterprises that qualify as a medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC and enterprises from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This Regulation aims to facilitate access to data for those entities, while ensuring that the corresponding obligations are as proportionate as possible to avoid overreach. At the same time, a small number of very large enterprises 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. Those very large enterprises include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and which existing or new market operators are unable to challenge or contest. Regulation (EU) 2022/1925 of the European Parliament and of the Council ([26]) aims to redress those inefficiencies and imbalances by allowing the Commission to designate an undertaking as a 'gatekeeper', and imposes a number of obligations on such 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. In accordance with Regulation (EU) 2022/1925, and given the unrivalled ability of those undertakings to acquire data, it is not necessary to achieve the objective of this Regulation, and would therefore be disproportionate for data holders made subject to such obligations, to include gatekeeper as beneficiaries of the data access right. Such inclusion would also likely limit the benefits of this Regulation for SMEs, linked to the fairness of the distribution of data value across market actors. This means that an undertaking that provides 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 connected product or related service or by a virtual assistant pursuant to this Regulation. Furthermore, third parties to whom data are made available at the request of the user may not make the data available to a gatekeeper. For instance, the third party may not subcontract the service provision to a gatekeeper. However, this does not prevent third parties from using data processing services offered by a gatekeeper. Nor does it prevent those undertakings from obtaining and using the same data through other lawful means. The access rights provided for in this Regulation contribute to a wider choice of services for consumers. As voluntary agreements between gatekeepers and data holders remain unaffected, the limitation on granting access to gatekeepers would not exclude them from the market or prevent them from offering their services.

(41) Given the current state of technology, it would be overly burdensome on microenterprises and small enterprises to impose further design obligations in relation to connected products manufactured or designed, or the related services provided, by them. That is not the case, however, where a microenterprise or a small enterprise has a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where it is subcontracted to manufacture or design a connected product or to provide a related service. In such situations, the enterprise which has subcontracted the manufacturing or design to a microenterprise or a small enterprise is able to compensate the subcontractor appropriately. A microenterprise or a 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 connected product or a provider of related services. A transitional period should apply to an enterprise that has qualified as a medium-sized enterprise for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise. Such a one-year period allows such a medium-sized enterprise to adjust and prepare before facing competition in the market for services for the connected products that it manufactures on the basis of the access rights provided by this Regulation. Such a transitional period does not apply where such a medium-sized enterprise has a partner enterprise or a linked enterprise that does not qualify as a microenterprise or a small enterprise or where such a medium-sized enterprise was subcontracted to manufacture or design the connected product or to provide the related service.

(42) Taking into account the variety of connected products producing data of different nature, volume and frequency, presenting different levels of data and cybersecurity risks and providing economic opportunities of different value, and for the purpose of ensuring consistency of data sharing practices in the internal market, including across sectors, and to encourage and promote fair data sharing practices even in areas where no such right to data access is provided for, this Regulation provides for horizontal rules on the arrangements for access to data whenever a data holder is obliged by Union law or national legislation adopted in accordance with Union law to make data available to a data recipient. Such access should be based on fair, reasonable, non-discriminatory and transparent terms and conditions. Those general access rules do not apply to obligations to make data available under

Regulation (EU) 2016/679. Voluntary data sharing remains unaffected by those rules. The non-binding model contractual terms for business-to-business data sharing to be developed and recommended by the Commission may help parties to conclude contracts which include fair, reasonable and non-discriminatory terms and conditions and which are to be implemented in a transparent way. The conclusion of contracts, which may include the non-binding model contractual terms, should not mean that the right to share data with third parties is in any way conditional upon the existence of such a contract. Should parties be unable to conclude a contract on data sharing, including with the support of dispute settlement bodies, the right to share data with third parties is enforceable in national courts or tribunals.

(43) On the basis of the principle of contractual freedom, parties should remain free to negotiate the precise conditions for making data available in their contracts within the framework for the general access rules for making data available. Terms of such contracts could include technical and organisational measures, including in relation to data security.

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

(45) Any agreement concluded in business-to-business relations for making data available should be non-discriminatory between comparable categories of data recipients, independently of whether the parties are large enterprises or SMEs. In order to compensate for the lack of information on the conditions contained in different contracts, which makes it difficult for the data recipient to assess whether the terms for making the data available are non-discriminatory, it should be the responsibility of data holders to demonstrate that a contractual term is not discriminatory. It is not unlawful discrimination where a data holder uses different contractual terms for making data available if those differences are justified by objective reasons. Those obligations are without prejudice to Regulation (EU) 2016/679.

(46) In order to promote continued investment in generating and making available valuable data, including investments in relevant technical tools, while at the same time avoiding excessive burdens on access to and the use of data which make data sharing no longer commercially viable, this Regulation contains the principle that in business-to-business relations data holders may request reasonable compensation when obliged pursuant to Union law or national legislation adopted in accordance with Union law to make data available to a data recipient. Such compensation should not be understood to constitute payment for the data itself. The Commission should adopt guidelines on the calculation of reasonable compensation in the data economy.

(47) First, reasonable compensation for meeting the obligation pursuant to Union law or national legislation adopted in accordance with Union law to comply with a request to make data available may include compensation for the costs incurred in making the data available. Those costs may be technical costs, such as the costs necessary for data reproduction, dissemination via electronic means and storage, but not for data collection or production. Such technical costs may also include the costs for processing, necessary to make data available, including costs associated with the formatting of data. Costs related to making the data available may also include the costs of facilitating concrete data sharing requests. They may also vary depending on the volume of the data as well as the arrangements taken for making the data available. Long-term arrangements between data holders and data recipients, for instance via a subscription model or the use of smart contracts, may 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. Second, reasonable compensation may also include a

margin, except regarding SMEs and not-for-profit research organisations. A margin may vary depending on factors related to the data itself, such as volume, format or nature of the data. It may consider the costs for collecting the data. A margin may therefore decrease where the data holder has collected the data for its own business without significant investments or may increase where the investments in the data collection for the purposes of the data holder's business are high. It may be limited or even excluded in situations where the use of the data by the data recipient does not affect the data holder's own activities. The fact that the data is co-generated by a connected product owned, rented or leased by the user could also reduce 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.

(48) It is not necessary to intervene in the case of data sharing between large enterprises, or where the data holder is a small enterprise or a medium-sized enterprise and the data recipient is a large enterprise. In such cases, the enterprises are considered to be capable of negotiating the compensation within the limits of what is reasonable and non-discriminatory.

(49) To protect SMEs from excessive economic burdens which would make it commercially too difficult for them to develop and run innovative business models, the reasonable compensation for making data available to be paid by them should not exceed the costs directly related to making the data available. Directly related costs are those costs which are attributable to individual requests, taking into account that the necessary technical interfaces or related software and connectivity is to be established on a permanent basis by the data holder. The same regime should apply to not-for-profit research organisations.

(50) In duly justified cases, including where there is a need to safeguard consumer participation and competition or to promote innovation in certain markets, regulated compensation for making available specific data types may be provided for in Union law or national legislation adopted in accordance with Union law.

(51) Transparency is an important principle for ensuring that the compensation requested by a data holder is reasonable, or, if the data recipient is an SME or a not-for-profit research organisation, 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 concerned. In order to put data recipients in a position to assess and verify that the compensation complies with the requirements of this Regulation, the data holder should provide to the data recipient sufficiently detailed information for the calculation of the compensation.

(52) 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. Where parties cannot agree on fair, reasonable and non-discriminatory terms and conditions of making data available, dispute settlement bodies should offer a simple, fast and low-cost solution to the parties. While this Regulation only lays down the conditions that dispute settlement bodies need to fulfil to be certified, Member States are free to adopt any specific rules for the certification procedure, including the expiry or revocation of certification. The provisions of this Regulation on dispute settlement should not require Member States to establish dispute settlement bodies.

(53) The dispute settlement procedure under this Regulation is a voluntary procedure that enables users, data holders and data recipients to agree to bring their disputes before dispute settlement bodies.

Therefore, the parties should be free to address a dispute settlement body of their choice, be it within or outside of the Member States in which those parties are established.

(54) To avoid cases in which two or more dispute settlement bodies are seized for the same dispute, in particular in a cross-border situation, a dispute settlement body should be able to 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 tribunal of a Member State.

(55) In order to ensure the uniform application of this Regulation, the dispute settlement bodies should take into account the non-binding model contractual terms to be developed and recommended by the Commission as well as Union or national law specifying data sharing obligations or guidelines issued by sectoral authorities for the application of such law.

(56) Parties to dispute settlement proceedings should not be prevented from exercising their fundamental rights to an effective remedy and 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 tribunal of a Member State. Dispute settlement bodies should make annual activity reports publicly available.

(57) Data holders may apply appropriate technical protection measures to prevent the unlawful disclosure of or access to data. However, those measures should neither discriminate between data recipients, nor hinder access to or the use of data for users or data recipients. In the case of abusive practices on the part of a data recipient, such as misleading the data holder by providing false information with the intent to use the data for unlawful purposes, including developing a competing connected product on the basis of the data, the data holder and, where applicable and where they are not the same person, the trade secret holder or the user can request the third party or data recipient to implement corrective or remedial measures without undue delay. Any such requests, and in particular requests to end the production, offering or placing on the market of goods, derivative data or services, as well as those to end importation, export, storage of infringing goods or their destruction, should be assessed in the light of their proportionality in relation to the interests of the data holder, the trade secret holder or the user.

(58) Where one party is in a stronger bargaining position, there is a risk that that party could leverage such a position to the detriment of the other contracting party when negotiating access to data with the result that access to data is commercially less viable and sometimes economically prohibitive. Such contractual imbalances harm all enterprises without a meaningful ability to negotiate the conditions for access to data, and which may have no choice but to accept take-it-or-leave-it contractual terms. Therefore, unfair contractual terms regulating access to and the use of data, or liability and remedies for the breach or the termination of data related obligations, should not be binding on enterprises when those terms have been unilaterally imposed on those enterprises.

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

(60) Furthermore, the rules on unfair contractual terms should apply only to those elements of a contract that are related to making data available, that is contractual terms concerning access to and use of the

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.

(61) Criteria for identifying unfair contractual terms should be applied only to excessive contractual terms where a stronger bargaining position has been 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. For the purposes of this Regulation, grossly deviating from good commercial practice would include, inter alia, objectively impairing the ability of the party upon whom the term has been unilaterally imposed to protect its legitimate commercial interest in the data in question.

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

(63) In situations of exceptional need, it may be necessary for public sector bodies, the Commission, the European Central Bank or Union bodies to use in the performance of their statutory duties in the public interest existing data, including, where relevant, accompanying metadata, to respond to public emergencies or in other exceptional cases. Exceptional needs are circumstances which are unforeseeable and limited in time, in contrast to other circumstances which might be planned, scheduled, periodic or frequent. While the notion of ‘data holder’ does not, generally, include public sector bodies, it may include public undertakings. 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, microenterprises and small enterprises should only be under the obligation to provide data to public sector bodies, the Commission, the European Central Bank or Union bodies in situations of exceptional need where such data is required to respond to a public emergency and the public sector body, the Commission, the European Central Bank or the Union body is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions.

(64) In the case of public emergencies, such as public health emergencies, emergencies resulting from natural disasters including those aggravated by climate change and environmental degradation, as well as human-induced major disasters, such as major cybersecurity incidents, the public interest resulting from the use of the data will outweigh the interests of the data holders to dispose freely of the data they hold. In such a case, data holders should be placed under an obligation to make the data available to public sector bodies, the Commission, the European Central Bank or Union bodies upon their request. The existence of a public emergency should be determined or declared in accordance with Union or national law and based on the relevant procedures, including those of the relevant international

organisations. In such cases, the public sector body should demonstrate that the data in scope of the request could not otherwise be obtained in a timely and effective manner and under equivalent conditions, for instance by way of the voluntary provision of data by another enterprise or the consultation of a public database.

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

(66) This Regulation should not apply to, or pre-empt, voluntary arrangements for the exchange of data between private and public entities, including the provision of data by SMEs, and is without prejudice to Union legal acts providing for mandatory information requests by public entities to private entities. Obligations placed on data holders to provide data that are motivated by needs of a non-exceptional nature, in particular where the range of data and of data holders is known or where data use can take place on a regular basis, as in the case of reporting obligations and internal market obligations, should not be affected by this Regulation. Requirements to access data to verify compliance with applicable rules, including 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.

(67) This Regulation complements and is without prejudice to the Union and national law providing for access to and the use of data for statistical purposes, in particular Regulation (EC) No 223/2009 of the European Parliament and of the Council ([27]) as well as national legal acts related to official statistics.

(68) For the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes, public sector bodies, the Commission, the European Central Bank or Union bodies should rely on their powers under Union or national law. This Regulation accordingly does not affect legislative acts on the sharing, access to and use of data in those areas.

(69) In accordance with Article 6(1) and (3) of Regulation (EU) 2016/679, a proportionate, limited and predictable framework at Union level is necessary when providing for the legal basis for the making available of data by data holders, in cases of exceptional needs, to public sector bodies, the Commission, the European Central Bank or Union bodies, both to ensure legal certainty and to minimise the administrative burdens placed on businesses. To that end, data requests from public sector bodies, the Commission, the European Central Bank or Union bodies to data holders should be

specific, transparent and proportionate in 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 carry out its specific tasks in the public interest. The request should also respect the legitimate interests of the data holder 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 the Commission, the European Central Bank or Union bodies. To ensure transparency, data requests made by the Commission, the European Central Bank or Union bodies should be made public without undue delay by the entity requesting the data. The European Central Bank and Union bodies should inform the Commission of their requests. If the data request has been made by a public sector body, that body should also notify the data coordinator of the Member State where the public sector body is established. Online public availability of all requests should be ensured. Upon the receipt of a notification of a data request, the competent authority can decide to assess the lawfulness of the request and exercise its functions in relation to the enforcement and application of this Regulation. Online public availability of all requests made by public sector bodies should be ensured by the data coordinator.

(70) The objective of the obligation to provide the data is to ensure that public sector bodies, the Commission, the European Central Bank or Union bodies have the necessary knowledge to respond to, prevent or recover from public emergencies or to maintain the capacity to fulfil specific tasks explicitly provided for by law. The data obtained by those entities may be commercially sensitive. Therefore, neither Regulation (EU) 2022/868 nor Directive (EU) 2019/1024 of the European Parliament and of the Council ([28]) should apply to data made available under this Regulation and should not be considered as open data available for reuse by third parties. This however should not affect the applicability of Directive (EU) 2019/1024 to the reuse of official statistics for the production of which data obtained pursuant to this Regulation was used, provided the reuse does not include the underlying data. In addition, provided the conditions laid down in this Regulation are met, the possibility of sharing the data for conducting research or for the development, production and dissemination of official statistics should not be affected. Public sector bodies should also be allowed to exchange data obtained pursuant to this Regulation with other public sector bodies, the Commission, the European Central Bank or Union bodies in order to address the exceptional needs for which the data has been requested.

(71) Data holders should have the possibility to either decline a request made by a public sector body, the Commission, the European Central Bank or a Union body or seek its modification without undue delay and, in any event, no later than within a period of five or 30 working days, depending on the nature of the exceptional need invoked in the request. Where relevant, the data holder should have this possibility where it does not have control over the data requested, namely where it does not have immediate access to the data and cannot determine its availability. A valid reason not to make the data available should exist if it can be shown that the request is similar to a previously submitted request for the same purpose by another public sector body or the Commission, the European Central Bank or a Union body and the data holder has not been notified of the erasure of the data pursuant to this Regulation. A data holder declining the request or seeking its modification should communicate the underlying justification to the public sector body, the Commission, the European Central Bank or a Union body requesting the data. Where the *sui generis* database rights under Directive 96/9/EC of the European Parliament and of the Council ([29]) apply in relation to the requested datasets, data holders should exercise their rights in such a way that does not prevent the public sector body, the

Commission, the European Central Bank or Union body from obtaining the data, or from sharing it, in accordance with this Regulation.

(72) In the case of an exceptional need related to a public emergency response, public sector bodies should use non-personal data wherever possible. In the case of requests on the basis of an exceptional need not related to a public emergency, personal data cannot be requested. Where personal data fall within the scope of the request, the data holder should anonymise the data. Where it is strictly necessary to include personal data in the data to be made available to a public sector body, the Commission, the European Central Bank or a Union body or where anonymisation proves impossible, the entity requesting the data should demonstrate the strict necessity and the specific and limited purposes for processing. The applicable rules on personal data protection should be complied with. The making available of the data and their subsequent use should be accompanied by safeguards for the rights and interests of individuals concerned by those data.

(73) Data made available to public sector bodies, the Commission, the European Central Bank or Union bodies on the basis of an exceptional need should be used only for the purposes for which they were requested, unless the data holder that made the data available has expressly agreed for the data to be used for other purposes. The data should be erased once it is no longer necessary for the purposes stated in the request, unless agreed otherwise, and the data holder should be informed thereof. This Regulation builds on the existing access regimes in the Union and the Member States and does not change the national law on public access to documents in the context of transparency obligations. Data should be erased once it is no longer needed to comply with such transparency obligations.

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

(75) When the safeguarding of a significant public good is at stake, such as responding to public emergencies, the public sector body, the Commission, the European Central Bank or the Union body concerned should not be expected to compensate enterprises for the data obtained. Public emergencies are rare events and not all such emergencies require the use of data held by enterprises. At the same time, the obligation to provide data might constitute a considerable burden on microenterprises and small enterprises. They should therefore be allowed to claim compensation even in the context of a public emergency response. The business activities of the data holders are therefore not likely to be negatively affected as a consequence of the public sector bodies, the Commission, the European Central Bank or Union bodies having recourse to this Regulation. However, as cases of an exceptional need, other than cases of responding to public emergencies, might be more frequent, data holders should in such cases be entitled to a reasonable compensation which should not exceed the technical and organisational costs incurred in complying with the request and the reasonable margin required for making the data available to the public sector body, the Commission, the European Central Bank or the Union body. The compensation should not be understood as constituting payment for the data itself or

as being compulsory. Data holders should not be able to claim compensation where national law prevents national statistical institutes or other national authorities responsible for the production of statistics from compensating data holders for making data available. The public sector body, the Commission, the European Central Bank or the Union body concerned should be able to challenge the level of compensation requested by the data holder by bringing the matter to the competent authority of the Member State where the data holder is established.

(76) A public sector body, the Commission, the European Central Bank or a Union body should be entitled to share the data it has obtained pursuant to the request with other entities or persons when this is necessary to carry out scientific research activities or analytical activities it cannot perform itself, provided that those activities are compatible with the purpose for which the data was requested. It should inform the data holder of such sharing in a timely manner. Such data may also be shared under the same circumstances with the national statistical institutes and Eurostat for the development, production and dissemination of official statistics. Such research activities should, however, be compatible with the purpose for which the data was requested and the data holder should be informed about the further sharing of the data it has provided. Individuals conducting research or research organisations with whom those data may be shared should act either on a not-for-profit basis or in the context of a public-interest mission recognised by the State. Organisations upon which commercial undertakings have a significant influence, allowing such undertakings to exercise control due to structural situations which could result in preferential access to the results of the research, should not be considered to be research organisations for the purposes of this Regulation.

(77) In order to handle a cross-border public emergency or another exceptional need, data requests may be addressed to data holders in Member States other than that of the requesting public sector body. In such a case, the requesting public sector body should notify the competent authority of the Member State where the data holder is established in order to allow it to examine the request against the criteria established in this Regulation. The same should apply to requests made by the Commission, the European Central Bank or a Union body. Where personal data are requested, the public sector body should notify the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 in the Member State where the public sector body is established. The competent authority concerned should be entitled to advise the public sector body, the Commission, the European Central Bank or the Union body to cooperate with the public sector bodies of the Member State in which the data holder is established on the need to ensure a minimised administrative burden on the data holder. When the competent authority has substantiated objections as regards the compliance of the request with this Regulation, it should reject the request of the public sector body, the Commission, the European Central Bank or the Union body, which should take those objections into account before taking any further action, including resubmitting the request.

(78) The ability of customers of data processing services, including cloud and edge services, to switch from one data processing service to another while maintaining a minimum functionality of service and without downtime of services, or to use the services of several providers simultaneously without undue obstacles and data transfer costs, is a key condition for a more competitive market with lower entry barriers for new providers of data processing services, and for ensuring further resilience for the users of those services. Customers benefiting from free-tier offerings should also benefit from the provisions for switching that are laid down in this Regulation, so that those offerings do not result in a lock-in situation for customers.

(79) Regulation (EU) 2018/1807 of the European Parliament and of the Council ([30]) encourages providers of data processing services to develop and effectively implement self-regulatory codes of conduct covering best practices for, inter alia, facilitating the switching of providers of data processing services 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 for providers of data processing services to eliminate pre-commercial, commercial, technical, contractual and organisational obstacles, which are not limited to reduced speed of data transfer at the customer's exit, which hamper effective switching between data processing services.

(80) Data processing services should cover services that allow ubiquitous and on-demand network access to a configurable, scalable and elastic shared pool of distributed computing resources. Those computing resources include resources such as networks, servers or other virtual or physical infrastructure, software, including software development tools, storage, applications and services. The capability of the customer of the data processing service to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the provider of data processing services could be described as requiring minimal management effort and as entailing minimal interaction between provider and customer. The term 'ubiquitous' is used to describe the computing capabilities 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.

(81) The generic concept 'data processing services' covers a substantial number of services with a very broad range of different purposes, functionalities and technical set-ups. As commonly understood by providers and users and in line with broadly used standards, data processing services fall into one or more of the following three data processing service delivery models, namely Infrastructure as a Service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS). Those service delivery models represent a specific, pre-packaged combination of ICT resources offered by a provider of data processing service. Those three fundamental data processing delivery models are further complemented by emerging variations, each comprised of a distinct combination of ICT resources, such as Storage as a Service and Database as a Service. Data processing services can be categorised in a more granular way and divided into a non-exhaustive list of sets of data processing services that share the same primary objective and main functionalities as well as the same type of data processing

models, that are not related to the service's operational characteristics (same service type). Services falling under the same service type may share the same data processing service model, however, two databases might appear to share the same primary objective, but after considering their data processing model, distribution model and the use cases that they are targeted at, such databases could fall into a more granular subcategory of similar services. Services of the same service type may have different and competing characteristics such as performance, security, resilience, and quality of service.

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

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

(84) This Regulation aims to facilitate switching between data processing services, which encompasses conditions and actions that are necessary for a customer to terminate a contract for a data processing service, to conclude one or more new contracts with different providers of data processing services, to port its exportable data and digital assets, and where applicable, benefit from functional equivalence.

(85) Switching is a customer-driven operation consisting of several steps, including data extraction, which refers to the downloading of data from the ecosystem of the source provider of data processing services; transformation, where the data is structured in a way that does not match the schema of the target location; and 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 a different provider should also be considered to be switching. The switching process is sometimes managed on behalf of the customer by a third-party entity. Accordingly, all rights and obligations of the customer established by this Regulation, including the obligation to cooperate in good faith, should be understood to apply to such a third-party entity in those circumstances. Providers of data processing services and customers have different levels of responsibilities, depending on the steps of the process referred to. For instance, the source provider of data processing services is responsible for extracting

the data to a machine-readable format, but it is the customer and the destination provider of data processing services who are to upload the data to the new environment, unless a specific professional transition service has been obtained. A customer who intends to exercise rights related to switching, which are provided for in this Regulation, should inform the source provider of data processing services of the decision to either switch to a different provider of data processing services, switch to an on-premises ICT infrastructure or to delete that customer's assets and erase its exportable data.

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

(87) Data processing services are used across sectors and vary in complexity and service type. This is an important consideration with regard to the porting process and timeframes. Nonetheless, an extension of the transitional period on the grounds of technical unfeasibility to allow the finalisation of the switching process in the given timeframe should be invoked only in duly justified cases. The burden of proof in that regard should fall fully on the provider of the data processing service concerned. This is without prejudice to the exclusive right of the customer to extend the transitional period once for a period that the customer considers to be more appropriate for its own purposes. The customer may evoke that right to an extension prior to or during the transitional period, taking into account that the contract remains applicable during the transitional period.

(88) Switching charges are charges imposed by providers of data processing services on the customers for the switching process. Typically, those charges are intended to pass on costs which the source provider of data processing services may incur because of the switching process to the customer who wishes to switch. Common examples of switching charges are costs related to the transit of data from one provider of data processing services to another or to an on-premises ICT infrastructure (data egress charges) or the costs incurred for specific support actions during the switching process. Unnecessarily high data egress charges and other unjustified charges unrelated to actual switching costs inhibit customers from switching, restrict the free flow of data, have the potential to limit competition and cause lock-in effects for the customers by reducing incentives to choose a different or additional service provider. Switching charges should therefore be abolished after three years from the date of entry into force of this Regulation. Providers of data processing services should be able to impose reduced switching charges up to that date.

(89) A source provider of data processing services should be able to outsource certain tasks and compensate third-party entities in order to comply with the obligations provided for in this Regulation. A customer should not bear the 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 to be unjustified unless they cover work undertaken by the provider of data processing services at the customer's request for additional support in the switching process which goes beyond the switching obligations of the provider as expressly provided for in this Regulation. Nothing in this Regulation prevents a customer from compensating third-party entities for support in the migration process or

parties from agreeing on contracts for data processing services of a fixed duration, including proportionate early termination penalties to cover the early termination of such contracts, in accordance with Union or national law. In order to foster competition, the gradual withdrawal of the charges associated with switching between different providers of data processing services should specifically include data egress charges imposed by a provider of data processing services on a customer. Standard service fees for the provision of the data processing services themselves are not switching charges. Those standard service fees are not subject to withdrawal and remain applicable until the contract for the provision of the relevant services ceases to apply. This Regulation allows the customer to request the provision of additional services that go beyond the provider's switching obligations under this Regulation. Those additional services, can be performed and charged for by the provider when they are performed at the customer's request and the customer agrees to the price of those services in advance.

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

(91) 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 remaining bound by this Regulation's obligations regarding their own service offerings.

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

(93) Providers of data processing services should also be required to remove existing obstacles and not impose new ones, including for customers wishing to switch to an on-premises ICT infrastructure. Obstacles can, inter alia, be of a pre-commercial, commercial, technical, contractual or organisational nature. Providers of data processing services should also be required to remove obstacles to unbundling a specific individual service from other data processing services provided under a contract

and make the relevant service available for switching, in the absence of major and demonstrated technical obstacles that prevent such unbundling.

(94) Throughout the switching process, a high level of security should be maintained. This means that the source provider of data processing services should extend the level of security to which it committed for the service to all technical arrangements for which such provider is responsible during the switching process, such as network connections or physical devices. Existing rights relating to the termination of contracts, including those introduced by Regulation (EU) 2016/679 and Directive (EU) 2019/770 of the European Parliament and of the Council ([31]) should not be affected. This Regulation should not be understood to prevent a provider of data processing services from providing to customers new and improved services, features and functionalities or from competing with other providers of data processing services on that basis.

(95) The information to be provided by providers of data processing services to the customer could support the customer's exit strategy. That information should include procedures for initiating switching from the data processing service; the machine-readable data formats to which the user's data can be exported; the tools intended to export data, including open interfaces as well as information on compatibility with harmonised standards or common specifications based on open interoperability specifications; information on known technical restrictions and limitations that could have an impact on the switching process; and the estimated time necessary to complete the switching process.

(96) To facilitate interoperability and switching between data processing services, users and providers of data processing services should consider the use of implementation and compliance tools, in particular those published by the Commission in the form of an EU Cloud Rulebook and a Guidance on public procurement of data processing services. In particular, standard contractual clauses are beneficial because they increase confidence in data processing services, create a more balanced relationship between users and providers of data processing services and improve legal certainty with regard to the conditions that apply for switching to other data processing services. In that context, users and providers of data processing services should consider the use of standard contractual clauses or other self-regulatory compliance tools provided that they fully comply with this Regulation, developed by relevant bodies or expert groups established under Union law.

(97) In order to facilitate switching between data processing services, all parties involved, including both source and destination providers of data processing services, should cooperate in good faith to make the switching process effective, enable the secure and timely transfer of necessary data in a commonly used, machine-readable format, and by means of open interfaces, while avoiding service disruptions and maintaining continuity of the service.

(98) Data processing services which concern services of which the majority of main features has been custom-built to respond to the specific demands of an individual customer or where all components have been developed for the purposes of an individual customer should be exempted from some of the obligations applicable to data processing service switching. This should not include services which the provider of data processing services offers at a broad commercial scale via its service catalogue. It is among the obligations of the provider of data processing services to duly inform prospective customers of such services, prior to the conclusion of a contract, of the obligations laid down in this Regulation that do not apply to the relevant services. Nothing prevents the provider of data processing services from eventually deploying such services at scale, in which case that provider would have to comply with all obligations for switching laid down in this Regulation.

(99) In line with the minimum requirement allowing switching between providers of data processing services, this Regulation also aims to improve interoperability for in-parallel use of multiple data processing services with complementary functionalities. This relates to situations in which customers do not terminate a contract to switch to a different provider of data processing services, but where multiple services of different providers are used in parallel, in an interoperable manner, to benefit from the complementary functionalities of the different services in the set-up of the customer's system. However, it is recognised that the egress of data from one provider of data processing services to another in order to facilitate the in-parallel use of services can be an ongoing activity, in contrast with the one-off egress required as part of the switching process. Providers of data processing services should therefore continue to be able to impose data egress charges, not exceeding the costs incurred, for the purposes of in-parallel use after three years from the date of entry into force of this Regulation. This is important, inter alia, for the successful deployment of multi-cloud strategies, which allow customers to implement future-proof ICT strategies and which decrease dependence on individual providers of data processing services. Facilitating a multi-cloud approach for customers of data processing services can also contribute to increasing their digital operational resilience, as recognised for financial service institutions in Regulation (EU) 2022/2554 of the European Parliament and of the Council ([32]).

(100) Open interoperability specifications and standards developed in accordance with Annex II to Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([33]) in the field of interoperability and portability are expected to enable a multi-vendor cloud environment, which is a key requirement for open innovation in the European data economy. As the market adoption of identified standards under the cloud standardisation coordination (CSC) initiative concluded in 2016 has been limited, it is also necessary that the Commission relies on parties in the market to develop relevant open interoperability specifications to keep up with the fast pace of technological development in this industry. Such open interoperability specifications can then be adopted by the Commission in the form of common specifications. In addition, where market-driven processes have not demonstrated a capacity to establish common specifications or standards that facilitate effective cloud interoperability at the PaaS and SaaS levels, the Commission should be able, on the basis of this Regulation and in accordance with Regulation (EU) No 1025/2012, to request European standardisation bodies to develop such standards for specific service types where such standards do not yet exist. In addition to this, the Commission will encourage parties in the market to develop relevant open interoperability specifications. After consulting stakeholders, the Commission, by means of implementing acts, should be able to mandate the use of harmonised standards for interoperability or common specifications for specific service types through a reference in a central Union standards repository for the interoperability of data processing services. Providers of data processing services should ensure compatibility with those harmonised standards and common specifications based on open interoperability specifications, which should not have an adverse impact on the security or integrity of data. Harmonised standards for the interoperability of data processing services and common specifications based on open interoperability specifications will be referenced only if they comply with the criteria specified in this Regulation, which have the same meaning as the requirements in Annex II to Regulation (EU) No 1025/2012 and the interoperability facets defined under the international standard ISO/IEC 19941:2017. In addition, standardisation should take into account the needs of SMEs.

(101)Third countries may adopt laws, regulations and other legal acts that aim to directly transfer or provide 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 under the national law of the relevant Member State, in particular regarding the protection of fundamental rights of the individual, such as the right to security and the right to an effective remedy, or the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data, including the protection of trade secrets, and the protection of intellectual property rights, including its contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, transfer of or access to non-personal data should be allowed only 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 third-country court or tribunal which is empowered to take duly into account the relevant legal interests of the provider of such data. Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested before granting access to those data in order to verify the presence of a potential conflict of such access with Union or national law, such as that on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality.

(102)To foster further trust in data, it is important that safeguards to ensure control of their data by Union citizens, the public sector bodies and businesses are implemented to the extent possible. In addition, Union law, values and standards regarding, inter alia, security, data protection and privacy, and consumer protection should be upheld. In order to prevent unlawful governmental access to non-personal data by third-country authorities, providers of data processing services subject to this Regulation, such as cloud and edge services, should take all reasonable measures to prevent access to systems on which non-personal data are stored, including, where relevant, through the encryption of data, frequent submission to audits, verified adherence to relevant security reassurance certification schemes, and by the modification of corporate policies.

(103)Standardisation and semantic interoperability should play a key role to provide technical solutions to ensure interoperability within and among common European data spaces which are purpose or sector specific or cross-sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives. This Regulation lays down certain essential requirements for interoperability. Participants in data spaces that offer data or data services to other participants, which are entities facilitating or engaging in data sharing within common European data spaces, including data holders, should comply with those requirements insofar as elements under their control are concerned. Compliance with those rules can be ensured by adhering to the essential requirements laid down in this Regulation, or presumed by complying with harmonised standards or common specifications via a presumption of conformity. In order to facilitate conformity with the requirements

for interoperability, it is necessary to provide for a presumption of conformity of interoperability solutions that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012, which represents the framework by default to elaborate standards that provide for such presumptions. The Commission should assess barriers to interoperability and prioritise standardisation needs, on the basis of which it may request one or more European standardisation organisations, pursuant to Regulation (EU) No 1025/2012, to draft harmonised standards which satisfy the essential requirements laid down in this Regulation. Where such requests do not result in harmonised standards or such harmonised standards are insufficient to ensure conformity with the essential requirements of this Regulation, the Commission should be able to adopt common specifications in those areas provided that in so doing it duly respects the role and functions of standardisation organisations. Common specification should be adopted only as an exceptional fall-back solution to facilitate compliance with the essential requirements of this Regulation, or when the standardisation process is blocked, or when there are delays in the establishment of appropriate harmonised standards. Where a delay is due to the technical complexity of the standard in question, this should be considered by the Commission before contemplating the establishment of common specifications. Common specifications should be developed in an open and inclusive manner and take into account, where relevant, the advice of the European Data Innovation Board (EDIB) established by Regulation (EU) 2022/868. Additionally, common specifications in different sectors could be adopted, in accordance with Union or national law, on the basis of specific needs of those sectors. Furthermore, the Commission should be enabled to mandate the development of harmonised standards for the interoperability of data processing services.

(104) To promote the interoperability of tools for the automated execution of data sharing agreements, it is necessary to lay down essential requirements for smart contracts which professionals create for others or integrate in applications that support the implementation of agreements for data sharing. In order to facilitate the conformity of such smart contracts with those essential requirements, it is necessary to provide for a presumption of conformity of smart contracts that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012. The notion of ‘smart contract’ in this Regulation is technologically neutral. Smart contracts can, for example, be connected to an electronic ledger. The essential requirements should apply only to the vendors of smart contracts, although not where they develop smart contracts in-house exclusively for internal use. The essential requirement to ensure that smart contracts can be interrupted and terminated implies mutual consent by the parties to the data sharing agreement. The applicability of the relevant rules of civil, contractual and consumer protection law to data sharing agreements remains or should remain unaffected by the use of smart contracts for the automated execution of such agreements.

(105) To demonstrate fulfilment of the essential requirements of this Regulation, the vendor of a smart contract, or in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available in the context of this Regulation, should perform a conformity assessment and issue an EU declaration of conformity. Such a conformity assessment should be subject to the general principles set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council ([34]) and Decision No 768/2008/EC of the European Parliament and of the Council ([35]).

(106) Besides the obligation on professional developers of smart contracts to comply with essential requirements, it is also important to encourage those participants within data spaces that offer data or

data-based services to other participants within and across common European data spaces to support interoperability of tools for data sharing including smart contracts.

(107) In order to ensure the application and enforcement of this Regulation, Member States should designate one or more competent authorities. If a Member State designates more than one competent authority, it should also designate from among them a data coordinator. Competent authorities should cooperate with each other. Through the exercise of their powers of investigation in accordance with applicable national procedures, competent authorities should be able to search for and obtain information, in particular in relation to the activities of entities within their competence and, including in the context of joint investigations, with due regard to the fact that oversight and enforcement measures concerning an entity under the competence of another Member State should be adopted by the competent authority of that other Member State, where relevant, in accordance with the procedures relating to cross-border cooperation. Competent authorities should assist each other in a timely manner, in particular when a competent authority in a Member State holds relevant information for an investigation carried out by the competent authorities in other Member States, or is able to gather such information to which the competent authorities in the Member State where the entity is established do not have access. Competent authorities and data coordinators should be identified in a public register maintained by the Commission. The data coordinator could be an additional means for facilitating cooperation in cross-border situations, such as when a competent authority from a given Member State does not know which authority it should approach in the data coordinator's Member State, for example where the case is related to more than one competent authority or sector. The data coordinator should act, inter alia, as a single point of contact for all issues related to the application of this Regulation. Where no data coordinator has been designated, the competent authority should assume the tasks assigned to the data coordinator under this Regulation. The authorities responsible for the supervision of compliance with data protection law and competent authorities designated under Union or national law should be responsible for the application of this Regulation in their areas of competence. In order to avoid conflicts of interest, the competent authorities responsible for the application and enforcement of this Regulation in the area of making data available following a request on the basis of an exceptional need should not benefit from the right to submit such a request.

(108) In order to enforce their rights under this Regulation, natural and legal persons should be entitled to seek redress for infringements of their rights under this Regulation by lodging complaints. The data coordinator should, upon request, provide all the necessary information to natural and legal persons for the lodging of their complaints with the appropriate competent authority. Those authorities should be obliged to cooperate to ensure a complaint is appropriately handled and resolved effectively and in a timely manner. In order to make use of the consumer protection cooperation network mechanism and to enable representative actions, this Regulation amends the Annexes to Regulation (EU) 2017/2394 of the European Parliament and of the Council ([36]) and Directive (EU) 2020/1828 of the European Parliament and of the Council ([37]).

(109) Competent authorities should ensure that infringements of the obligations laid down in this Regulation are subject to penalties. Such penalties could include financial penalties, warnings, reprimands or orders to bring business practices into compliance with the obligations imposed by this Regulation. Penalties established by the Member States should be effective, proportionate and dissuasive, and should take into account the recommendations of the EDIB, thus contributing to achieving the greatest possible level of consistency in the establishment and application of penalties.

Where appropriate, competent authorities should make use of interim measures to limit the effects of an alleged infringement while the investigation of that infringement is ongoing. In so doing, they should take into account, inter alia the nature, gravity, scale and duration of the infringement in view of the public interest at stake, the scope and kind of activities carried out, and the economic capacity of the infringing party. They should also take into account whether the infringing party systematically or recurrently fails to comply with its obligations under this Regulation. In order to ensure that the principle of *ne bis in idem* is respected, and in particular to avoid that the same infringement of the obligations laid down in this Regulation is penalised more than once, a Member State that intends to exercise its competence in relation to an infringing party that is not established and has not designated a legal representative in the Union should, without undue delay, inform all data coordinators as well as the Commission.

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

(111) In order to help enterprises to draft and negotiate contracts, the Commission should develop and recommend non-binding 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. Those model contractual terms should be primarily a practical tool to help in particular SMEs to conclude a contract. When used widely and integrally, those model contractual terms should also have the beneficial effect of influencing the design of contracts regarding access to and the use of data and therefore lead more broadly towards fairer contractual relations when accessing and sharing data.

(112) In order to eliminate the risk that holders of data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service or other machine-generated data, claim the *sui generis* right under Article 7 of Directive 96/9/EC, and in so doing hinder, in particular, the effective exercise of the right of users to access and use data and the right to share data with third parties under this Regulation, it should be clarified that the *sui generis* right does not apply to such databases. That does not affect the possible application of the *sui generis* right under Article 7 of Directive 96/9/EC to databases containing data falling outside the scope of this

Regulation, provided that the requirements for protection pursuant to paragraph 1 of that Article are fulfilled.

(113) 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 in order to establish a monitoring mechanism on switching charges imposed by providers of data processing services on the market, and to further specify the essential requirements in respect of interoperability for participants in data spaces that offer data or data services to other participants. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([38]). 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.

(114) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of the adoption of common specifications to ensure the interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces, common specifications on the interoperability of data processing services, and common specifications on the interoperability of smart contracts. Implementing powers should also be conferred on the Commission for the purpose of publishing the references of harmonised standards and common specifications for the interoperability of data processing services in a central Union standards repository for the interoperability of data processing services. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([39]).

(115) 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 the technical aspects of data access, such as interfaces for data access, or how data access could be provided, for example directly from the product or via data intermediation services. Such rules may also include limits on the rights of data holders to access or use user data, or other aspects beyond data access and use, such as governance aspects or security requirements, including cybersecurity requirements. This Regulation should also be without prejudice to more specific rules in the context of the development of common European data spaces or, subject to the exceptions provided for in this Regulation, to Union and national law providing for access to and authorising the use of data for scientific research purposes.

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

(117) In order to allow actors within the scope of this Regulation to adapt to the new rules provided for herein, and to make the necessary technical arrangements, those rules should apply from 12 September 2025.

(118) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered their opinion on 4 May 2022.

(119)Since the objectives of this Regulation, namely ensuring fairness in the allocation of value from data among actors in the data economy and fostering fair access to and use of data in order to contribute to establishing a genuine internal market for data, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale or effects of the action and cross-border use of data, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives,

HAVE ADOPTED THIS REGULATION:

## CHAPTER I
## GENERAL PROVISIONS

*Article 1*

**Subject matter and scope**

1. This Regulation lays down harmonised rules, inter alia, on:

(a) the making available of product data and related service data to the user of the connected product or related service;

(b) the making available of data by data holders to data recipients;

(c) the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there is an exceptional need for those data for the performance of a specific task carried out in the public interest;

(d) facilitating switching between data processing services;

(e) introducing safeguards against unlawful third-party access to non-personal data; and

(f) the development of interoperability standards for data to be accessed, transferred and used.

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

(a) Chapter II applies to data, with the exception of content, concerning the performance, use and environment of connected products and related services;

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

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

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

(e) Chapter VI applies to any data and services processed by providers of data processing services;

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

3. This Regulation applies to:

(a) manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;

(b) users in the Union of connected products or related services as referred to in point (a);

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

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

(e) public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need for those data for the performance of a specific task carried out in the public interest and to the data holders that provide those data in response to such request;

(f) providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;

(g) participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.

4. Where this Regulation refers to connected products or related services, such references are also understood to include virtual assistants insofar as they interact with a connected product or related service.

5. This Regulation is without prejudice to Union and national law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, which shall apply to personal data processed in connection with the rights and obligations laid down herein, in particular Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive 2002/58/EC, including the powers and competences of supervisory authorities and the rights of data subjects. Insofar as users are data subjects, the rights laid down in Chapter II of this Regulation shall complement the rights of access by data subjects and rights to data portability under Articles 15 and 20 of Regulation (EU) 2016/679. In the event of a conflict between this Regulation and Union law on the protection of personal data or privacy, or national legislation adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data or privacy shall prevail.

6. This Regulation does not apply to or pre-empt voluntary arrangements for the exchange of data between private and public entities, in particular voluntary arrangements for data sharing.

This Regulation does not affect Union or national legal acts providing for the sharing of, access to and the use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties, or for customs and taxation purposes, in particular Regulations (EU) 2021/784, (EU) 2022/2065 and (EU) 2023/1543 and Directive (EU) 2023/1544, or international cooperation in that area. This Regulation does not apply to the collection or sharing of, access to or the use of data under Regulation (EU) 2015/847 and Directive (EU) 2015/849. This Regulation does not apply to areas that fall outside the scope of Union law and in any event does not affect the competences of the Member States concerning public security, defence or national security, regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences, or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and the maintenance of law and order. This Regulation does not affect the competences of the Member States concerning customs and tax administration or the health and safety of citizens.

7. This Regulation complements the self-regulatory approach of Regulation (EU) 2018/1807 by adding generally applicable obligations on cloud switching.

8. This Regulation is without prejudice to Union and national legal acts providing for the protection of intellectual property rights, in particular Directives 2001/29/EC, 2004/48/EC and (EU) 2019/790.

9. This Regulation complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection, and to protect their health, safety and economic interests, in particular Directives 93/13/EEC, 2005/29/EC and 2011/83/EU.

10. This Regulation does not preclude the conclusion of voluntary lawful data sharing contracts, including contracts concluded on a reciprocal basis, which comply with the requirements laid down in this Regulation.

*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;

(2) ‘metadata’ means a structured description of the contents or the use of data facilitating the discovery or use of that data;

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

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

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

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

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

(8) ‘data processing service’ means a digital service that is provided to a customer and that enables 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 that can be rapidly provisioned and released with minimal management effort or service provider interaction;

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

(10) ‘data intermediation service’ means data intermediation service as defined in Article 2, point (11), of Regulation (EU) 2022/868;

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

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

(13) ‘data holder’ means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;

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

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

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

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

(18) ‘trade secret’ means trade secret as defined in Article 2, point (1), of Directive (EU) 2016/943;

(19) ‘trade secret holder’ means a trade secret holder as defined in Article 2, point (2), of Directive (EU) 2016/943;

(20) ‘profiling’ means profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679;

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

(22) ‘placing on the market’ means the first making available of a connected product on the Union market;

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

(24) ‘enterprise’ means a natural or legal person that, 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;

(25) ‘small enterprise’ means a small enterprise as defined in Article 2(2) of the Annex to Recommendation 2003/361/EC;

(26) ‘microenterprise’ means a microenterprise as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC;

(27) ‘Union bodies’ means the Union bodies, offices and agencies set up by or pursuant to acts adopted on the basis of the Treaty on European Union, the TFEU or the Treaty establishing the European Atomic Energy Community;

(28) ‘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;

(29) ‘public emergency’ means an exceptional situation, limited in time, such as a public health emergency, an emergency resulting from natural disasters, a human-induced major disaster, including a major cybersecurity incident, negatively affecting the population of the Union or the whole or part of a Member State, with a risk of serious and lasting repercussions for living conditions or economic stability, financial stability, or the substantial and immediate degradation of economic assets in the Union or the relevant Member State and which is determined or officially declared in accordance with the relevant procedures under Union or national law;

(30) ‘customer’ means a natural or legal person that has entered into a contractual relationship with a provider of data processing services with the objective of using one or more data processing services;

(31) ‘virtual assistants’ means software that can process demands, tasks or questions including those based on audio, written input, gestures or motions, and that, based on those demands, tasks or questions, provides access to other services or controls the functions of connected products;

(32) ‘digital assets’ means elements in digital form, including applications, for which the customer has the right of use, independently from the contractual relationship with the data processing service it intends to switch from;

(33) ‘on-premises ICT infrastructure’ means ICT infrastructure and computing resources owned, rented or leased by the customer, located in the data centre of the customer itself and operated by the customer or by a third-party;

(34) ‘switching’ means the process involving a source provider of data processing services, a customer of a data processing service and, where relevant, a destination provider of data processing services, whereby the customer of a data processing service changes from using one data processing service to using another data processing service of the same service type, or other service, offered by a different provider of data processing services, or to an on-premises ICT infrastructure, including through extracting, transforming and uploading the data;

(35) ‘data egress charges’ means data transfer fees charged to customers for extracting their data through the network from the ICT infrastructure of a provider of data processing services to the system of a different provider or to on-premises ICT infrastructure;

(36) ‘switching charges’ means charges, other than standard service fees or early termination penalties, imposed by a provider of data processing services on a customer for the actions mandated by this Regulation for switching to the system of a different provider or to on-premises ICT infrastructure, including data egress charges;

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

(38) ‘exportable data’, for the purpose of Articles 23 to 31 and Article 35, 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 assets or data protected by intellectual property rights, or constituting a trade secret, of providers of data processing services or third parties;

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

(40) ‘interoperability’ means the ability of two or more data spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions;

(41) open interoperability specification’ means a technical specification in the field of information and communication technologies which is performance oriented towards achieving interoperability between data processing services;

(42) ‘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;

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

## CHAPTER II

## BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING

*Article 3*

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

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

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

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

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

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

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

3. Before concluding a contract for the provision of a related service, the provider of such related service shall provide at least the following information to the user, in a clear and comprehensible manner:

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

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

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

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

(e) the means of communication which make it possible to contact the prospective data holder quickly and communicate with that data holder efficiently;

(f) how the user can request that the data are shared with a third party and, where applicable, end the data sharing;

(g) the user's right to lodge a complaint alleging an infringement of any of the provisions of this Chapter with the competent authority designated pursuant to Article 37;

(h) whether a prospective data holder is the holder of trade secrets contained in the data that is accessible from the connected product or generated during the provision of a related service, and, where the prospective data holder is not the trade secret holder, the identity of the trade secret holder;

(i) the duration of the contract between the user and the prospective data holder, as well as the arrangements for terminating such a contract.

*Article 4*

**The rights and obligations of users and data holders with regard to access, use and making available product data and related service data**

1. Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.

2. Users and data holders may contractually restrict or prohibit accessing, using or further sharing data, if such processing could undermine security requirements of the connected product, as laid down by Union or national law, resulting in a serious adverse effect on the health, safety or security of natural persons. Sectoral authorities may provide users and data holders with technical expertise in that context. Where the data holder refuses to share data pursuant to this Article, it shall notify the competent authority designated pursuant to Article 37.

3. Without prejudice to the user's right to seek redress at any stage before a court or tribunal of a Member State, the user may, in relation to any dispute with the data holder concerning the contractual restrictions or prohibitions referred to in paragraph 2:

(a) lodge, in accordance with Article 37(5), point (b), a complaint with the competent authority; or

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

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

5. For the purpose of verifying whether a natural or legal person qualifies as a user for the purposes of paragraph 1, a data holder shall not require that person to provide any information beyond what is necessary. Data holders shall not keep any information, in particular log data, on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and maintenance of the data infrastructure.

6. Trade secrets shall be preserved and shall be disclosed only where the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality in particular regarding third parties. The data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the user proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.

7. Where there is no agreement on the necessary measures referred to in paragraph 6, or if the user fails to implement the measures agreed pursuant to paragraph 6 or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the user without undue delay. In such cases, the data holder shall notify the competent authority designated pursuant to Article 37 that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined.

8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product, and shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.

9. Without prejudice to a user's right to seek redress at any stage before a court or tribunal of a Member State, a user wishing to challenge a data holder's decision to refuse or to withhold or suspend data sharing pursuant to paragraphs 7 and 8 may:

(a) lodge, in accordance with Article 37(5), point (b), a complaint with the competent authority, which shall, without undue delay, decide whether and under which conditions data sharing is to start or resume; or

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

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

11. The user shall not use coercive means or abuse gaps in the technical infrastructure of a data holder which is designed to protect the data in order to obtain access to data.

12. Where the user is not the data subject whose personal data is requested, any personal data generated by the use of a connected product or related service shall be made available by the data holder to the user only where there is a valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled.

13. A data holder shall only use any readily available data that is non-personal data on the basis of a contract with the user. A data holder shall not use such data to derive insights about the economic situation, assets and production methods of, or the use by, the user in any other manner that could undermine the commercial position of that user on the markets in which the user is active.

14. Data holders shall not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them.

*Article 5*

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

1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9.

2. Paragraph 1 shall not apply to readily available data in the context of the testing of new connected products, substances or processes that are not yet placed on the market unless their use by a third party is contractually permitted.

3. Any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925, shall not be an eligible third party under this Article and therefore shall not:

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

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

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

4. For the purpose of verifying whether a natural or legal person qualifies as a user or as a third party for the purposes of paragraph 1, the user or the third party shall not be required to provide any information beyond what is necessary. Data holders shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and maintenance of the data infrastructure.

5. The third party shall not use coercive means or abuse gaps in the technical infrastructure of a data holder which is designed to protect the data in order to obtain access to data.

6. A data holder shall not use any readily available data to derive insights about the economic situation, assets and production methods of, or the use by, the third party in any other manner that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has given permission to such use and has the technical possibility to easily withdraw that permission at any time.

7. Where the user is not the data subject whose personal data is requested, any personal data generated by the use of a connected product or related service shall be made available by the data holder to the third party only where there is a valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled.

8. 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.

9. Trade secrets shall be preserved and shall be disclosed to third parties only to the extent that such disclosure is strictly necessary to fulfil the purpose agreed between the user and the third party. The data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the third party all proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.

10. Where there is no agreement on the necessary measures referred to in paragraph 9 of this Article or if the third party fails to implement the measures agreed pursuant to paragraph 9 of this Article or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the third party without undue delay. In such cases, the data holder shall notify the competent authority designated pursuant to Article 37 that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined.

11. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, that

data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product, and shall be provided in writing to the third party without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.

12. Without prejudice to the third party's right to seek redress at any stage before a court or tribunal of a Member State, a third party wishing to challenge a data holder's decision to refuse or to withhold or suspend data sharing pursuant to paragraphs 10 and 11 may:

(a) lodge, in accordance with Article 37(5), point (b), a complaint with the competent authority, which shall, without undue delay, decide whether and under which conditions the data sharing is to start or resume; or

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

13. The right referred to in paragraph 1 shall not adversely affect the rights of data subjects pursuant to the applicable Union and national law on the protection of personal data.

*Article 6*

**Obligations of third parties receiving data at the request of the user**

1. A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user and subject to Union and national law on the protection of personal data including the rights of the data subject insofar as personal data are concerned. The third party shall erase the data when they are no longer necessary for the agreed purpose, unless otherwise agreed with the user in relation to non-personal data.

2. The third party shall not:

(a) make the exercise of choices or rights under Article 5 and this Article by the user unduly difficult, including by offering choices to the user in a non-neutral manner, or by coercing, deceiving or manipulating the user, or by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a user digital interface or a part thereof;

(b) notwithstanding Article 22(2), points (a) and (c), of Regulation (EU) 2016/679, use the data it receives for the profiling, unless it is necessary to provide the service requested by the user;

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

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

(e) use the data it receives to develop a product that competes with the connected product from which the accessed data originate or share the data with another third party for that purpose; third parties shall also not use any non-personal product data or related service data made available to them to derive insights about the economic situation, assets and production methods of, or use by, the data holder;

(f) use the data it receives in a manner that has an adverse impact on the security of the connected product or related service;

(g) disregard the specific measures agreed with a data holder or with the trade secrets holder pursuant to Article 5(9) and undermine the confidentiality of trade secrets;

(h) prevent the user that is a consumer, including on the basis of a contract, from making the data it receives available to other parties.

*Article 7*

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

1. The obligations of this Chapter shall not apply to data generated through the use of connected products manufactured or designed or related services provided by a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service.

The same shall apply to data generated through the use of connected products manufactured by or related services provided by an enterprise that has qualified as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise.

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

## CHAPTER III

## OBLIGATIONS FOR DATA HOLDERS OBLIGED TO MAKE DATA AVAILABLE PURSUANT TO UNION LAW

*Article 8*

**Conditions under which data holders make data available to data recipients**

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

2. A contractual term concerning access to and the use of data, or liability and remedies for the breach or termination of data-related obligations, shall not be binding if it constitutes an unfair contractual term within the meaning of Article 13 or if, to the detriment of the user, it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II.

3. A data holder shall not discriminate regarding the arrangements for making data available between comparable categories of data recipients, including partner enterprises or linked enterprises of the data holder when making data available. Where a data recipient considers that the conditions under which data

has been made available to it are discriminatory, the data holder shall without undue delay provide the data recipient, upon its reasoned request, with information showing that there has been no discrimination.

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

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

6. Unless otherwise provided for in Union law, including Article 4(6) and Article 5(9) of this Regulation, or by national legislation adopted in accordance with Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets.

*Article 9*

**Compensation for making data available**

1. Any compensation agreed upon between a data holder and a data recipient for making data available in business-to-business relations shall be non- discriminatory and reasonable and may include a margin.

2. When agreeing on any compensation, the data holder and the data recipient shall take into account in particular:

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

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

3. The compensation referred to in paragraph 1 may also depend on the volume, format and nature of the data.

4. Where the data recipient is an SME or a not-for-profit research organisation and where such a data recipient does not have partner enterprises or linked enterprises that do not qualify as SMEs, any compensation agreed shall not exceed the costs referred to in paragraph 2, point (a).

5. The Commission shall adopt guidelines on the calculation of reasonable compensation, taking into account the advice of the European Data Innovation Board (EDIB) referred to in Article 42.

6. This Article shall not preclude other Union law or national legislation adopted in accordance with Union law from excluding compensation for making data available or providing for lower compensation.

7. The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can assess whether the requirements of paragraphs 1 to 4 are met.

*Article 10*

**Dispute settlement**

1. Users, data holders and data recipients shall have access to a dispute settlement body, certified in accordance with paragraph 5 of this Article, to settle disputes pursuant to Article 4(3) and (9) and Article 5(12) as well as disputes relating to the fair, reasonable and non-discriminatory terms and

conditions for, and transparent manner of, making data available in accordance with this Chapter and Chapter IV.

2. 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.

3. For disputes referred to a dispute settlement body pursuant to Article 4(3) and (9) and Article 5(12), where the dispute settlement body decides a dispute in favour of the user or of the data recipient, the data holder shall bear all the fees charged by the dispute settlement body and shall reimburse that user or that data recipient for any other reasonable expenses that it has incurred in relation to the dispute settlement. If the dispute settlement body decides a dispute in favour of the data holder, the user or the data recipient shall not be required to reimburse any fees or other expenses that the data holder paid or is to pay in relation to the dispute settlement, unless the dispute settlement body finds that the user or the data recipient manifestly acted in bad faith.

4. Customers and providers of data processing services shall have access to a dispute settlement body, certified in accordance with paragraph 5 of this Article, to settle disputes relating to breaches of the rights of customers and the obligations of providers of data processing services, in accordance with Articles 23 to 31.

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

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

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

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

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

6. Member States shall notify to the Commission the dispute settlement bodies certified in accordance with paragraph 5. The Commission shall publish a list of those bodies on a dedicated website and keep it updated.

7. A dispute settlement body 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 tribunal of a Member State.

8. A dispute settlement body shall grant parties the possibility, within a reasonable period of time, to express their points of view on the matters those parties have brought before that body. In that context, each party to a dispute shall be provided with the submissions of the other party to their dispute and any statements made by experts. The parties shall be given the possibility to comment on those submissions and statements.

9. A dispute settlement body shall adopt its decision on a matter referred to it within 90 days of receipt of a request pursuant to paragraphs 1 and 4. That decision shall be in writing or on a durable medium and shall be supported by a statement of reasons.

10. Dispute settlement bodies shall draw up and make publicly available annual activity reports. Such annual reports shall include, in particular, the following general information:

(a) an aggregation of the outcomes of disputes;

(b) the average time taken to resolve disputes;

(c) the most common reasons for disputes.

11. In order to facilitate the exchange of information and best practices, a dispute settlement body may decide to include recommendations in the report referred to in paragraph 10 as to how problems can be avoided or resolved.

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

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

*Article 11*

**Technical protection measures on the unauthorised use or disclosure of data**

1. A data holder may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with Articles 4, 5, 6, 8 and 9, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation adopted in accordance with Union law. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.

2. In the circumstances referred to in paragraph 3, the third party or data recipient shall comply, without undue delay, with the requests of the data holder and, where applicable and where they are not the same person, the trade secret holder or the user:

(a) to erase the data made available by the data holder and any copies thereof;

(b) to end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where there is a serious risk that the unlawful use of those data will cause significant harm to the data holder, the trade secret holder or the user or where such a measure would not be disproportionate in light of the interests of the data holder, the trade secret holder or the user;

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

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

3. Paragraph 2 shall apply where a third party or a data recipient has:

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

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

(c) unlawfully disclosed data to another party;

(d) not maintained the technical and organisational measures agreed pursuant to Article 5(9); or

(e) altered or removed technical protection measures applied by the data holder pursuant to paragraph 1 of this Article without the agreement of the data holder.

4. Paragraph 2 shall also apply where a user alters or removes technical protection measures applied by the data holder or does not maintain the technical and organisational measures taken by the user in agreement with the data holder or, where they are not the same person, the trade secrets holder, in order to preserve trade secrets, as well as in respect of any other party that receives the data from the user by means of an infringement of this Regulation.

5. Where the data recipient infringes Article 6(2), point (a) or (b), users shall have the same rights as data holders under paragraph 2 of this Article.

*Article 12*

**Scope of obligations for data holders obliged pursuant to Union law to make data available**

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

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

## CHAPTER IV

## UNFAIR CONTRACTUAL TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES

*Article 13*

**Unfair contractual terms unilaterally imposed on another enterprise**

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

2. A contractual term which reflects mandatory provisions of Union law, or provisions of Union law which would apply if the contractual terms did not regulate the matter, shall not be considered to be unfair.

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

4. In particular, a contractual term shall be unfair for the purposes of paragraph 3, 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 contractual term.

5. A contractual term shall be presumed to be unfair for the purposes of paragraph 3 if its object or effect is to:

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

(b) allow the party that unilaterally imposed the term to access and use the data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party, in particular when such data contain commercially sensitive data or are protected by trade secrets or by intellectual property rights;

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

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

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

(f) enable the party that unilaterally imposed the term to terminate the contract at unreasonably short notice, taking into consideration any reasonable possibility 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 so doing;

(g) enable the party that unilaterally imposed the term to substantially change the price specified in the contract or any other substantive condition related to the nature, format, quality or quantity of the data to be shared, where no valid reason and no right of the other party to terminate the contract in the case of such a change is specified in the contract.

Point (g) of the first subparagraph shall not affect terms by which the party that unilaterally imposed the term reserves the right to unilaterally change the terms of a contract of an indeterminate duration, provided that the contract specified a valid reason for such unilateral changes, that the party that unilaterally imposed the term is required to provide the other contracting party with reasonable notice of any such intended change, and that the other contracting party is free to terminate the contract at no cost in the case of a change.

6. 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 the contractual term bears the burden of proving that that term has not been unilaterally imposed. The contracting party that supplied the contested contractual term may not argue that the term is an unfair contractual term.

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

8. This Article does not apply to contractual terms defining the main subject matter of the contract or to the adequacy of the price, as against the data supplied in exchange.

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

## CHAPTER V

## MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF AN EXCEPTIONAL NEED

*Article 14*

### Obligation to make data available on the basis of an exceptional need

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

*Article 15*

### Exceptional need to use data

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

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

(b) in circumstances not covered by point (a) and only insofar as non-personal data is concerned, where:

  (i) a public sector body, the Commission, the European Central Bank or a Union body is acting on the basis of Union or national law and has identified specific data, the lack of which prevents it from fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency; and

  (ii) the public sector body, the Commission, the European Central Bank or the Union body has exhausted all other means at its disposal to obtain such data, including purchase of non-personal data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data.

2. Paragraph 1, point (b), shall not apply to microenterprises and small enterprises.

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

*Article 16*

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

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

2. This Chapter shall not apply to public sector bodies, the Commission, the European Central Bank or Union bodies carrying out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or to customs or taxation administration. This Chapter does not affect applicable Union and national law on the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, or for customs or taxation administration.

*Article 17*

**Requests for data to be made available**

1. When requesting data pursuant to Article 14, a public sector body, the Commission, the European Central Bank or a Union body shall:

(a) specify the data required, including the relevant metadata necessary to interpret and use those data;

(b) demonstrate that the conditions necessary for the existence of an exceptional need as referred to in Article 15 for the purpose of which the data are requested are met;

(c) explain the purpose of the request, the intended use of the data requested, including, where applicable, by a third party in accordance with paragraph 4 of this Article, the duration of that use, and, where relevant, how the processing of personal data is to address the exceptional need;

(d) specify, if possible, when the data are expected to be erased by all parties that have access to them;

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

(f) specify any other public sector bodies or the Commission, European Central Bank or Union bodies and the third parties with which the data requested is expected to be shared with;

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

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

(i) specify the deadline by which the data are to be made available and the deadline referred to in Article 18(2) by which the data holder may decline or seek modification of the request;

(j) make its best efforts to avoid compliance with the data request resulting in the data holders' liability for infringement of Union or national law.

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

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

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

(c) be proportionate to the exceptional need and duly justified, regarding the granularity and volume of the data requested and frequency of access of the data requested;

(d) respect the legitimate aims of the data holder, committing to ensuring the protection of trade secrets in accordance with Article 19(3), and the cost and effort required to make the data available;

(e) concern non-personal data, and only if this is demonstrated to be insufficient to respond to the exceptional need to use data, in accordance with Article 15(1), point (a), request personal data in pseudonymised form and establish the technical and organisational measures that are to be taken to protect the data;

(f) inform the data holder of the penalties that are to be imposed pursuant to Article 40 by the competent authority designated pursuant to Article 37 in the event of non-compliance with the request;

(g) where the request is made by a public sector body, be transmitted to the data coordinator referred to in Article 37 of the Member State where the requesting public sector body is established, who shall make the request publicly available online without undue delay unless the data coordinator considers that such publication would create a risk for public security;

(h) where the request is made by the Commission, the European Central Bank or a Union body, be made available online without undue delay;

(i) where personal data are requested, be notified without undue delay to the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 in the Member State where the public sector body is established.

The European Central Bank and Union bodies shall inform the Commission of their requests.

3. A public sector body, the Commission, the European Central Bank or a Union body shall not make data obtained pursuant to this Chapter available for reuse as defined in Article 2, point (2), of Regulation (EU) 2022/868 or Article 2, point (11), of Directive (EU) 2019/1024. Regulation (EU) 2022/868 and Directive (EU) 2019/1024 shall not apply to the data held by public sector bodies obtained pursuant to this Chapter.

4. Paragraph 3 of this Article does not preclude a public sector body, the Commission, the European Central Bank or a Union body to exchange data obtained pursuant to this Chapter with another public sector body or the Commission, the European Central Bank or a Union body in view of completing the tasks referred to in Article 15, as specified in the request in accordance with paragraph 1, point (f), of this Article or to make the data available to a third party where it has delegated, by means of a publicly available agreement, technical inspections or other functions to that third party. The obligations on public

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

5. Where the data holder considers that its rights under this Chapter have been infringed by the transmission or making available of data, it may lodge a complaint with the competent authority designated pursuant to Article 37 of the Member State where the data holder is established.

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

*Article 18*

**Compliance with requests for data**

1. A data holder receiving a request to make data available under this Chapter shall make the data available to the requesting public sector body, the Commission, the European Central Bank or a Union body without undue delay, taking into account necessary technical, organisational and legal measures.

2. Without prejudice to specific needs regarding the availability of data defined in Union or national law, a data holder may decline or seek the modification of a request to make data available under this Chapter without undue delay and, in any event, no later than five working days after the receipt of a request for the data necessary to respond to a public emergency and without undue delay and, in any event, no later than 30 working days after the receipt of such a request in other cases of an exceptional need, on any of the following grounds:

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

(b) a similar request for the same purpose has been previously submitted by another public sector body or the Commission, the European Central Bank or a Union body and the data holder has not been notified of the erasure of the data pursuant to Article 19(1), point (c);

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

3. If the data holder decides to decline the request or to seek its modification in accordance with paragraph 2, point (b), it shall indicate the identity of the public sector body or the Commission, the European Central Bank or the Union body that previously submitted a request for the same purpose.

4. Where the data requested includes personal data, the data holder shall properly anonymise the data, unless the compliance with the request to make data available to a public sector body, the Commission, the European Central Bank or a Union body requires the disclosure of personal data. In such cases, the data holder shall pseudonymise the data.

5. Where the public sector body, the Commission, the European Central Bank or the Union body wishes to challenge a data holder’s refusal to provide the data requested, or where the data holder wishes to challenge the request and the matter cannot be resolved by an appropriate modification of the request, the matter shall be referred to the competent authority designated pursuant to Article 37 of the Member State where the data holder is established.

*Article 19*

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

1. A public sector body, the Commission, the European Central Bank or a Union body receiving data pursuant to a request made under Article 14 shall:

(a) not use the data in a manner incompatible with the purpose for which they were requested;

(b) have implemented technical and organisational measures that preserve the confidentiality and integrity of the requested data and the security of the data transfers, in particular personal data, and safeguard the rights and freedoms of data subjects;

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

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

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

(b) share the data with another third party for any of the purposes referred to in point (a).

3. Disclosure of trade secrets to a public sector body, the Commission, the European Central Bank or a Union body shall be required only to the extent that it is strictly necessary to achieve the purpose of a request under Article 15. In such a case, the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata. The public sector body, the Commission, the European Central Bank or the Union body shall, prior to the disclosure of trade secrets, take all necessary and appropriate technical and organisational measures to preserve the confidentiality of the trade secrets, including, as appropriate, the use of model contractual terms, technical standards and the application of codes of conduct.

4. A public sector body, the Commission, the European Central Bank or a Union body shall be responsible for the security of the data it receives.

*Article 20*

**Compensation in cases of an exceptional need**

1. Data holders other than microenterprises and small enterprises shall make available data necessary to respond to a public emergency pursuant to Article 15(1), point (a), free of charge. The public sector body, the Commission, the European Central Bank or the Union body that has received data shall provide public acknowledgement to the data holder if requested by the data holder.

2. The data holder shall be entitled to fair compensation for making data available in compliance with a request made pursuant to Article 15(1), point (b). Such compensation shall cover the technical and organisational costs incurred to comply with the request including, where applicable, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, and a reasonable margin. Upon request of the public sector body, the Commission, the European Central Bank or the Union body, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.

3. Paragraph 2 shall also apply where a microenterprise and small enterprise claims compensation for making data available.

4. Data holders shall not be entitled to compensation for making data available in compliance with a request made pursuant to Article 15(1), point (b), where the specific task carried out in the public interest is the production of official statistics and where the purchase of data is not allowed by national law. Member States shall notify the Commission where the purchase of data for the production of official statistics is not allowed by national law.

5. Where the public sector body, the Commission, the European Central Bank or the Union body disagrees with the level of compensation requested by the data holder, they may lodge a complaint with the competent authority designated pursuant to Article 37 of the Member State where the data holder is established.

*Article 21*

**Sharing of data obtained in the context of an exceptional need with research organisations or statistical bodies**

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

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

(b) with national statistical institutes and Eurostat for the production of official statistics.

2. Individuals or organisations receiving the data pursuant to paragraph 1 shall act on a not-for-profit basis or in the context of a public-interest mission recognised in Union or national law. They shall not include organisations upon which commercial undertakings have a significant influence which is likely to result in preferential access to the results of the research.

3. Individuals or organisations receiving the data pursuant to paragraph 1 of this Article shall comply with the same obligations that are applicable to the public sector bodies, the Commission, the European Central Bank or Union bodies pursuant to Article 17(3) and Article 19.

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

5. Where a public sector body, the Commission, the European Central Bank or a Union body intends to transmit or make data available under paragraph 1 of this Article, it shall notify without undue delay the data holder from whom the data was received, stating the identity and contact details of the organisation or the individual receiving the data, the purpose of the transmission or making available of the data, the period for which the data is to be used and the technical protection and organisational measures taken, including where personal data or trade secrets are involved. Where the data holder disagrees with the transmission or making available of data, it may lodge a complaint with the competent authority designated pursuant to Article 37 of the Member State where the data holder is established.

*Article 22*

**Mutual assistance and cross-border cooperation**

1. Public sector bodies, the Commission, the European Central Bank and Union bodies shall cooperate and assist one another, to implement this Chapter in a consistent manner.

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

3. Where a public sector body intends to request data from a data holder established in another Member State, it shall first notify the competent authority designated pursuant to Article 37 in that Member State of that intention. This requirement shall also apply to requests by the Commission, the European Central Bank and Union bodies. The request shall be examined by the competent authority of the Member State where the data holder is established.

4. After having examined the request in light of the requirements laid down in Article 17, the relevant competent authority shall, without undue delay, take one of the following actions:

(a) transmit the request to the data holder and, if applicable, advise the requesting public sector body, the Commission, the European Central Bank or the Union body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established with the aim of reducing the administrative burden on the data holder in complying with the request;

(b) reject the request on duly substantiated grounds in accordance with this Chapter.

The requesting public sector body, the Commission, the European Central Bank and the Union body shall take into account the advice of and the grounds provided by the relevant competent authority pursuant to the first subparagraph before taking any further action such as resubmitting the request, if applicable.

## CHAPTER VI

## SWITCHING BETWEEN DATA PROCESSING SERVICES

*Article 23*

### Removing obstacles to effective switching

Providers of data processing services shall take the measures provided for in Articles 25, 26, 27, 29 and 30 to enable customers to switch to a data processing service, covering the same service type, which is provided by a different provider of data processing services, or to on-premises ICT infrastructure, or, where relevant, to use several providers of data processing services at the same time. In particular, providers of data processing services shall not impose and shall remove pre-commercial, commercial, technical, contractual and organisational obstacles, which inhibit customers from:

(a) terminating, after the maximum notice period and the successful completion of the switching process, in accordance with Article 25, the contract of the data processing service;

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

(c) porting the customer’s exportable data and digital assets, to a different provider of data processing services or to an on-premises ICT infrastructure, including after having benefited from a free-tier offering;

(d) in accordance with Article 24, achieving functional equivalence in the use of the new data processing service in the ICT environment of a different provider of data processing services covering the same service type;

(e) unbundling, where technically feasible, data processing services referred to in Article 30(1) from other data processing services provided by the provider of data processing services.

*Article 24*

**Scope of the technical obligations**

The responsibilities of providers of data processing services laid down in Articles 23, 25, 29, 30 and 34 shall apply only to the services, contracts or commercial practices provided by the source provider of data processing services.

*Article 25*

**Contractual terms concerning switching**

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

2. Without prejudice to Directive (EU) 2019/770, the contract referred to in paragraph 1 of this Article shall include at least the following:

(a) clauses allowing the customer, upon request, to switch to a data processing service offered by a different provider of data processing services or to port all exportable data and digital assets to an on-premises ICT infrastructure, without undue delay and in any event not after the mandatory maximum transitional period of 30 calendar days, to be initiated after the maximum notice period referred to in point (d), during which the service contract remains applicable and during which the provider of data processing services shall:

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

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

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

  (iv) ensure that a high level of security is maintained throughout the switching process, in particular the security of the data during their transfer and the continued security of the data during the retrieval period specified in point (g), in accordance with applicable Union or national law;

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

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

  (i) where applicable, upon the successful completion of the switching process;

  (ii) at the end of the maximum notice period referred to in paragraph (d), where the customer does not wish to switch but to erase its exportable data and digital assets upon service termination;

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

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

(f) an exhaustive specification of categories of data specific to the internal functioning of the provider's data processing service that are to be exempted from the exportable data under point (e) of this paragraph where a risk of breach of trade secrets of the provider exists, provided that such exemptions do not impede or delay the switching process provided for in Article 23;

(g) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transitional period that was agreed between the customer and the provider of data processing services, in accordance with point (a) of this paragraph and paragraph 4;

(h) a clause guaranteeing full erasure of all exportable data and digital assets generated directly by the customer, or relating to the customer directly, after the expiry of the retrieval period referred to in point (g) or after the expiry of an alternative agreed period at a date later than the date of expiry of the retrieval period referred to in point (g), provided that the switching process has been completed successfully;

(i) switching charges, that may be imposed by providers of data processing services in accordance with Article 29.

3. The contract referred to in paragraph 1 shall include clauses providing that the customer may notify the provider of data processing services of its decision to perform one or more of the following actions upon termination of the maximum notice period referred to in paragraph 2, point (d):

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

(b) switch to an on-premises ICT infrastructure;

(c) erase its exportable data and digital assets.

4. Where the mandatory maximum transitional period as provided for in paragraph 2, point (a) is technically unfeasible, the provider of data processing services shall notify the customer within 14 working days of the making of the switching request, and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which shall not exceed seven months. In accordance with paragraph 1, service continuity shall be ensured throughout the alternative transitional period.

5. Without prejudice to paragraph 4, the contract referred to in paragraph 1 shall include clauses providing the customer with the right to extend the transitional period once for a period that the customer considers more appropriate for its own purposes.

*Article 26*

**Information obligation of providers of data processing services**

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

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

(b) a reference to an up-to-date online register hosted by the provider of data processing services, with details of all the data structures and data formats as well as the relevant standards and open interoperability specifications, in which the exportable data referred to in Article 25(2), point (e), are available.

*Article 27*

**Obligation of good faith**

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

*Article 28*

**Contractual transparency obligations on international access and transfer**

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

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

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

2. The websites referred to in paragraph 1 shall be listed in contracts for all data processing services offered by providers of data processing services.

*Article 29*

**Gradual withdrawal of switching charges**

1. From 12 January 2027, providers of data processing services shall not impose any switching charges on the customer for the switching process.

2. From 11 January 2024 to 12 January 2027, providers of data processing services may impose reduced switching charges on the customer for the switching process.

3. The reduced switching charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned.

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

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

6. Where applicable, providers of data processing services shall make the information referred to in paragraphs 4 and 5 publicly available to customers via a dedicated section of their website or in any other easily accessible way.

7. The Commission is empowered to adopt delegated acts in accordance with Article 45 to supplement this Regulation by establishing 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, pursuant to paragraphs 1 and 2 of this Article are to be attained in accordance with the deadlines laid down in those paragraphs.

*Article 30*

**Technical aspects of switching**

1. Providers of data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall, in accordance with Article 27, take all reasonable measures in their power to facilitate that the customer, after switching to a service covering the same service type, achieves functional equivalence in the use of the destination data processing service. The source provider of data processing services shall facilitate the switching process by providing capabilities, adequate information, documentation, technical support and, where appropriate, the necessary tools.

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

3. For data processing services other than those referred to in paragraph 1 of this Article, providers of data processing services shall ensure compatibility with common specifications based on open interoperability specifications or harmonised standards for interoperability at least 12 months after the references to those common specifications or harmonised standards for interoperability of data processing services were published in the central Union standards repository for the interoperability of data processing services following the publication of the underlying implementing acts in the *Official Journal of the European Union* in accordance with Article 35(8).

4. Providers of data processing services other than those referred to in paragraph 1 of this Article shall update the online register referred to in Article 26, point (b) in accordance with their obligations under paragraph 3 of this Article.

5. In the case of switching between services of the same service type, for which common specifications or the harmonised standards for interoperability referred to in paragraph 3 of this Article have not been published in the central Union standards repository for the interoperability of data processing services in accordance with Article 35(8), the provider of data processing services shall, at the request of the customer, export all exportable data in a structured, commonly used and machine-readable format.

6. Providers of data processing services shall not be required to develop new technologies or services, or disclose or transfer digital assets that are protected by intellectual property rights or that constitute a trade

secret, to a customer or to a different provider of data processing services or compromise the customer's or provider's security and integrity of service.

*Article 31*

**Specific regime for certain data processing services**

1. The obligations laid down in Article 23, point (d), Article 29 and Article 30(1) and (3) shall not apply to data processing services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where those data processing services are not offered at broad commercial scale via the service catalogue of the provider of data processing services.

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

3. Prior to the conclusion of a contract on the provision of the data processing services referred to in this Article, the provider of data processing services shall inform the prospective customer of the obligations of this Chapter that do not apply.

## CHAPTER VII

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

*Article 32*

**International governmental access and transfer**

1. Providers of data processing services shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State, without prejudice to paragraph 2 or 3.

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

3. In the absence of an international agreement as referred to in paragraph 2, where a provider of data processing services is the addressee of a decision or judgment of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data falling within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where:

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

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

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

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

The EDIB referred to in Article 42 shall advise and assist the Commission in developing guidelines on the assessment of whether the conditions laid down in the first subparagraph of this paragraph are met.

4. If the conditions laid down in paragraph 2 or 3 are met, the provider of data processing services shall provide the minimum amount of data permissible in response to a request, on the basis of the reasonable interpretation of that request by the provider or relevant national body or authority referred to in paragraph 3, second subparagraph.

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

## CHAPTER VIII
## INTEROPERABILITY

*Article 33*

### Essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces

1. Participants in data spaces that offer data or data services to other participants shall comply with the following essential requirements to facilitate the interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces which are purpose- or sector-specific or cross-sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives:

(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in 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, where available, shall be described in a publicly available and consistent manner;

(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine-readable format where that is technically feasible and does not hamper the good functioning of the connected product;

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

The requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements arising from other Union or national law.

2. The Commission is empowered to adopt delegated acts, in accordance with Article 45 of this Regulation to supplement this Regulation by further specifying the essential requirements laid down in paragraph 1 of this Article, in relation to those requirements that, by their nature, cannot produce the intended effect unless they are further specified in binding Union legal acts and in order to properly reflect technological and market developments.

The Commission shall when adopting delegated acts take into account the advice of the EDIB in accordance with Article 42, point (c)(iii).

3. The participants in data spaces that offer data or data services to other participants in data spaces which meet the harmonised standards or parts thereof, the references of which are published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards or parts thereof.

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

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

(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard that satisfies the essential requirements laid down in paragraph 1 of this Article and:

  (i) the request has not been accepted;

  (ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or

  (iii) the harmonised standards do not comply with the request; and

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

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

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

7. When preparing the draft implementing act referred to in paragraph 5, the Commission shall take into account the advice of the EDIB and views of other relevant bodies or expert groups and shall duly consult all relevant stakeholders.

8. The participants in data spaces that offer data or data services to other participants in data spaces that meet the common specifications established by implementing acts referred to in paragraph 5 or parts thereof shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such common specifications or parts thereof.

9. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the *Official Journal of the European Union*, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. Where the reference of a harmonised standard is published in the *Official Journal of the European Union*, the Commission shall repeal the implementing acts referred to in paragraph 5 of this Article, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.

10. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraph 1, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.

11. The Commission may adopt guidelines taking into account the proposal of the EDIB in accordance with Article 30, point (h), of Regulation (EU) 2022/868 laying down interoperable frameworks for common standards and practices for the functioning of common European data spaces.

*Article 34*

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

1. The requirements laid down in Article 23, Article 24, Article 25(2), points (a)(ii), (a)(iv), (e) and (f) and Article 30(2) to (5) shall also apply *mutatis mutandis* to providers of data processing services to facilitate interoperability for the purposes of in-parallel use of data processing services.

2. Where a data processing service is being used in parallel with another data processing service, the providers of data processing services may impose data egress charges, but only for the purpose of passing on egress costs incurred, without exceeding such costs.

*Article 35*

**Interoperability of data processing services**

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

(a) achieve, where technically feasible, interoperability between different data processing services that cover the same service type;

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

(c) facilitate, where technically feasible, functional equivalence between different data processing services referred to in Article 30(1) that cover the same service type;

(d) not have an adverse impact on the security and integrity of data processing services and data;

(e) be designed in such a way so as to allow for technical advances and the inclusion of new functions and innovation in data processing services.

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

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

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

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

3. Open interoperability specifications shall comply with Annex II to Regulation (EU) No 1025/2012.

4. After taking into account relevant international and European standards and self-regulatory initiatives, the Commission may, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraphs 1 and 2 of this Article.

5. The Commission may, by means of implementing acts, adopt common specifications based on open interoperability specifications covering all of the essential requirements laid down in paragraphs 1 and 2.

6. When preparing the draft implementing act referred to in paragraph 5 of this Article, the Commission shall take into account the views of the relevant competent authorities referred to in Article 37(5), point (h) and other relevant bodies or expert groups and shall duly consult all relevant stakeholders.

7. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraphs 1 and 2, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.

8. For the purpose of Article 30(3), the Commission shall, by means of implementing acts, publish the references of harmonised standards and common specifications for the interoperability of data processing services in a central Union standards repository for the interoperability of data processing services.

9. The implementing acts referred to in this Article shall be adopted in accordance with the examination procedure referred to in Article 46(2).

*Article 36*

**Essential requirements regarding smart contracts for executing data sharing agreements**

1. The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an

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

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

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

(c) data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);

(d) access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers; and

(e) consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.

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

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

4. A smart contract that meets the harmonised standards or the relevant parts thereof, the references of which are published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards or parts thereof.

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

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

(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard that satisfies the essential requirements laid down in paragraph 1 of this Article and:

  (i) the request has not been accepted;

  (ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or

(iii) the harmonised standards do not comply with the request; and

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

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

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

8. When preparing the draft implementing act referred to in paragraph 6, the Commission shall take into account the advice of the EDIB and views of other relevant bodies or expert groups and shall duly consult all relevant stakeholders.

9. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available that meet the common specifications established by implementing acts referred to in paragraph 6 or parts thereof shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such common specifications or parts thereof.

10. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the *Official Journal of the European Union*, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. Where the reference of a harmonised standard is published in the *Official Journal of the European Union*, the Commission shall repeal the implementing acts referred to in paragraph 6 of this Article, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.

11. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraph 1, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.

## CHAPTER IX

## IMPLEMENTATION AND ENFORCEMENT

*Article 37*

### Competent authorities and data coordinators

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

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

Competent authorities shall, in the exercise of the tasks and powers assigned to them under paragraph 5, cooperate with each other.

3. The supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned. Chapters VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*.

The European Data Protection Supervisor shall be responsible for monitoring the application of this Regulation insofar as it concerns the Commission, the European Central Bank or Union bodies. Where relevant, Article 62 of Regulation (EU) 2018/1725 shall apply *mutatis mutandis*.

The tasks and powers of the supervisory authorities referred to in this paragraph shall be exercised with regard to the processing of personal data.

4. Without prejudice to paragraph 1 of this Article:

(a) for specific sectoral data access and use issues related to the application of this Regulation, the competence of sectoral authorities shall be respected;

(b) the competent authority responsible for the application and enforcement of Articles 23 to 31 and Articles 34 and 35 shall have experience in the field of data and electronic communications services.

5. Member States shall ensure that the tasks and powers of the competent authorities are clearly defined and include:

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

(b) handling complaints arising from alleged infringements of this Regulation, including in relation to trade secrets, and investigating, to the extent appropriate, the subject matter of complaints and regularly informing complainants, where relevant in accordance with national law, of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another competent authority is necessary;

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

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

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

(f) cooperating with competent authorities of other Member States and, where relevant, with the Commission or the EDIB, to ensure the consistent and efficient application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay, including regarding paragraph 10 of this Article;

(g) cooperating with the relevant competent authorities responsible for the implementation of other Union or national legal acts, including with authorities competent in the field of data and electronic communication services, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 or with sectoral authorities to ensure that this Regulation is enforced consistently with other Union and national law;

(h) cooperating with the relevant competent authorities to ensure that Articles 23 to 31 and Articles 34 and 35 are enforced consistently with other Union law and self-regulation applicable to providers of data processing services;

(i) ensuring that switching charges are withdrawn in accordance with Article 29;

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

Where designated, the data coordinator shall facilitate the cooperation referred to in points (f), (g) and (h) of the first subparagraph and shall assist the competent authorities upon their request.

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

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

(b) ensure the online public availability of requests to make data available made by public sector bodies in the case of exceptional need under Chapter V and promote voluntary data sharing agreements between public sector bodies and data holders;

(c) inform the Commission, on an annual basis, of the refusals notified under Article 4(2) and (8) and Article 5(11).

7. Member States shall notify the Commission of the names of the competent authorities and of their tasks and powers and, where applicable, the name of the data coordinator. The Commission shall maintain a public register of those authorities.

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

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

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

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

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

13. An entity falling within the scope of this Regulation that makes connected products available or offers services in the Union, shall be considered to be under the competence of the Member State in which its legal representative is located. The designation of a legal representative by such an entity shall be without prejudice to the liability of, and any legal action that could be initiated against, such an entity. Until such time as an entity designates a legal representative in accordance with this Article, it shall be under the competence of all Member States, where applicable, for the purposes of ensuring the application and enforcement of this Regulation. Any competent authority may exercise its competence, including by imposing effective, proportionate and dissuasive penalties, provided that the entity is not subject to enforcement proceedings under this Regulation regarding the same facts by another competent authority.

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

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

16. Competent authorities shall respect the principles of confidentiality and of professional and commercial secrecy and shall protect personal data in accordance with Union or national law. Any information exchanged in the context of a request for assistance and provided pursuant to this Article shall be used only in respect of the matter for which it was requested.

*Article 38*

**Right to lodge a complaint**

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed. The data coordinator shall, upon request, provide all the necessary information to natural and legal persons for the lodging of their complaints with the appropriate competent authority.

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

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

*Article 39*

**Right to an effective judicial remedy**

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

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

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

*Article 40*

**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.

2. Member States shall by 12 September 2025 notify the Commission of those rules and measures and shall notify it without delay of any subsequent amendment affecting them. The Commission shall regularly update and maintain an easily accessible public register of those measures.

3. Member States shall take into account the recommendations of the EDIB and the following non-exhaustive criteria for the imposition of penalties for infringements of this Regulation:

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

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

(c) any previous infringements by the infringing party;

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

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

(f) infringing party’s annual turnover in the preceding financial year in the Union.

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

5. For infringements of the obligations laid down in Chapter V of this Regulation, the European Data Protection Supervisor 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 41*

**Model contractual terms and standard contractual clauses**

The Commission, before 12 September 2025, shall develop and recommend non-binding model contractual terms on data access and use, including terms on reasonable compensation and the protection of trade secrets, and non-binding standard contractual clauses for cloud computing contracts to assist parties in drafting and negotiating contracts with fair, reasonable and non-discriminatory contractual rights and obligations.

*Article 42*

**Role of the EDIB**

The EDIB established by the Commission as an expert group pursuant to Article 29 of Regulation (EU) 2022/868, in which competent authorities shall be represented, shall support the consistent application of this Regulation by:

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

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

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

(i) whether to request the drafting of harmonised standards referred to in Article 33(4), Article 35(4) and Article 36(5);

(ii) the preparation of the implementing acts referred to in Article 33(5), Article 35(5) and (8) and Article 36(6);

(iii) the preparation of the delegated acts referred to in Article 29(7) and Article 33(2); and

(iv) the adoption of the guidelines laying down interoperable frameworks for common standards and practices for the functioning of common European data spaces referred to in Article 33(11).

## CHAPTER X

## *SUI GENERIS* RIGHT UNDER DIRECTIVE 96/9/EC

*Article 43*

**Databases containing certain data**

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

## CHAPTER XI

## FINAL PROVISIONS

*Article 44*

**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 11 January 2024, and delegated or implementing acts pursuant thereto, shall remain unaffected.

2. This Regulation is without prejudice to Union law 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.

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

*Article 45*

**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 Article 29(7) and Article 33(2) shall be conferred on the Commission for an indeterminate period of time from 11 January 2024.

3. The delegation of power referred to in Article 29(7) and Article 33(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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 Article 29(7) or Article 33(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

*Article 46*

**Committee procedure**

1. The Commission shall be assisted by the Committee established by Regulation (EU) 2022/868. 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 47*

**Amendment to Regulation (EU) 2017/2394**

In the Annex to Regulation (EU) 2017/2394 the following point is added:

‘29. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).’

*Article 48*

**Amendment to Directive (EU) 2020/1828**

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

‘68. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj). ’

*Article 49*

**Evaluation and review**

1. By 12 September 2028, 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, and to the European Economic and Social Committee. That evaluation shall assess, in particular:

(a) situations to be considered to be situations of exceptional need for the purpose of Article 15 of this Regulation and the application of Chapter V of this Regulation in practice, in particular the experience in the application of Chapter V of this Regulation by public sector bodies, the Commission, the European Central Bank and Union bodies; the number and outcome of the proceedings brought to the competent authority under Article 18(5) on the application of Chapter V of this Regulation, as reported by the competent authorities; the impact of other obligations laid down in Union or national law for the purposes of complying with requests for access to information; the impact of voluntary data-sharing mechanisms, such as those put in place by data altruism organisations recognised under Regulation (EU) 2022/868, on meeting the objectives of Chapter V of this Regulation, and the role of personal data in the context of Article 15 of this Regulation, including the evolution of privacy-enhancing technologies;

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

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

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

(e) the absence of any impact on intellectual property rights;

(f) the impact on trade secrets, including on the protection against their unlawful acquisition, use and disclosure, as well as the impact of the mechanism allowing the data holder to refuse the user’s request under Article 4(8) and Article 5(11), taking into account, to the extent possible, any revision of Directive (EU) 2016/943;

(g) whether the list of unfair contractual terms referred to in Article 13 is up-to-date in light of new business practices and the rapid pace of market innovation;

(h) changes in the contractual practices of providers of data processing services and whether this results in sufficient compliance with Article 25;

(i) the diminution of charges imposed by providers of data processing services for the switching process, in line with the gradual withdrawal of switching charges pursuant to Article 29;

(j) the interplay of this Regulation with other Union legal acts of relevance to the data economy;

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

(l) the efficacy of the enforcement regime required under Article 37;

(m) the impact of this Regulation on SMEs with regard to their capacity to innovate and to the availability of data processing services for users in the Union and the burden of complying with new obligations.

2. By 12 September 2028, 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, and to the European Economic and Social Committee. That evaluation shall assess the impact of Articles 23 to 31 and Articles 34 and 35, in particular regarding pricing and the diversity of data processing services offered within the Union, with a special focus on SME providers.

3. Member States shall provide the Commission with the information necessary for the preparation of the reports referred to in paragraphs 1 and 2.

4. On the basis of the reports referred to in paragraphs 1 and 2, the Commission may, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.

*Article 50*

**Entry into force and application**

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 12 September 2025.

The obligation resulting from Article 3(1) shall apply to connected products and the services related to them placed on the market after 12 September 2026.

Chapter III shall apply in relation to obligations to make data available under Union law or national legislation adopted in accordance with Union law, which enters into force after 12 September 2025.

Chapter IV shall apply to contracts concluded after 12 September 2025.

Chapter IV shall apply from 12 September 2027 to contracts concluded on or before 12 September 2025 provided that they are:

(a) of indefinite duration; or

(b) due to expire at least 10 years from 11 January 2024.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 13 December 2023.

*For the European Parliament*

*The President*

R. METSOLA

*For the Council*

*The President*

P. NAVARRO RÍOS

(1) OJ C 402, 19.10.2022, p. 5.

(2) OJ C 365, 23.9.2022, p. 18.

(3) OJ C 375, 30.9.2022, p. 112.

(4) Position of the European Parliament of 9 November 2023 (not yet published in the Official Journal) and decision of the Council of 27 November 2023.

(5) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(6) 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).

(7) 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).

(8) 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).

(9) Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

(10) 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).

(11) 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 (OJ L 304, 22.11.2011, p. 64).

(12) 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).

(13) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

(14) Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118).

(15) Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181).

(16) Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (OJ L 141, 5.6.2015, p. 1).

(17) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

([18]) 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).

([19]) 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).

([20]) 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).

([21]) 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).

([22]) 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).

([23]) 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).

([24]) Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers (OJ L 80, 18.3.1998, p. 27).

([25]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) (OJ L 178, 17.7.2000, p. 1).

([26]) 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).

([27]) 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).

([28]) 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).

([29]) 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).

([30]) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59).

([31]) 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).

([32]) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

([33]) 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).

([34]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

([35]) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

([36]) 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).

([37]) 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).

([38]) OJ L 123, 12.5.2016, p. 1.

([39]) 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).

ELI: http://data.europa.eu/eli/reg/2023/2854/oj

ISSN 1977-0677 (electronic edition)