Changes made in the Data Act proposed by European Commission in the draft Digital Omnibus published on November 19, 2025

Added: green; replaced: blue; deleted: red (Last update: December 01, 2025)

“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)

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

(ea) voluntary registration of data intermediation services;

(eb) voluntary registration of entities which collect and process data made available for altruistic purposes;

(ec) the establishment of a European Data Innovation Board;

(ed) data localisation requirements and the availability of data to competent authorities;

(ee) the re-use of certain data and documents held by public sector bodies or by certain public undertakings, and of research data.’

(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.

(g) Chapter VIIa applies to personal and non-personal data;

(h) Chapter VIIb applies to any non-personal data;

(i) Chapter VIIc applies to personal and non-personal data, namely the following:

(i) documents held by public sector bodies of Member States as referred

(1) to in Article 32i(1), point (a) or by public undertakings as referred

(2) to in Article 32i(1), point (b);

(ii) research data as referred to in Article 32i(1), point (c);

(iii) certain categories of protected data as referred to in Article 32i(1), point (a).

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.~~

(g) participants in data spaces.

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.

11. Chapter VIIb of this Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as to laws, regulations, and administrative provisions of Member States that provide for the implementation of such powers and responsibilities.

12. Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements that relate to Chapters VIIa and VIIb, including through an authorisation or certification regime, those provisions of that sectorspecific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.

13. With regards to data and documents in scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation does not affect the possibility for Member States to adopt more detailed or stricter rules, provided that those rules allow for more extensive re-use of data and documents.

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;

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

(4b) ‘permission’ means giving data users the right to the processing of non-personal data;

(4c) ‘access’ means data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of 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;~~

(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 or 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;

(28a) ‘bodies governed by public law’ means bodies that have all of the following characteristics:

(a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;

(b) they have legal personality;

(c) they are financed, for the most part by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law;

(28b) ‘public undertaking’ means any undertaking over which a public sector body may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly:

(a) hold the majority of the undertaking's subscribed capital;

(b) control the majority of the votes attaching to shares issued by the undertaking;

(c) can appoint more than half of the undertaking's administrative, management or supervisory body;

(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;

(38a) ‘data intermediation service’ means a service which aims to establish relationships of an economic character for the purposes of data sharing between an undetermined number of data subjects or data holders and data users, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, and which :

(1) do not have as their main purpose the intermediation of copyrightprotected content;

(2) are not jointly procured by several legal persons for exclusive use among them;

(38b) 'data altruism' means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or of permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest;

(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.

(44) 'medium-sized enterprise' means a medium-sized enterprise as defined inArticle 2 of Annex I to Recommendation 2003/361/EC;

(45) 'small mid-cap' or 'SMC' means a small mid-cap enterprise as defined inArticle 2 of the Annex to Commission Recommendation (EU) 2025/1099;

(46) 'university' means a public sector body that provides post-secondary-school higher education leading to academic degrees;

(47) 'standard licence' means a set of predefined re-use conditions in a digital format, preferably compatible with standardised public licences available online;

(48) 'document' means:

(a) any content that is non-digital whatever its medium (paper or as a sound, visual or audiovisual recording); or

(b) any part of such content;

(50) ‘dynamic data’ means data and documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data;

(51) ‘research data’ means data , other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results;

(52) ‘re-use’ means the use by natural persons or legal entities of documents held by:

(a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced, except for the exchange of documents between public sector bodies purely in pursuit of their public tasks; or

(b) public undertakings, under Chapter VIIc Section 2 for commercial or non-commercial purposes other than for the initial purpose of providing services in the general interest for which the documents were produced, except for the exchange of documents between public undertakings and public sector bodies purely in pursuit of the public tasks of public sector bodies;

(53) ‘high-value datasets’ means data and documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of valueadded services, applications and new, high-quality and decent jobs, and because of the number of potential beneficiaries of the value-added services and applications based on those data and documents;

(54) ‘certain categories of protected data’ means data and documents held by public sector bodies which are protected on the grounds of

(a) commercial confidentiality, including business, professional and company secrets;

(b) statistical confidentiality;

(c) the protection of intellectual property rights of third parties; or

(d) the protection of personal data, insofar as such data fall outside the scope of Section 2 of Chapter VIIc;

(56) ‘secure processing environment’ means the physical or virtual environment and organisational means to ensure compliance with Union law in particular with regard to data subjects’ rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with

applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms;

(57) 're-user' means a natural or legal person who was granted the right to reuse data or documents held by a public sector body or a public undertaking under Chapter VIIc or to research data or certain categories of protected data;

(58) 'machine-readable format' means a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure;

(59) 'open format' means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents;

(60) 'formal open standard' means a standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability;

(61) 'reasonable return on investment' means a percentage of the overall charge, in addition to the amount needed to recover the eligible costs, not exceeding 5 percentage points above the fixed interest rate of the ECB;

(62) 'data localisation requirement' means any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State;

(63) 'pseudonymisation' means pseudonymisation as referred to under Article 4(5) of Regulation (EU) 2016/679.'

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 caseby-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.~~

8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, 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, such as 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. It 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.~~

11. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, 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, such as 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. It 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~~

CHAPTER V: MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF A PUBLIC EMERGENCY

~~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 15a: Obligation for data holders to make data available on the basis of a public emergency

1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates an exceptional need to use certain data to carry out its statutory duties in the public interest when responding to, mitigating, or supporting the recovery from a public emergency, it may request from data holders that are legal persons, other than public sectors bodies, to make available those data, including the metadata necessary to interpret and use those data. Upon such duly reasoned request, data holders shall make the data and metadata available to the requesting public sector body, the Commission, the European Central Bank or Union body. Such requests may also be made where the production of official statistics is required in relation to a public emergency.

2. Where the data requested are necessary to respond to a public emergency, and the requesting body pursuant to paragraph 1 is unable to obtain such data by other means in a timely and effective manner under equivalent conditions, the request shall concern non-personal data. Where the provision of non-personal data is insufficient to address the public emergency, personal data may also be requested and, where possible, made available in pseudonymized form, subject to appropriate technical and organisational measures to ensure their protection.

3. Where the data requested are necessary to mitigate or support the recovery from a public emergency, a requesting body pursuant to paragraph 1 acting on the basis of Union or national law, may request specific non-personal data, the lack of which prevent it from mitigating or supporting the recovery from a public emergency. Such requests shall not be made to microenterprises and small enterprises.

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.~~

2. This Chapter shall not apply to activities carried out by public sector bodies, the Commission, the European Central Bank or Union bodies relating to 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 Union or national law governing such activities.

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:~~

1. When requesting data pursuant to Article 15a, 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;~~

(b) demonstrate that the conditions to make a request under Article 15a 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 public emergency;

(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;~~

(c) be proportionate to the public emergency and duly justified, regarding the granularity and volume of the data requested and the frequency of access to 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:~~

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 pursuant to Article 15a(2) and without undue delay and, in any event, no later than 30 working days after the receipt of a request pursuant to Article 15a(3), 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:~~

1. A public sector body, the Commission, the European Central Bank or a Union body receiving data pursuant to a request made under Article 15a 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.~~

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 15a. 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 20: Compensation for making data available under Chapter V

1. Data holders shall make available data necessary to respond to a public emergency pursuant to Article 15a(2) 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 15a(3). 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. By way of derogation from paragraph 1 of this Article, a data holder that is a microenterprise or small enterprise may claim compensation for making data available in response to a request under Article 15a(2), according to the conditions set in paragraph 2 of this Article.

4. Data holders shall not be entitled to compensation for making data available in compliance with a request made pursuant to Article 15a(3), 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.

~~**Article 21: Sharing of data obtained in the context of an exceptional need with research organisations or statistical bodies**~~

Article 21: Sharing of data obtained in the context of a public emergency 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.~~

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, it shall without undue delay notify the data holder from whom the data was received, stating the following:

(a) the identity and contact details of the organisation or the individual receiving the data;

(b) the purpose of the transmission or making available of the data;

(c) the period for which the data is to be used and the technical protection;

(d) the organisational measures taken, including where personal data or trade secrets are involved.

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.

Article 22a: Right to lodge a complaint

Where a dispute arises concerning a request for data under Article 15a, including its refusal, modification, the level of compensation, or the transmission or making available of data, the data holder, the public sector body, the Commission, the European Central Bank or the Union body may lodge a complaint with the competent authority, designated pursuant to Article 37, of the Member State where the data holder is established

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.

1a. The obligations laid down in Chapter VI, with the exception of Article 29,and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer, if the provision of such services is based on a contract concluded before or on 12 September 2025.

The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.

1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).

Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.

Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than those referred to in Article 30(1) before its expiry 1 if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.

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.~~

1. Providers of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation 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.~~

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, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation 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:~~

3. In the absence of an international agreement as referred to in paragraph 2, where a provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation 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 or judgement 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.~~

4. If the conditions laid down in paragraph 2 or 3 are met, the provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation 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.~~

5. The provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall inform the natural or legal person whose rights and interests might be affected 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 VIIa: DATA INTERMEDIATION SERVICES AND DATA ALTRUISM ORGANISATIONS

Article 32a: Public Union registers

(1) The Commission shall keep and regularly update public Union registers of:

(a) recognised data intermediation services providers and

(b) recognised data altruism organisations.

(2) Data intermediation services providers registered in the public Union registerreferred to in paragraph 1 point (a) may use the label ‘data intermediation services provider recognised in the Union’ in its written and spoken communication, as well as a common logo referred to in paragraph 4.

(3) Data altruism organisations registered in the public Union register referred to in paragraph 1 point (b) may use the label ‘data altruism organisation recognised in the Union’ in its written and spoken communication, as well as the common logoreferred to in paragraph 4.

(4) In order to ensure that data intermediation services providers recognised in the Union are easily identifiable throughout the Union, the Commission is empowered to adopt implementing acts establishing a design for the common logo. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 46(1a).

Article 32b: Competent authorities for the registration of data intermediation services providers and data altruism organisations

(1) Each Member State shall designate one or more competent authorities responsible for the application and enforcement of this Chapter in accordance with Article 37(1).

(2) The competent authorities shall be set up in a manner so that their independence from any recognised data intermediation services provider or recognised data altruism organisation is guaranteed.

Article 32c: General requirements for registration of recognised data intermediation services providers

In order to qualify for registration in the public Union register referred to in Article 32a paragraph 1 point (a), a data intermediation services provider shall meet all of the following requirements:

(a) they do not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users;

(b) the data they collect with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service, are used only for the development of that data intermediation service;

(c) where they offer additional tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, encryption, anonymisation and pseudonymisation, such tools and services are used only at the explicit request or approval of the data holder or data subject;

(d) where data intermediation service providers which are not micro and small sized enterprises offer value-added services to their clients other than the services referred to in point (c), they fulfil the following conditions:

(i) the value-added services are explicitly requested by the user;

(ii) the data are not used for other purposes than performing the value-added service;

(iii) the value-added services are offered through a functionally separate entity;

(iv) the undertaking seeking to offer the value-added services is not designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925;

(v) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user are not dependent upon whether the data holder or data user uses value-added services provided by the data intermediation services provider or by a related entity;

(e) the data intermediation services provider offering services to data subjects acts in the data subjects' best interest where it facilitates the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible manner about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent.

Article 32d: General requirements for registration of recognised data altruism organisations

In order to qualify for registration in the public Union register referred to in Art. 32a paragraph 1 point (b), a data altruism organisation shall meet all of the following requirements:

(a) they carry out data altruism activities;

(b) they are a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, where applicable;

(c) they operate on a not-for-profit basis and are legally independent from any entity that operates on a for-profit basis;

(d) they carry out their data altruism activities through a structure that is functionally separate from their other activities.

Article 32e: Registration

(1) Data intermediation services provider which meets the requirements set out in Article 32c may submit an application for registration in the public Union register of recognised data intermediation services providers to the competent authority referred to in Article 32b in the Member State in which they have their main establishment.

Data altruism organisation which meets the requirements set out in Article 32d may submit an application for registration in the public Union register of recognised data altruism organisations to the competent authority referred to in Article 32b in the Member State in which they have their main establishment.

(2) Data intermediation services providers and data altruism organisations that have no main establishment in the Union shall designate a legal representative in one of the Member States. The legal representative shall be mandated to be addressed in addition to or instead of the data intermediation services provider or data altruism organisation by competent authorities or data subjects and data holders. The legal representative shall cooperate with and comprehensively demonstrate to the competent authority, upon request, the actions taken and provisions put in place by the data intermediation services provider or the data altruism organisation to ensure compliance with this Regulation.

The data intermediation services provider or data altruism organisation shall be deemed to be under the jurisdiction of the Member State in which the legal representative is located. The designation of a legal representative shall be without prejudice to any legal actions which could be initiated against the data intermediation services provider or data altruism organisation.

(3) Competent authorities shall establish the necessary application forms.

(4) Where a data intermediation services provider has submitted all necessary information pursuant to paragraph 3 of this Article, and complies with the requirements set out in Article 32c, the competent

authority shall, within 12 weeks after the receipt of the application for registration, take a decision on whether the provider complies with the criteria set out in Article 32c. Where the provider complies with the criteria, the competent authority shall submit the relevant information to the Commission which shall register the providers in the public Union register as a recognised data intermediation services provider.

The first subparagraph shall also apply where a data altruism organisation has submitted all necessary information pursuant to paragraph 2, and complies with the registration requirements set out in Article 32d.

The registration in the public Union register shall be valid in all Member States.

(5) The competent authority may charge fees for the registration in accordance with national law. Such fees shall be proportionate and objective and be based on the administrative costs related to the monitoring of compliance. In the case of small-mid caps, small and medium-sized enterprises, and start-ups, the competent authority may charge a discounted fee or waive the fee.

(6) Registered entities shall notify the competent authority of any subsequent changes to the information as provided during the application process or where they cease their data intermediation or data altruism activities in the Union.

(7) The competent authority shall without delay and by electronic means notify the Commission of any notification pursuant to paragraph 6. The Commission shall without undue delay update the public Union register.

Article 32f: Duties of recognised data altruism organisations

(1) Recognised data altruism organisations shall inform data subjects or data holders prior to any processing of their data in a clear and easily comprehensible manner ofthe following:

(a) the objectives of general interest and, if applicable, the specified, explicit and legitimate purpose for which personal data is to be processed, and for which it permits the processing of their data by a data user;

(b) the location of the processing and the objectives of general interest for which it permits any processing carried out in a third country, where the processing is carried out by the recognised data altruism organisation.

(2) Recognised data altruism organisations shall not use the data for other objectives than the objectives of general interest for which the data subject or data holder allows the processing. The recognised data altruism organisation shall not use misleading marketing practices to solicit the provision of data.

(3) Recognised data altruism organisations shall provide electronic means for obtaining consent from data subjects or permissions to process data made available by data holders as well as for their withdrawal.

(4) Recognised data altruism organisations shall, without delay, inform data holders in the event of any unauthorised transfer, access or use of the non-personal data that it has shared.

(5) Where recognised data altruism organisations facilitate data processing by third parties, including by providing tools for obtaining consent from data subjects or permissions to process data made available by data holders, they shall, where relevant, specify the third-country in which the data use is intended to take place.

Article 32g: Monitoring of compliance

(1) The competent authorities referred to in Article 32b shall, either on their own initiative or on a request by a natural or legal person, monitor and supervise whether recognised data intermediation services providers and recognised data altruism organisations comply with the requirements laid down in this Chapter, including whether they continue to comply with the requirements for registration laid down therein.

(2) The competent authorities shall have the power to request from recognised data intermediation services providers or recognised data altruism organisations, or their legal representative, all the information that is necessary to verify compliance with the requirements laid down in this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

(3) Where a competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter, it shall notify that entity, or its legal representative, of those findings and give it the opportunity to state its views, within 30 days of the receipt of the notification.

(4) The competent authority shall have the power to require the cessation of the noncompliance referred to in paragraph 3 either immediately or within a reasonable time limit and shall take appropriate and proportionate measures with the aim of ensuring compliance.

(5) If a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter even after having been notified in accordance with paragraph 3, that entity shall:

(a) lose its right to use the label referred to in Article 32a in written and spoken communication;

(b) be removed from the public Union register referred to in Article 32a.

Any decision revoking the right to use the label as referred to in the first subparagraph, point (a), shall be made public by the competent authority.

CHAPTER VIIb: Free flow of non-personal data in the Union

Article 32h: Prohibition of localisation requirements for non-personal data within the Union

(1) Data localisation requirements for non-personal data shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality or laid down on the basis of Union law.

(2) Member States shall immediately communicate to the Commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement in accordance with the procedures set out in Articles 5, 6 and 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council.

Chapter VIIc: Re-use of data and documents held by public sector bodies

SECTION 1: GENERAL PROVISIONS

Article 32i: Subject matter and scope

(1) This Chapter establishes a set of rules governing the re-use and the practical arrangements for facilitating the re-use of the following:

(a) existing data and documents held by public sector bodies of the Member States, including certain categories of protected data;

(b) existing data and documents held by public undertakings that are:

(i) active in the areas referred to in Chapter II of Directive 2014/25/EU of the European Parliament and of the Council;

(ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007 of the European Parliament and of the Council;

(iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008 of the European Parliament and of the Council; or

(iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Council Regulation (EEC) No 3577/92 ;

(c) research data pursuant to the conditions set out in Article 32t.

(2) This Chapter does not apply to the following:

(a) data and documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or, in the absence of such rules, as defined in accordance with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;

(b) data and documents held by public undertakings and:

(i) produced outside the scope of the provision of services in the general interest as defined by law or other binding rules in the Member State;

(ii) related to activities directly exposed to competition and therefore, pursuant to Article 34 of Directive 2014/25/EU, not subject to procurement rules;

(c) data and documents, such as sensitive data, which are excluded from access by virtue of the access regimes in the Member State on grounds of the protection of national security (namely, State security), defence, or public security;

(d) data and documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit.

(3) Section 2 of this Chapter does not apply to:

(a) data or documents, such as sensitive data or documents, which are excluded from access by virtue of the access regimes in the Member State, including on grounds of:

(i) statistical confidentiality;

(ii) commercial confidentiality (including business, professional or company secrets);

(b) data or documents access to which is restricted by virtue of the access regimes in the Member States,

(i) including cases whereby citizens or legal entities have to prove a particular interest to obtain access to documents;

(ii) on grounds of protection of personal data, and parts of data or documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data; logos, crests and insignia;

(c) data or documents for which third parties hold intellectual property rights;

(d) data or documents held by cultural establishments other than libraries, including university libraries, museums and archives;

(e) data or documents held by educational establishments of secondary level and below, and, in the case of all other educational establishments, data other than those referred to in paragraph 1, point (c);

(f) data or documents other than those referred to in paragraph 1, point (c), held by research performing organisations and research funding organisations, including organisations established for the transfer of research results;

(g) Data or documents access to which is excluded or restricted on grounds of critical entity or critical infrastructure protection related information as defined in points (1) and (4) of Article 2 of Directive (EU) 2022/2557.

(4) Section 3 of this Chapter does not apply to:

(a) data and documents that are not certain categories of protected data;

(b) data or documents held by public undertakings;

(c) data or documents held by cultural establishments and educational establishments;

(d) data and documents covered by Section 2 of this Chapter.

(5) This Chapter builds on, and is without prejudice to, Union and national access regimes, in particular with regard to the granting of access to and disclosure of official documents.

(6) The obligations imposed in accordance with this Chapter shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (Berne Convention), the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS Agreement and the World Intellectual Property Organization Copyright Treaty (WCT).

(7) The right for the maker of a database provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of data and documents or to restrict re-use beyond the limits set by this Chapter.

(8) This Chapter governs the re-use of existing data and documents held by public sector bodies and public undertakings of the Member States, including data and documents to which Directive 2007/2/EC of the European Parliament and of the Council applies.

(9) This Chapter is without prejudice to Union and national law and international agreements to which the Union or Member States are party on the protection of categories of data or documents referred to in Article 2(54).

Article 32j: Non-discrimination

(1) Any applicable conditions for the re-use of data or documents shall be nondiscriminatory, transparent, proportionate and objectively justified with regard to the categories of data or documents and the purposes of re-use and the nature of the data or documents for which re-use is allowed. Those conditions shall not be used to restrict competition. This principle shall equally apply for comparable categories of re-use, including for cross-border re-use.

(2) If data or documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the data or documents for those activities as the ones that apply to other re-users.

Article 32k: Exclusive arrangements

(1) The re-use of data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements or practices pertaining to the re-use of data or documents, which have as their objective or effect to grant exclusive rights or to restrict the availability of data or documents for re-use by entities other than the parties to such agreements, arrangements or practices, shall be prohibited.

(2) By way of derogation of paragraph 1, where an exclusive right is necessary for the provision of a service of general interest, such a right may be granted to the extent necessary for the provision of the service or the supply of the product under the following conditions:

(a) the exclusive right is granted through an administrative act or contractual agreement in accordance with applicable Union and national law and in compliance with the principles of transparency, equal treatment and non-discrimination.

(b) the agreements granting the exclusive right, including the reasons as to why it is necessary to grant such a right, is transparent and made publicly available online, in a form that complies with relevant Union law on public procurement and national law.

(c) except for exclusive rights related to the digitisation of cultural resources, the validity of the reason for granting exclusive rights concerning data and documents within the scope of Section 2 shall be subject to regular review, and shall in any event, be reviewed every three years.

(d) exclusive arrangements established on or after 16 July 2019 shall be made publicly available online at least two months before they come into effect. The final terms of such arrangements shall be transparent and shall be made publicly available online.

(3) By way of derogation of paragraph 1, where an exclusive right relates to the digitisation of cultural resources, the period of exclusivity shall in general not exceed 10 years. Where that period exceeds 10 years, its duration shall be in accordance with applicable Union and national law subject to review during the 11th year and, if applicable, every seven years thereafter.

(4) In the case of an exclusive right referred to in paragraph 3, the public sector body concerned shall be provided free of charge with a copy of the digitised cultural resources as part of those arrangements. That copy shall be available for re-use at the end of the period of exclusivity.

(5) For certain categories of protected data, the duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded, the duration of the contract shall be the same as the duration of the exclusive right.

(6) Agreements or other arrangements or practices that, without expressly granting an exclusive right, aim at, or could reasonably be expected to lead to, a restricted availability for the re-use of data and documents within the scope of Section 2 by entities other than parties to such arrangements shall be made publicly available online at least two months before their coming into effect. The effect of such legal or practical arrangements on the availability of data for re-use shall be subject to regular reviews and shall, in any event, be reviewed every three years. The final terms of such arrangements shall be transparent and made publicly available online.

(7) For existing exclusive arrangements, the following shall apply:

(a) exclusive arrangements concerning data and documents within the scope of Section 2existing on 17 July 2013 that do not qualify for the exceptions set out in paragraphs 2 and 3 and that were entered into by public sector bodies shall be terminated at the end of the contract and in any event not later than 18 July 2043;

(b) exclusive arrangements concerning data and documents within the scope of Section 2 existing on 16 July 2019 that do not qualify for the exceptions set out in paragraphs 2 and 3, and that were entered into by public undertakings, shall be terminated at the end of the contract and in any event not later than 17 July 2049;

Article 32l: General principles relating to charging

(1) Any charges set out under Section 2 or Section 3 shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition.

(2) In the case of standard charges for the re-use of data or documents, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be established in advance and published, through electronic means where possible and appropriate.

(3) In the case of charges for the re-use other than those referred to in paragraph 1, the factors that are taken into account in the calculation of those charges shall be indicated at the outset. Upon request, the holder of the data or documents in question shall also indicate the way in which such charges have been calculated in relation to a specific re-use request.

(4) Public sector bodies shall ensure that any charges can also be paid online through widely available cross-border payment services, without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union.

Article 32m: Information on means of redress

Public sector bodies shall ensure that applicants for re-use of data or documents are informed of available means of redress relating to decisions or practices affecting them.

SECTION 2: RE-USE OF OPEN GOVERNMENT DATA

Subsection 1: Scope and General Principles

Article 32n: General principle for re-use of open government data

(1) Data or documents in scope of this Section shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3.

(2) For data or documents in which libraries, including university libraries, museums and archives hold intellectual property rights and for data or documents held by public undertakings, where the re-use of such data or documents is allowed, those data or documents shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3.

Subsection 2: Requests for re-use

Article 32o: Processing requests for re-use

(1) Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time frames laid down for the processing of requests for access to data or documents.

(2) Where no time limits or other rules regulating the timely provision of data or documents have been established, public sector bodies shall process the request and shall deliver the data or documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible, and in any event within 20 working days of receipt. That time frame may be extended by a further 20 working days in the case of extensive or complex requests. In such cases, the applicant shall be notified as soon as possible, and in any event within three weeks of the initial request, that more time is needed to process the request and the reasons why.

(3) In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or the provisions of this Regulation, in particular points (a) to (c) of paragraph 2 of Article 32i and points (a) to (d) of paragraph 3 of Article 32i or Article 32n (general principle ODD Section). Where a negative decision is based on point (d) of paragraph 3 of Article 32i, the public sector body shall include a reference to the natural or legal person who is the rightsholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries, including university libraries, museums and archives, shall not be required to include such a reference.

(4) The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to data or documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned.

(5) For the purposes of this Article, Member States shall establish practical arrangements to facilitate effective re-use of data or documents. Those arrangements may in particular include the means to supply adequate information on the rights provided for in this Regulation and to offer relevant assistance and guidance.

(6) This Article shall not apply to the following entities:

(a) public undertakings;

(b) educational establishments, research performing organisations and research funding organisations.

Subsection 3: Conditions for re-use

Article 32p: Available formats

(1) Without prejudice to Subsection 5, public sector bodies and public undertakings shall make their data or documents available in any pre-existing format or language and, where possible and appropriate, by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata.

Both the format and the metadata shall, where possible, comply with formal open standards.

(2) Member States shall encourage public sector bodies and public undertakings to produce and make available data or documents falling within the scope of this Section in accordance with the principle of 'open by design and by default.

(3) Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt data or documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.

(4) Public sector bodies shall not be required to continue the production and storage of a certain type of document with a view to the re-use of such data or documents by a private or public sector organisation.

(5) Public sector bodies shall make dynamic data available for re-use immediately after collection, via suitable APIs and, where relevant, as a bulk download.

(6) Where making dynamic data available for re-use immediately after collection, as referred to in paragraph 5, would exceed the financial and technical capacities of the public sector body, thereby imposing a disproportionate effort, those dynamic data shall be made available for re-use within a time frame or with temporary technical restrictions that do not unduly impair the exploitation of their economic and social potential.

(7) Paragraphs 1 to 6 shall apply to existing data or documents held by public undertakings which are available for re-use.

(8) The high-value datasets, as listed in accordance with Article 32v(1) shall be made available for re-use in machine- readable format, via suitable APIs and, where relevant, as a bulk download.'

Article 32q: Principles governing charging for open government data

(1) The re-use of data or documents within the scope of this Section shall be free of charge. However, the recovery by the public sector body holding the data of the marginal costs incurred for the reproduction, provision and dissemination of such data or documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed.

(2) Paragraph 1 shall not apply to the following entities:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) libraries, including university libraries, museums and archives;

(c) public undertakings.

(3) Member States shall publish online a list of the public sector bodies referred to in paragraph 2, point (a).

(4) In the cases referred to in paragraph 2, points (a) and (c), the total charges shall be calculated in accordance with objective, transparent and verifiable criteria. Such criteria shall be laid down by Member States. The total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of their collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment, and where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information. Charges shall be calculated in accordance with the applicable accounting principles.

(5) Where charges are made by the public sector bodies referred to in paragraph 2, point (b), the total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, data storage, preservation and rights clearance and, where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information, together with a reasonable return on investment. Charges shall be calculated in accordance with the accounting principles applicable to the public sector bodies involved.

(6) Public sector bodies may set out higher charges for the re-use of data and documents by very large enterprises than the charges provided for in paragraphs 1, 4 and 5. Any such charges shall be proportionate and based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. In addition to the elements listed in paragraph 1 of this Article, such charges may cover the cost of collection, production, reproduction dissemination and data storage and where applicable the

cost of anonymisation or measures to protect the confidentiality of the data or documents, together with a reasonable return on investment.

(7) The re-use of the following shall be free of charge for the user:

(a) subject to Article 32v paragraph (3), (4) and (5), the high-value datasets, as listed in accordance with paragraph 1 of that Article;

(b) research data referred to in point (c) of paragraph 1 of Article 32i.

Article 32r: Standard licences

(1) The re-use of data or documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective.

(2) When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

(3) In Member States where licences are used, public sector bodies shall ensure that the standard licences for the re-use of public sector data or documents, which can be adapted to meet particular licence applications, are available in digital format and able to be processed electronically.

(4) Public sector bodies may establish special conditions for the re-use of data and documents by very large enterprises. Such conditions shall be proportionate and should be based on objective criteria. They shall be established taking into consideration the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925.

Article 32s: Practical arrangements

(1) Member States shall make practical arrangements facilitating the search for data or documents available for re-use, such as asset lists of main data or documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists. Where possible, Member States shall facilitate the cross-linguistic search for data or documents, in particular by enabling metadata aggregation at Union level. Member States shall also encourage public sector bodies to make practical arrangements facilitating the preservation of data or documents available for re-use.

(2) Member States shall, in cooperation with the Commission, continue efforts to simplify access to datasets, in particular by providing a single point of access and by progressively making available suitable datasets held by public sector bodies with regard to the data or documents to which this Section applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means.

Subsection 4: Research data

Article 32t: Research data

(1) Member States shall support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available ('open access policies'), following the principle of 'open by default' and compatible with the FAIR principles. In that context, concerns relating to intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests, shall be taken into account in accordance with the principle of 'as open as possible, as closed as necessary'. Those open access policies shall be addressed to research performing organisations and research funding organisations.

(2) Without prejudice to Article 32n, paragraph 3, point (d), research data shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account.

Subsection 5: High-value datasets

Article 32u: Thematic categories of high-value datasets

(1) The thematic categories of high-value datasets shall be as set out in Annex I.

(2) The Commission is empowered to adopt delegated acts in accordance with Article 45(2a) in order to amend Annex I by adding new thematic categories of high-value datasets reflecting technological and market developments.

Article 32v: Specific high-value datasets and arrangements for publication and re-use

(1) The Commission shall adopt implementing acts laying down a list of specific high-value datasets belonging to the categories set out in Annex I and held by public sector bodies and public undertakings among the data or documents to which this Section applies.

Such specific high-value datasets shall be:

(a) available free of charge, subject to paragraphs 3, 4 and 5;

(b) machine readable;

(c) provided via APIs; and

(d) provided as a bulk download, where relevant.

Those implementing acts may specify the arrangements for the publication and reuse of high-value datasets. Such arrangements shall be compatible with open standard licences.

The arrangements may include terms applicable to re-use, formats of data and metadata and technical arrangements for dissemination. Investments made by the Member States in open data approaches, such as investments into the development and roll-out of certain standards, shall be taken into account and balanced against the potential benefits from inclusion in the list.

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

(2) The identification of specific high-value datasets pursuant to paragraph 1 shall be based on the assessment of their potential to:

(a) generate significant socioeconomic or environmental benefits and innovative services;

(b) benefit a high number of users, in particular SMEs and SMCs;

(c) assist in generating revenues; and

(d) be combined with other datasets.

For the purpose of identifying such specific high-value datasets, the Commission shall carry out appropriate consultations, including at expert level, conduct an impact assessment and ensure complementarity with existing legal acts, such as Directive 2010/40/EU of the European Parliament and of the Council, with respect to the re-use of data or documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment.

(3) By way of derogation from paragraph 1, second subparagraph, point (a), the implementing acts referred to in that paragraph shall provide that the availability of high-value datasets free of charge is not to apply to specific high-value datasets held by public undertakings where that would lead to a distortion of competition in the relevant markets.

(4) The requirement to make high-value datasets available free of charge pursuant to point (a) of the second subparagraph of paragraph 1 shall not apply to libraries, including university libraries, museums and archives.

(5) Where making high-value datasets available free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of the bodies involved, Member States may exempt those bodies from the requirement to make those high-value datasets available free of charge for a period of no more than two years following the entry into force of the relevant implementing act adopted in accordance with paragraph 1.

Section 3: Re-use of certain categories of protected data held by public sector bodies

Article 32w: Conditions for re-use

(1) Public sector bodies which are competent under national law to grant or refuse access for the re-use of data or documents belonging to certain categories of protected data shall make publicly available the conditions for allowing such re-use and the procedure to request the re-use via the single information point referred to in Article 32aa. Where they grant or refuse access for re-use, they may be assisted by the competent bodies referred to in Article 32z (1).

Member States shall ensure that public sector bodies are equipped with the necessary resources to comply with this Article and Article 32x.

(2) Re-use of data or documents shall not affect the protected nature of those data or documents and shall only be allowed:

(a) in compliance with intellectual property rights.

(b) if data that is considered confidential in accordance with Union or national law on commercial or statistical confidentiality, is not disclosed, as a result of allowing re-use, unless such re-use is allowed based on the data subject's consent or the data holder's permission in accordance with paragraph 5.

(c) in compliance with Regulation (EU) 2016/679.

(3) To ensure the preservation of the protected nature as referred to in paragraph 2, public sector bodies may establish the following requirements:

(a) to grant access for the re-use of data or documents only where the public sector body or the competent body, following the request for re-use, has ensured that those data or documents have been:

(i) anonymised, in the case of personal data;

(ii) subject to other forms of preparation of personal data;

(iii) modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights;

(b) to access and re-use the data or documents remotely within a secure processing environment that is provided or controlled by the public sector body;

(c) to access and re-use the data or documents within the physical premises in which the secure processing environment is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties.

In the case of re-use allowed in accordance with the first subparagraph, point (a)(i), the re-use of data or documents shall be subject to the rules on open government data set out in Section 2. This is without prejudice to Article 32y, which prevails in case of conflict.

In the case of re-use allowed in accordance with the first subparagraph, points (b) and (c), the public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used.

(4) The public sector body shall reserve the right to verify the process, the means and any results of processing of data or documents undertaken by the re-user to preserve the integrity of the protection of the data or documents. It shall also reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user.

Unless national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of certain categories of protected data, the public sector body shall make the re-use of data or documents provided in accordance with paragraph 3 conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties and that the re-user may have acquired despite the safeguards put in place. In the event of the unauthorised re-use of non-personal data, the re-user shall be obliged, without delay, where appropriate with the assistance of the public sector body, to inform the natural or legal persons whose rights and interests may be affected.

(5) Where the re-use of data or documents cannot be allowed in accordance with paragraphs 3 and 4, re-use shall only be possible:

(a) where there is no legal basis other than consent for transmitting the data under Regulation (EU) 2016/679, with the consent of the data subjects;

(b) with the permission from the data holders whose rights and interests may be affected by such re-use.

The public sector body shall make best efforts, in accordance with Union and national law, to provide assistance to potential re-users in seeking consent of the data subjects or permission from the data holders whose rights and interests may be affected by such re-use, where this is feasible without a disproportionate burden on the public sector body.

Where it provides such assistance, the public sector body may be assisted by the competent bodies referred to in Article 32z.

Article 32x: Requirements for transfers of non-personal data to third countries by re-users

(1) Where a re-user intends to transfer certain categories of protected data that are non-personal to a third country, it shall inform the public sector body of its intention to transfer such data and the purpose

of such transfer at the time of requesting the re-use of the data. In the case of re-use based on the data holder's permission the re-user shall, where appropriate with the assistance of the public sector body, inform the natural or legal person whose rights and interests may be affected of that intention, purpose and the appropriate safeguards. The public sector body shall not allow the re-use unless the natural or legal person gives permission for the transfer.

(2) Public sector bodies shall transmit non-personal confidential data or data protected by intellectual property rights to a re-user which intends to transfer those data to a third country other than a country designated in accordance with paragraph 7 only if the re-user contractually commits to:

(a) complying with the obligations imposed in accordance with intellectual property rights and Union or national law on commercial or statistical confidentiality even after the data is transferred to the third country;

(b) accepting the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body with regard to any dispute related to compliance with intellectual property rights and Union or national law on commercial or statistical confidentiality.

(3) The Commission may adopt implementing acts establishing model contractual clauses for complying with the obligations referred to in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

(4) Public sector bodies shall, where relevant and to the extent of their capabilities, provide guidance and assistance to re-users in complying with the obligations referred to in paragraph 2.

(5) Where justified because of the substantial number of requests across the Union concerning the re-use of non- personal data in specific third countries, the Commission may adopt implementing acts declaring that the legal, supervisory and enforcement arrangements of a third country:

(a) ensure protection of intellectual property and trade secrets in a way that is essentially equivalent to the protection ensured under Union law;

(b) are being effectively applied and enforced; and

(c) provide effective judicial redress.

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

(7) Specific Union legislative acts may deem certain non-personal data categories held by public sector bodies to be highly sensitive for the purposes of this Article where their transfer to third countries may put at risk Union public policy objectives, such as safety and public health or may lead to the risk of re-identification of non-personal, anonymised data. Where such an act is adopted, the Commission shall

adopt delegated acts in accordance with Article 45 supplementing this Regulation by laying down special conditions applicable to the transfers of such data to third countries.

If required by a specific Union legislative act referred to in the first subparagraph, such special conditions may include terms applicable for the transfer or technical arrangements in this regard, limitations with regard to the re-use of data in third countries or categories of persons entitled to transfer such data to third countries or, in exceptional cases, restrictions with regard to transfers to third countries.

The re-user to whom the right to re-use non-personal data was granted may transfer the data only to those third countries for which the requirements set out in paragraphs 2, 4 and 5 are met.

Article 32y: Fees

(1) Public sector bodies which allow re-use of certain categories of protected data may charge fees for allowing the re-use of such data.

(2) Where public sector bodies charge fees, they shall take measures to provide incentives for the re-use of certain categories of protected data for non-commercial purposes, such as scientific research purposes, and by start-ups, SMEs and SMCs in accordance with Union State aid rules. In that regard, public sector bodies may also make the data available at a discounted fee or free of charge, in particular to startups, SMEs and SMCs, civil society, research and educational establishments. To that end, public sector bodies may establish a list of categories of re-users to which data or documents for re-use is made available at a discounted fee or free of charge. That list, together with the criteria used to establish it, shall be made public.

(3) Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of certain categories of protected data and limited to the necessary costs in relation to:

(a) the reproduction, provision and dissemination of data;

(b) the clearance of rights;

(c) anonymisation or other forms of preparation of personal data and commercially confidential data as provided for in Article 32w(3)[conditions for re-use];

(d) the maintenance of the secure processing environment;

(e) the acquisition of the right to allow re-use in accordance with this Section by third parties outside the public sector; and assisting re-users in seeking consent from data subjects and permission from data holders whose rights and interests may be affected by such re-use.

(4) The criteria and methodology for calculating fees shall be laid down by the Member States and published. The public sector body shall publish a description of the main categories of costs and the rules used for the allocation of costs.

(5) Public sector bodies may charge higher fees than those allowed in accordance with paragraph 2 and 3 of this Article with respect to very large enterprises, based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. Any such calculated fees shall be proportionate. In addition to the elements listed in paragraph 3 of this Article, they can cover the cost of collection and production of the data, together with a reasonable return on investment.

Article 32z: Competent bodies

(1) For the purpose of carrying out the tasks referred to in this Article, each Member State shall designate one or more competent bodies in accordance with Article 37(1), which may be competent for particular sectors, but that collectively need to cover all sectors, to assist the public sector bodies which grant or refuse access for the re-use of certain categories of protected data. Member States may either establish one or more new competent bodies or rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions laid down in this Section.

(2) The competent bodies may be empowered to grant access for the re-use of certain categories of protected data pursuant to Union or national law which provides for such access to be granted. Where they grant or refuse access for re-use, those competent bodies shall be subject to Articles 32k, 32w, 32x, 32y and 32ab.

(3) The competent bodies shall have adequate legal, financial, technical and human resources to carry out the tasks assigned to them, including the necessary technical knowledge to be able to comply with relevant Union or national law concerning the access regimes for the categories of protected data referred to in in Article 2(54).

(4) The assistance referred to in paragraph 1 shall include, where necessary:

(a) providing technical support by making available a secure processing environment for providing access for the re-use of data or documents;

(b) providing guidance and technical support on how to best structure and store data to make that those data or documents easily accessible;

(c) providing technical support for anonymization, pseudonymisation and state-ofthe-art privacy-preserving methods. not limited to personal data, but also to commercially confidential information, including trade secrets or content protected by intellectual property rights;

(d) assisting the public sector bodies, where relevant, to provide support to re-users in requesting consent for re-use from data subjects or permission from data holders in line with their specific decisions, including on the jurisdiction in which the data processing is intended to take place and assisting the public sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible;

(e) providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 32x(2).

Article 32aa: Single information point

(1) Each Member State shall designate a single information point. That point shall make available easily accessible information concerning the application of Articles 32w, 32x and 32y.

(2) The single information point shall be competent to receive enquiries or requests for the re-use of the certain categories of protected data and shall transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies referred to in Paragraph 1 of Article 32z, where relevant.

(3) The single information point may include a separate, simplified and well-documented information channel for SMEs, SMCs, start-ups and research establishments addressing their needs and capabilities in requesting the re-use of the categories of data referred to in Article 2(54).

(4) The single information point shall make available by electronic means a searchable asset list containing an overview of all available document resources including, where relevant, those document resources that are available at sectoral, regional or local information points, with relevant information describing the available data or documents, including at least the data format and size and the conditions for their re-use.

(5) The Commission shall establish a European single access point offering a searchable electronic register of data or documents available in the national single information points and further information on how to request data or documents via those national single information points.

Article 32ab: Procedure for requests for re-use

(1) Unless shorter time limits have been established in accordance with national law, the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall adopt a decision on the request for the re-use of certain categories of protected data within two months of the date of receipt of the request.

(2) In the case of exceptionally extensive and complex requests for re-use, that two-month period may be extended by up to 30 days. In such cases the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall notify the applicant as soon as possible that more time is needed for conducting the procedure, together with the reasons for the delay.

(3) Any natural or legal person directly affected by a decision as referred to in paragraph 1 shall have an effective right of redress in the Member State where the relevant body is located. Such a right of redress shall be laid down in national law and shall include the possibility of review by an impartial body with the appropriate expertise, such as the national competition authority, the relevant access-to-documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or

a national judicial authority, whose decisions are binding upon the public sector body or the competent body concerned.

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.~~

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:

(a) 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;

(b) any matter falling within the scope of this Regulation specifically against a recognised data intermediation services provider or a recognised data altruism organisation, with the relevant competent authority for the registration of data intermediation services or the relevant competent authority for the registration of data altruism organisations.

(2) 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.

(3) The competent authority with which the complaint has been lodged shall inform the complainant, in accordance with national law, of:

(a) the progress of the proceedings, of the decision taken; and

(b) the judicial remedies provided for in Article 39.'

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.

6. This Article shall not apply to Chapter VIIc.

CHAPTER IXa: European Data Innovation Board

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 41a: European Data Innovation Board

(1) The European Data Innovation Board is established as a means to advising and assisting the Commission in coordinating the enforcement of this Regulation and to serve as a forum of discussion for the development of a European data economy and data policies.

(2) It shall be composed at least of representatives of Member States competent for

matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group.

(3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks.

(4) The Commission shall chair the meetings of the European Data Innovation Board.

~~**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).~~

Article 42: Role of the EDIB

(1) The EDIB shall support the consistent application of this Regulation by:

(a) serving as a forum for strategic discussions on data policies, data governance, international data flows and cross-sectoral developments relevant to the European data economy;

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

(c) facilitating cooperation between competent authorities through capacitybuilding and the exchange of information;

(d) fostering an exchange of experience and good practice between the Member States in the field of re-use of public sector information in collaboration with other relevant governance bodies.

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.~~

2. The power to adopt delegated acts referred to in Article 29(7), Article 32u(2) and Article 33(2) shall be conferred on the Commission for an indeterminate period of time.

~~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.~~

3. The delegation of power referred to in Article 29(7), Article 32u(2) 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.~~

6. A delegated act adopted pursuant to Article 29(7), Article 32u(2) 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.~~ The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

1a. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

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:~~

1. By 12 September 2028, the Commission shall carry out an evaluation of chapters II, III, IV, V, VI, VII, and VIII 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.~~

(m) the impact of this Regulation on SMEs and SMCs 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.

2a. By [date = entry into force plus 5 years], the Commission shall carry out an evaluation of chapters VIIa, VIIb and VIIc of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee.

The report shall assess, in particular:

(a) the state of registrations of data intermediation services and the type of services they offer;

(b) the type of data altruism organisations registered and an overview of the objectives of general interests for which data are shared in view of establishing clear criteria in that respect.'

(c) the scope and social and economic impact of Chapter VIIc Section 2 including

(d) the extent of the increase in re-use of public sector documents to which Section 2 of Chapter VIIc applies, especially by SMEs and SMCs;

(e) the impact of the high-value datasets;

(f) the interaction between data protection rules and re-use possibilities;

(g) Member States shall provide the Commission with the Information necessary for the preparation of that report.

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.

5. On the basis of the reports referred to in paragraphs 1, and 2 and 2a, 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	For the Council
The President - R. METSOLA	The President - P. NAVARRO RÍO

Annex I: List of thematic categories of high-value datasets, as referred to in Article 32ab(1) of Regulation (EU) 2023/2854

1. Geospatial

2. Earth observation and environment

3. Meteorological

4. Statistics

5. Companies and company ownership

6. Mobility