I

*(Legislative acts)*

# REGULATIONS

## REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## of 30 May 2022

## on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

**(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) The Treaty on the Functioning of the European Union (TFEU) provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted. The establishment of common rules and practices in the Member States relating to the development of a framework for data governance should contribute to the achievement of those objectives, while fully respecting fundamental rights. It should also guarantee the strengthening of the open strategic autonomy of the Union while fostering international free flow of data.

(2) Over the last decade, digital technologies have transformed the economy and society, affecting all sectors of activity and daily life. Data is at the centre of that transformation: data-driven innovation will bring enormous benefits to both Union citizens and the economy, for example by improving and personalising medicine, providing new mobility, and contributing to the communication of the Commission of 11 December 2019 on the European Green Deal. In order to make the data-driven economy inclusive for all Union citizens, particular attention must be paid to reducing the digital divide, boosting the participation of women in the data economy and fostering cutting-edge European expertise in the technology sector. The data economy has to be built in a way that enables undertakings, in particular micro, small and medium-sized enterprises (SMEs), as defined in the Annex to Commission Recommendation 2003/361/EC ([3]), and start-ups to thrive, ensuring data access neutrality and data portability and interoperability, and avoiding lock-in effects. In its communication of 19 February 2020 on a European strategy for data (the 'European strategy for data'), the Commission described the vision of a common European data space, meaning an internal market for data in which data could be used irrespective of its physical storage location in the Union in compliance with applicable law, which, *inter alia*, could be pivotal for the rapid development of artificial intelligence technologies.

([1]) OJ C 286, 16.7.2021, p. 38.

([2]) Position of the European Parliament of 6 April 2022 (not yet published in the Official Journal) and decision of the Council of 16 May 2022.

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

The Commission also called for the free and safe flow of data with third countries, subject to exceptions and restrictions for public security, public order and other legitimate public policy objectives of the Union, in line with international obligations, including on fundamental rights. In order to turn that vision into reality, the Commission proposed establishing domain-specific common European data spaces for data sharing and data pooling. As proposed in the European strategy for data, such common European data spaces could cover areas such as health, mobility, manufacturing, financial services, energy or agriculture, or a combination of such areas, for example energy and climate, as well as thematic areas such as the European Green Deal or European data spaces for public administration or skills. Common European data spaces should make data findable, accessible, interoperable and re-usable (the 'FAIR data principles'), while ensuring a high level of cybersecurity. Where there is a level playing field in the data economy, undertakings compete on quality of services, and not on the amount of data they control. For the purposes of the design, creation and maintenance of the level playing field in the data economy, sound governance is needed in which relevant stakeholders of a common European data space need to participate and be represented.

(3) It is necessary to improve the conditions for data sharing in the internal market, by creating a harmonised framework for data exchanges and laying down certain basic requirements for data governance, paying specific attention to facilitating cooperation between Member States. This Regulation should aim to develop further the borderless digital internal market and a human-centric, trustworthy and secure data society and economy. Sector-specific Union law can develop, adapt and propose new and complementary elements, depending on the specificities of the sector, such as the Union law envisaged on the European health data space and on access to vehicle data. Moreover, certain sectors of the economy are already regulated by sector-specific Union law, which includes rules relating to the sharing of or access to data across borders or across the Union, for example Directive 2011/24/EU of the European Parliament and of the Council ([4]) in the context of the European health data space, and relevant legislative acts in the field of transport, such as Regulations (EU) 2019/1239 ([5]) and (EU) 2020/1056 ([6]) and Directive 2010/40/EU ([7]) of the European Parliament and of the Council in the context of the European mobility data space.

([4]) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

([5]) Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU (OJ L 198, 25.7.2019, p. 64).

([6]) Regulation (EU) 2020/1056 of the European Parliament and of the Council of 15 July 2020 on electronic freight transport information (OJ L 249, 31.7.2020, p. 33).

([7]) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

This Regulation should therefore be without prejudice to Regulations (EC) No 223/2009 ([8]), (EU) 2018/858 ([9]) and (EU) 2018/1807 ([10]) as well as Directives 2000/31/EC ([11]), 2001/29/EC ([12]), 2004/48/EC ([13]), 2007/2/EC ([14]), 2010/40/EU, (EU) 2015/849 ([15]), (EU) 2016/943 ([16]), (EU) 2017/1132 ([17]), (EU) 2019/790 ([18]) and (EU) 2019/1024 ([19]) of the European Parliament and of the Council and any other sector-specific Union law that regulates access to and re-use of data. This Regulation should be without prejudice to Union and national law on the access to and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as international cooperation in that context.

This Regulation should be without prejudice to the competences of the Member States with regard to their activities concerning public security, defence and national security. The re-use of data protected for such reasons and held by public sector bodies, including data from procurement procedures falling within the scope of Directive 2009/81/EC of the European Parliament and of the Council ([20]), should not be covered by this Regulation. A horizontal regime for the re-use of certain categories of protected data held by public sector bodies, the provision of data intermediation services and of services based on data altruism in the Union should be established. Specific characteristics of different sectors may require the design of sectoral data-based systems, while building on the requirements of this Regulation. Data intermediation services providers that meet the requirements laid down in this Regulation should be able to use the label 'data intermediation services provider recognised in the Union'. Legal persons that seek to support objectives of general interest by making available relevant data based on data altruism at scale and that meet the requirements laid down in this Regulation should be able to register as and use the label 'data altruism organisation recognised in the Union'. Where sector-specific Union or national law requires public sector bodies, such data intermediation services providers or such legal persons (recognised data altruism organisations) to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law should also apply.

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

([9]) Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

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

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

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

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

([14]) Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) (OJ L 108, 25.4.2007, p. 1).

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

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

([17]) Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (OJ L 169, 30.6.2017, p. 46).

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

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

([20]) Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC (OJ L 216, 20.8.2009, p. 76).

(4) This Regulation should be without prejudice to Regulations (EU) 2016/679 ([21]) and (EU) 2018/1725 ([22]) of the European Parliament and of the Council and to Directives 2002/58/EC ([23]) and (EU) 2016/680 ([24]) of the European Parliament and of the Council and the corresponding provisions of national law, including where personal and non-personal data in a data set are inextricably linked. In particular, this Regulation should not be read as creating a new legal basis for the processing of personal data for any of the regulated activities, or as amending the information requirements laid down in Regulation (EU) 2016/679. The implementation of this Regulation should not prevent cross-border transfers of data in accordance with Chapter V of Regulation (EU) 2016/679. In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data should prevail. It should be possible to consider data protection authorities to be competent authorities under this Regulation. Where other authorities function as competent authorities under this Regulation, they should do so without prejudice to the supervisory powers and competences of data protection authorities under Regulation (EU) 2016/679.

(5) Action at Union level is necessary to increase trust in data sharing by establishing appropriate mechanisms for control by data subjects and data holders over data that relates to them, and in order to address other barriers to a well-functioning and competitive data-driven economy. That action should be without prejudice to obligations and commitments in the international trade agreements concluded by the Union. A Union-wide governance framework should have the objective of building trust among individuals and undertakings in relation to data access, control, sharing, use and re-use, in particular by establishing appropriate mechanisms for data subjects to know and meaningfully exercise their rights, as well as with regard to the re-use of certain types of data held by the public sector bodies, the provision of services by data intermediation services providers to data subjects, data holders and data users, as well as the collection and processing of data made available for altruistic purposes by natural and legal persons. In particular, more transparency regarding the purpose of data use and conditions under which data is stored by undertakings can help increase trust.

(6) The idea that data that has been generated or collected by public sector bodies or other entities at the expense of public budgets should benefit society has been part of Union policy for a long time. Directive (EU) 2019/1024 and sector-specific Union law ensure that the public sector bodies make more of the data they produce easily available for use and re-use. However, certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data, in public databases are often not made available, not even for research or innovative activities in the public interest, despite such availability being possible in accordance with the applicable Union law, in particular Regulation (EU) 2016/679 and Directives 2002/58/EC and (EU) 2016/680. Due to the sensitivity of such data, certain technical and legal procedural requirements must be met before they are made available, not least in order to ensure the respect of rights others have over such data or to limit the negative impact on fundamental rights, the principle of non-discrimination and data protection. The fulfilment of such requirements is usually time- and knowledge-intensive. This has led to the insufficient use of such data. While some Member States are establishing structures, processes or legislation to facilitate that type of re-use, this is not the case across the Union. In order to facilitate the use of data for European research and innovation by private and public entities, clear conditions for access to and use of such data are needed across the Union.

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

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

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

([24]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

(7) There are techniques enabling analyses on databases that contain personal data, such as anonymisation, differential privacy, generalisation, suppression and randomisation, the use of synthetic data or similar methods and other state-of-the-art privacy-preserving methods that could contribute to a more privacy-friendly processing of data. Member States should provide support to public sector bodies to make optimal use of such techniques, thus making as much data as possible available for sharing. The application of such techniques, together with comprehensive data protection impact assessments and other safeguards, can contribute to more safety in the use and re-use of personal data and should ensure the safe re-use of commercially confidential business data for research, innovation and statistical purposes. In many cases the application of such techniques, impact assessments and other safeguards implies that data can be used and re-used only in a secure processing environment that is provided or controlled by the public sector body. There is experience at Union level with such secure processing environments that are used for research on statistical microdata on the basis of Commission Regulation (EU) No 557/2013 ([25]). In general, insofar as personal data are concerned, the processing of personal data should be based upon one or more of the legal bases for processing provided in Articles 6 and 9 of Regulation (EU) 2016/679.

(8) In accordance with Regulation (EU) 2016/679, the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Re-identification of data subjects from anonymised datasets should be prohibited. This should not prejudice the possibility to conduct research into anonymisation techniques, in particular for the purpose of ensuring information security, improving existing anonymisation techniques and contributing to the overall robustness of anonymisation, undertaken in accordance with Regulation (EU) 2016/679.

(9) In order to facilitate the protection of personal data and confidential data and to speed up the process of making such data available for re-use under this Regulation, Member States should encourage public sector bodies to create and make available data in accordance with the principle of 'open by design and by default' referred to in Article 5(2) of Directive (EU) 2019/1024 and to promote the creation and the procurement of data in formats and structures that facilitate anonymisation in that regard.

(10) The categories of data held by public sector bodies which should be subject to re-use under this Regulation fall outside the scope of Directive (EU) 2019/1024 that excludes data which is not accessible due to commercial and statistical confidentiality and data that is included in works or other subject matter over which third parties have intellectual property rights. Commercially confidential data includes data protected by trade secrets, protected know-how and any other information the undue disclosure of which would have an impact on the market position or financial health of the undertaking. This Regulation should apply to personal data that fall outside the scope of Directive (EU) 2019/1024 insofar as the access regime excludes or restricts access to such data for reasons of data protection, privacy and the integrity of the individual, in particular in accordance with data protection rules. The re-use of data, which may contain trade secrets, should take place without prejudice to Directive (EU) 2016/943, which sets out the framework for the lawful acquisition, use or disclosure of trade secrets.

(11) This Regulation should not create an obligation to allow the re-use of data held by public sector bodies. In particular, each Member State should therefore be able to decide whether data is made accessible for re-use, also in terms of the purposes and scope of such access. This Regulation should complement and be without prejudice to more specific obligations on public sector bodies to allow re-use of data laid down in sector-specific Union or national law. Public access to official documents may be considered to be in the public interest. Taking into account the role of public access to official documents and transparency in a democratic society, this Regulation should also be without prejudice to Union or national law on granting access to and disclosing official documents. Access to official documents may in particular be granted in accordance with national law without imposing specific conditions or by imposing specific conditions that are not provided by this Regulation.

([25]) Commission Regulation (EU) No 557/2013 of 17 June 2013 implementing Regulation (EC) No 223/2009 of the European Parliament and of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No 831/2002 (OJ L 164, 18.6.2013, p. 16).

(12) The re-use regime provided for in this Regulation should apply to data the supply of which forms part of the public tasks of the public sector bodies concerned under law or other binding rules in the Member States. In the absence of such rules, the public tasks should be defined in accordance with common administrative practice in the Member States, provided that the scope of the public tasks is transparent and subject to review. The public tasks could be defined generally or on a case-by-case basis for individual public sector bodies. As public undertakings are not covered by the definition of public sector body, the data held by public undertakings should not be covered by this Regulation. Data held by cultural establishments, such as libraries, archives and museums as well as orchestras, operas, ballets and theatres, and by educational establishments should not be covered by this Regulation since the works and other documents they hold are predominantly covered by third party intellectual property rights. Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law.

This Regulation should apply to such hybrid organisations only in their capacity as research-performing organisations. If a research-performing organisation holds data as a part of a specific public-private association with private sector organisations or other public sector bodies, bodies governed by public law or hybrid research-performing organisations, i.e. organised as either public sector bodies or public undertakings, with the main purpose of pursuing research, those data should also not be covered by this Regulation. Where relevant, Member States should be able to apply this Regulation to public undertakings or private undertakings that exercise public sector duties or provide services of general interest. The exchange of data, purely in pursuit of their public tasks, among public sector bodies in the Union or between public sector bodies in the Union and public sector bodies in third countries or international organisations, as well as the exchange of data between researchers for non-commercial scientific research purposes, should not be subject to the provisions of this Regulation concerning the re-use of certain categories of protected data held by public sector bodies.

(13) Public sector bodies should comply with competition law when establishing the principles for re-use of data they hold, avoiding the conclusion of agreements which might have as their objective or effect the creation of exclusive rights for the re-use of certain data. Such agreements should be possible only where justified and necessary for the provision of a service or the supply of a product in the general interest. This may be the case where the exclusive use of the data is the only way to maximise the societal benefits of the data in question, for example where there is only one entity (which has specialised in the processing of a specific dataset) capable of providing the service or supplying the product which allows the public sector body to provide a service or supply a product in the general interest. Such arrangements should, however, be concluded in accordance with applicable Union or national law and be subject to regular review based on a market analysis in order to ascertain whether such exclusivity continues to be necessary. In addition, such arrangements should comply with the relevant State aid rules, as appropriate, and should be concluded for a limited duration which should not exceed 12 months. In order to ensure transparency, such exclusive agreements should be published online, in a form that complies with relevant Union law on public procurement. Where an exclusive right to re-use data does not comply with this Regulation, that exclusive right should be invalid.

(14) Prohibited exclusive agreements and other practices or arrangements pertaining to the re-use of data held by public sector bodies which do not expressly grant exclusive rights but which can reasonably be expected to restrict the availability of data for re-use that have been concluded or were already in place before the date of entry into force of this Regulation should not be renewed after the expiry of their term. In the case of indefinite or longer-term agreements, they should be terminated within 30 months of the date of entry into force of this Regulation.

(15) This Regulation should lay down conditions for re-use of protected data that apply to public sector bodies designated as competent under national law to grant or refuse access for re-use, and which are without prejudice to rights or obligations concerning access to such data. Those conditions should be non-discriminatory, transparent, proportionate and objectively justified, while not restricting competition, with a specific focus on promoting access to such data by SMEs and start-ups. The conditions for re-use should be designed in a manner promoting scientific research so that, for example, privileging scientific research should, as a rule, be considered to be non-discriminatory. Public sector bodies allowing re-use should have in place the technical means necessary to ensure the protection of rights and interests of third parties and should be empowered to request the necessary information from the re-user. Conditions attached to the re-use of data should be limited to what is necessary to preserve the rights and interests of third parties in the data and the integrity of the information technology and communication systems of the public sector bodies. Public sector bodies should apply conditions which best serve the interests of the re-user without leading to a disproportionate burden on the public sector bodies. Conditions

attached to the re-use of data should be designed to ensure effective safeguards with regard to the protection of personal data. Before transmission, personal data should be anonymised, in order not to allow the identification of the data subjects, and data containing commercially confidential information should be modified in such a way that no confidential information is disclosed. Where the provision of anonymised or modified data would not respond to the needs of the re-user, subject to fulfilling any requirements to carry out a data protection impact assessment and consult the supervisory authority pursuant to Articles 35 and 36 of Regulation (EU) 2016/679 and where the risks to the rights and interests of data subjects have been found to be minimal, on-premise or remote re-use of the data within a secure processing environment could be allowed.

This could be a suitable arrangement for the re-use of pseudonymised data. Data analyses in such secure processing environments should be supervised by the public sector body, so as to protect the rights and interests of third parties. In particular, personal data should be transmitted to a third party for re-use only where a legal basis under data protection law allows such transmission. Non-personal data should be transmitted only where there is no reason to believe that the combination of non-personal data sets would lead to the identification of data subjects. This should also apply to pseudonymised data which retain their status as personal data. In the event of the reidentification of data subjects, an obligation to notify such a data breach to the public sector body should apply in addition to an obligation to notify such a data breach to a supervisory authority and to the data subject in accordance with Regulation (EU) 2016/679. Where relevant, the public sector bodies should facilitate the re-use of data on the basis of the consent of data subjects or the permission of data holders on the re-use of data pertaining to them through adequate technical means. In that respect, the public sector body should make best efforts to provide assistance to potential re-users in seeking such consent or permission by establishing technical mechanisms that permit transmitting requests for consent or permission from re-users, where practically feasible. No contact information should be given that allows re-users to contact data subjects or data holders directly. Where the public sector body transmits a request for consent or permission, it should ensure that the data subject or data holder is clearly informed of the possibility to refuse consent or permission.

(16) In order to facilitate and encourage the use of data held by public sector bodies for the purposes of scientific research, public sector bodies are encouraged to develop a harmonised approach and harmonised processes to make that data easily accessible for the purposes of scientific research in the public interest. That could mean, *inter alia*, creating streamlined administrative procedures, standardised data formatting, informative metadata on the methodological and data collection choices and standardised data fields that enable the easy joining of data sets from different public sector data sources where relevant for the purposes of analysis. The objective of those practices should be to promote the publicly funded and produced data for the purposes of scientific research in accordance with the principle of 'as open as possible, as closed as necessary'.

(17) The intellectual property rights of third parties should not be affected by this Regulation. This Regulation should neither affect the existence or ownership of intellectual property rights of public sector bodies nor limit the exercise of those rights in any way. The obligations imposed in accordance with this Regulation should apply only insofar as they are compatible with 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), and Union or national intellectual property law. Public sector bodies should, however, exercise their copyright in a way that facilitates re-use.

(18) Data subject to intellectual property rights as well as trade secrets should be transmitted to a third party only where such transmission is lawful by virtue of Union or national law or with the agreement of the rights holder. Where public sector bodies are holders of the right of the maker of a database provided for in Article 7(1) of Directive 96/9/EC of the European Parliament and of the Council ([26]) they should not exercise that right in order to prevent the re-use of data or to restrict re-use beyond the limits set by this Regulation.

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

(19) Undertakings and data subjects should be able to have confidence in the fact that the re-use of certain categories of protected data which are held by the public sector bodies will take place in a manner that respects their rights and interests. Additional safeguards should therefore be put in place for situations in which the re-use of such public sector data takes place on the basis of a processing of the data outside the public sector, such as a requirement that public sector bodies ensure that the rights and interests of natural and legal persons are fully protected, in particular with regard to personal data, commercially sensitive data and intellectual property rights, in all cases, including where such data is transferred to third countries. Public sector bodies should not allow the re-use of information stored in e-health applications by insurance undertakings or any other service provider for the purpose of discriminating in the setting of prices, as this would run counter to the fundamental right of access to health.

(20) Furthermore, in order to preserve fair competition and the open market economy it is of the utmost importance to safeguard protected data of non-personal nature, in particular trade secrets, but also non-personal data representing content protected by intellectual property rights from unlawful access that may lead to intellectual property theft or industrial espionage. In order to ensure the protection of the rights or interests of data holders, it should be possible to transfer non-personal data which is to be protected from unlawful or unauthorised access in accordance with Union or national law and which is held by public sector bodies to third countries, but only where appropriate safeguards for the use of data are provided. Such appropriate safeguards should include a requirement that the public sector body transmit protected data to a re-user only if that re-user makes contractual commitments in the interest of the protection of the data. A re-user that intends to transfer the protected data to a third country should comply with the obligations laid down in this Regulation even after the data has been transferred to the third country. To ensure the proper enforcement of such obligations, the re-user should also accept the jurisdiction of the Member State of the public sector body that allowed the re-use for the judicial settlement of disputes.

(21) Appropriate safeguards should also be considered to be implemented where, in the third country to which non-personal data is being transferred, there are equivalent measures in place which ensure that data benefit from a level of protection similar to that applicable by means of Union law, in particular with regard to the protection of trade secrets and intellectual property rights. To that end, the Commission should be able to declare, by means of implementing acts, where justified because of the substantial number of requests across the Union concerning the re-use of non-personal data in specific third countries, that a third country provides a level of protection that is essentially equivalent to that provided by Union law. The Commission should assess the necessity of such implementing acts on the basis of information provided by the Member States through the European Data Innovation Board. Such implementing acts would reassure public sector bodies that re-use of data held by public sector bodies in the third country concerned would not compromise the protected nature of that data. The assessment of the level of protection afforded in the third country concerned should, in particular, take into consideration the relevant general and sectoral law, including on public security, defence, national security and criminal law, concerning access to and protection of non-personal data, any access by the public sector bodies of that third country to the data transferred, the existence and effective functioning of one or more independent supervisory authorities in the third country with responsibility for ensuring and enforcing compliance with the legal regime ensuring access to such data, the third country's international commitments regarding the protection of data, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems.

The existence of effective legal remedies for data holders, public sector bodies or data intermediation services providers in the third country concerned is of particular importance in the context of the transfer of non-personal data to that third country. Such safeguards should therefore include the availability of enforceable rights and of effective legal remedies. Such implementing acts should be without prejudice to any legal obligation or contractual arrangements already undertaken by a re-user in the interest of the protection of non-personal data, in particular industrial data, and to the right of public sector bodies to oblige re-users to comply with conditions for re-use, in accordance with this Regulation.

(22) Some third countries adopt laws, regulations and other legal acts which aim to directly transfer or provide governmental access to non-personal data in the Union under the control of natural and legal persons under the jurisdiction of the Member States. Decisions and judgments of third-country courts or tribunals or decisions of third-country administrative authorities requiring such transfer of or access to non-personal data should be enforceable where they are based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. In some cases, situations may arise where

the obligation to transfer or provide access to non-personal data arising from a third country law conflicts with a competing obligation to protect such data under Union or national law, in particular with regard to the protection of the fundamental rights of the individual or of the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data and the protection of intellectual property rights, including contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, the transfer of or access to non-personal data should be allowed only if, in particular, it has been verified that the third-country's legal system requires the reasons and proportionality of the decision or judgment to be set out, that the decision or judgment is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal, which is empowered to take duly into account the relevant legal interests of the provider of such data.

Moreover, public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation services providers and recognised data altruism organisations should ensure, where they sign contractual agreements with other private parties, that non-personal data held in the Union are accessed in or transferred to third countries only in accordance with Union law or the national law of the relevant Member State.

(23) To foster further trust in the data economy of the Union, it is essential that the safeguards in relation to Union citizens, the public sector and undertakings that ensure control over their strategic and sensitive data are implemented and that Union law, values and standards are upheld in terms of, but not limited to, security, data protection and consumer protection. In order to prevent unlawful access to non-personal data, public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation services providers and recognised data altruism organisations should take all reasonable measures to prevent access to the systems where non-personal data is stored, including encryption of data or corporate policies. To that end, it should be ensured that public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation services providers and recognised data altruism organisations adhere to all relevant technical standards, codes of conduct and certifications at Union level.

(24) In order to build trust in re-use mechanisms, it may be necessary to attach stricter conditions for certain types of non-personal data that may be identified as highly sensitive in future specific Union legislative acts, with regard to the transfer to third countries, if such transfer could jeopardise Union public policy objectives, in line with international commitments. For example, in the health domain, certain datasets held by actors in the public health system, such as public hospitals, could be identified as highly sensitive health data. Other relevant sectors include transport, energy, environment and finance. In order to ensure harmonised practices across the Union, such types of highly sensitive non-personal public data should be defined by Union law, for example in the context of the European health data space or other sectoral law. Those conditions attached to the transfer of such data to third countries should be laid down in delegated acts. Conditions should be proportionate, non-discriminatory and necessary to protect legitimate Union public policy objectives identified, such as the protection of public health, safety, the environment, public morality, consumer protection, privacy and personal data protection. The conditions should correspond to the risks identified in relation to the sensitivity of such data, including in terms of the risk of the re-identification of individuals. Such conditions could include terms applicable for the transfer or technical arrangements, such as the requirement to use a secure processing environment, 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 to access the data in the third country. In exceptional cases such conditions could also include restrictions to the transfer of the data to third countries to protect the public interest.

(25) Public sector bodies should be able to charge fees for the re-use of data but should also be able to allow re-use at a discounted fee or free of charge, for example for certain categories of re-use such as non-commercial re-use for scientific research purposes, or re-use by SMEs and start-ups, civil society and educational establishments, so as to provide incentives for such re-use in order to stimulate research and innovation and support undertakings that are an important source of innovation and typically find it more difficult to collect relevant data themselves, in accordance with State aid rules. In that specific context, scientific research purposes should be understood to include any type of research-related purpose regardless of the organisational or financial structure of the research institution in question, with the exception of research that is being conducted by an undertaking with the aim of

developing, enhancing or optimising products or services. Such fees should be transparent, non-discriminatory and limited to the necessary costs incurred and should not restrict competition. A list of categories of re-users to which a discounted fee or no charge applies, together with the criteria used to establish that list, should be made public.

(26) In order to provide incentives for the re-use of specific categories of data held by public sector bodies, Member States should establish a single information point to act as an interface for re-users that seek to re-use that data. It should have a cross-sector remit, and should complement, if necessary, arrangements at the sectoral level. The single information point should be able to rely on automated means where it transmits enquiries or requests for re-use. Sufficient human oversight should be ensured in the transmission process. For that purpose existing practical arrangements such as open data portals could be used. The single information point should have an asset list containing an overview of all available data resources including, where relevant, those data resources that are available at sectoral, regional or local information points, with relevant information describing the available data. In addition, Member States should designate, establish or facilitate the establishment of competent bodies to support the activities of public sector bodies allowing re-use of certain categories of protected data. Their tasks may include granting access to data, where mandated under sectoral Union or national law. Those competent bodies should provide assistance to public sector bodies with state-of-the-art techniques, including on how to best structure and store data to make data easily accessible, in particular through application programming interfaces, as well as make data interoperable, transferable and searchable, taking into account best practices for data processing, as well as any existing regulatory and technical standards and secure data processing environments, which allow data analysis in a manner that preserves the privacy of the information.

The competent bodies should act in accordance with the instructions received from the public sector body. Such an assistance structure could assist the data subjects and data holders with management of the consent or permission for re-use, including consent and permission to certain areas of scientific research where in keeping with recognised ethical standards for scientific research. The competent bodies should not have a supervisory function, which is reserved for supervisory authorities under Regulation (EU) 2016/679. Without prejudice to the supervisory powers of data protection authorities, data processing should be carried out under the responsibility of the public sector body responsible for the register containing the data, which remains a data controller as defined in Regulation (EU) 2016/679 insofar as personal data are concerned. Member States should be able to have one or more competent bodies, which could act in different sectors. The internal services of public sector bodies could also act as competent bodies. A competent body could be a public sector body assisting other public sector bodies in allowing re-use of data, where relevant, or a public sector body allowing re-use itself. Assisting other public sector bodies should entail informing them, upon request, about best practices on how to fulfil the requirements laid down in this Regulation such as the technical means to make a secure processing environment available or the technical means to ensure privacy and confidentiality where access to re-use of data within the scope of this Regulation is provided.

(27) Data intermediation services are expected to play a key role in the data economy, in particular in supporting and promoting voluntary data sharing practices between undertakings or facilitating data sharing in the context of obligations set by Union or national law. They could become a tool to facilitate the exchange of substantial amounts of relevant data. Data intermediation services providers, which may include public sector bodies, that offer services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediation services that are independent from data subjects, data holders and data users could have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power, while allowing non-discriminatory access to the data economy for undertakings of all sizes, in particular SMEs and start-ups with limited financial, legal or administrative means. This will be particularly important in the context of the establishment of common European data spaces, namely purpose- or sector-specific or cross-sectoral interoperable frameworks of 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. Data intermediation services could include bilateral or multilateral sharing of data or the creation of platforms or databases enabling the sharing or joint use of data, as well as the establishment of specific infrastructure for the interconnection of data subjects and data holders with data users.

(28) This Regulation should cover services which aim to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data. Where undertakings or other entities offer multiple data-related services, only the activities which directly concern the provision of data intermediation services should be covered by this Regulation. The provision of cloud storage, analytics, data sharing software, web browsers, browser plug-ins or email services should not be considered to be data intermediation services within the meaning of this Regulation, provided that such services only provide technical tools for data subjects or data holders to share data with others, but the provision of such tools neither aims to establish a commercial relationship between data holders and data users nor allows the data intermediation services provider to acquire information on the establishment of commercial relationships for the purposes of data sharing. Examples of data intermediation services include data marketplaces on which undertakings could make data available to others, orchestrators of data sharing ecosystems that are open to all interested parties, for instance in the context of common European data spaces, as well as data pools established jointly by several legal or natural persons with the intention to license the use of such data pools to all interested parties in a manner that all participants that contribute to the data pools would receive a reward for their contribution.

This would exclude services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users. This would also exclude services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things.

(29) Services that focus on the intermediation of copyright-protected content, such as online content-sharing service providers as defined in Article 2, point (6), of Directive (EU) 2019/790, should not be covered by this Regulation. Consolidated tape providers as defined in Article 2(1), point (35), of Regulation (EU) No 600/2014 of the European Parliament and of the Council ([27]) and account information service providers as defined in Article 4, point (19), of Directive (EU) 2015/2366 of the European Parliament and of the Council ([28]) should not be considered to be data intermediation services providers for the purposes of this Regulation. This Regulation should not apply to services offered by public sector bodies in order to facilitate either the re-use of protected data held by public sector bodies in accordance with this Regulation or the use of any other data, insofar as those services do not aim to establish commercial relationships. Data altruism organisations regulated by this Regulation should not be considered to be offering data intermediation services provided that those services do not establish a commercial relationship between potential data users, on the one hand, and data subjects and data holders who make data available for altruistic purposes, on the other. Other services that do not aim to establish commercial relationships, such as repositories that aim to enable the re-use of scientific research data in accordance with open access principles should not be considered to be data intermediation services within the meaning of this Regulation.

(30) A specific category of data intermediation services includes providers of services that offer their services to data subjects. Such data intermediation services providers seek to enhance the agency of data subjects, and in particular individuals' control over data relating to them. Such providers would assist individuals in exercising their rights under Regulation (EU) 2016/679, in particular giving and withdrawing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, the right of erasure or right 'to be forgotten', the right to restrict processing and the right to data portability, which allows data subjects to move their personal data from one data controller to the other. In that context, it is important that the business model of such providers ensures that there are no misaligned incentives that encourage individuals to use such services to make more data relating to them available for processing than would be in their interest. This could include advising individuals on the possible uses of their data and making due diligence checks on data users before allowing them to contact data subjects, in order to avoid fraudulent practices. In certain situations, it could be desirable to collate actual data within a personal data space so that processing can happen within that space without personal data being transmitted to third parties in order to maximise the protection of personal data and privacy. Such personal

([27]) Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

([28]) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

data spaces could contain static personal data such as name, address or date of birth as well as dynamic data that an individual generates through, for example, the use of an online service or an object connected to the Internet of Things. They could also be used to store verified identity information such as passport numbers or social security information, as well as credentials such as driving licences, diplomas or bank account information.

(31) Data cooperatives seek to achieve a number of objectives, in particular to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use in a manner that gives better choices to the individual members of the group or potentially finding solutions to conflicting positions of individual members of a group on how data can be used where such data relates to several data subjects within that group. In that context it is important to acknowledge that the rights under Regulation (EU) 2016/679 are personal rights of the data subject and that data subjects cannot waive such rights. Data cooperatives could also provide a useful means for one-person undertakings and SMEs which, in terms of knowledge of data sharing, are often comparable to individuals.

(32) In order to increase trust in such data intermediation services, in particular related to the use of data and compliance with the conditions imposed by data subjects and data holders, it is necessary to create a Union-level regulatory framework which establishes highly harmonised requirements related to the trustworthy provision of such data intermediation services, and which is implemented by the competent authorities. That framework will contribute to ensuring that data subjects and data holders, as well as data users, have better control over access to and use of their data, in accordance with Union law. The Commission could also encourage and facilitate the development of codes of conduct at Union level, involving relevant stakeholders, in particular on interoperability. Both in situations where data sharing occurs in a business-to-business context and where it occurs in a business-to-consumer context, data intermediation services providers should offer a novel, 'European' way of data governance, by providing a separation in the data economy between data provision, intermediation and use. Data intermediation services providers could also make available specific technical infrastructure for the interconnection of data subjects and data holders with data users. In that regard, it is of particular importance to shape that infrastructure in such a way that SMEs and start-ups encounter no technical or other barriers to their participation in the data economy.

Data intermediation services providers should be allowed to offer additional specific 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, anonymisation and pseudonymisation. Those tools and services should be used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context should not use data for other purposes. At the same time, data intermediation services providers should be allowed to adapt the data exchanged in order to improve the usability of the data by the data user where the data user so desires, or to improve interoperability by, for example, converting the data into specific formats.

(33) It is important to enable a competitive environment for data sharing. A key element by which to increase the trust and control of data holders, data subjects and data users in data intermediation services is the neutrality of data intermediation services providers with regard to the data exchanged between data holders or data subjects and data users. It is therefore necessary that data intermediation services providers act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose. The commercial terms, including pricing, for the provision of data intermediation services should not be dependent on whether a potential data holder or data user is using other services, including storage, analytics, artificial intelligence or other data-based applications, provided by the same data intermediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services. This will also require structural separation between the data intermediation service and any other services provided, so as to avoid conflicts of interest. This means that the data intermediation service should be provided through a legal person that is separate from the other activities of that data intermediation services provider. However, the data intermediation services providers should be able to use the data provided by the data holder for the improvement of their data intermediation services.

Data intermediation services providers should be able to put at the disposal of data holders, data subjects or data users their own or third-party tools for the purpose of facilitating the exchange of data, for example tools for the conversion or curation of data only at the explicit request or approval of the data subject or data holder. The third-party tools offered in that context should not use data for purposes other than those related to data intermediation services. Data intermediation services providers that intermediate the exchange of data between individuals as data

subjects and legal persons as data users should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data subjects. Questions of liability for all material and immaterial damage and detriment resulting from any conduct of the data intermediation services provider could be addressed in the relevant contract, on the basis of national liability regimes.

(34) Data intermediation services providers should take reasonable measures to ensure interoperability within a sector and between different sectors to ensure the proper functioning of the internal market. Reasonable measures could include following the existing, commonly-used standards in the sector where the data intermediation services providers operate. The European Data Innovation Board should facilitate the emergence of additional industry standards, where necessary. Data intermediation services providers should implement in due time the measures for interoperability between the data intermediation services adopted by the European Data Innovation Board.

(35) This Regulation should be without prejudice to the obligation of data intermediation services providers to comply with Regulation (EU) 2016/679 and the responsibility of supervisory authorities to ensure compliance with that Regulation. Where data intermediation services providers process personal data, this Regulation should not affect the protection of personal data. Where the data intermediation services providers are data controllers or processors as defined in Regulation (EU) 2016/679 they are bound by the rules of that Regulation.

(36) Data intermediation services providers are expected to have in place procedures and measures to impose penalties for fraudulent or abusive practices in relation to parties seeking access through their data intermediation services, including measures such as the exclusion of data users that breach the terms of service or infringe existing law.

(37) Data intermediation services providers should also take measures to ensure compliance with competition law and have procedures in place to that effect. This applies in particular in situations where data sharing enables undertakings to become aware of market strategies of their actual or potential competitors. Competitively sensitive information typically includes information on customer data, future prices, production costs, quantities, turnovers, sales or capacities.

(38) A notification procedure for data intermediation services should be established in order to ensure that data governance within the Union is based on trustworthy exchange of data. The benefits of a trustworthy environment would be best achieved by imposing a number of requirements for the provision of data intermediation services, but without requiring any explicit decision or administrative act by the competent authority for data intermediation services for the provision of such services. The notification procedure should not impose undue obstacles for SMEs, start-ups and civil society organisations and should comply with the principle of non-discrimination.

(39) In order to support effective cross-border provision of services, the data intermediation services provider should be requested to send a notification only to the competent authority for data intermediation services from the Member State where its main establishment is located or where its legal representative is located. Such a notification should not entail more than a mere declaration of the intention to provide such services and should be completed only by providing the information set out in this Regulation. After the relevant notification the data intermediation services provider should be able to start operating in any Member State without further notification obligations.

(40) The notification procedure laid down in this Regulation should be without prejudice to specific additional rules for the provision of data intermediation services applicable by means of sector-specific law.

(41) The main establishment of a data intermediation services provider in the Union should be the place of its central administration in the Union. The main establishment of a data intermediation services provider in the Union should be determined in accordance with objective criteria and should imply the effective and real exercise of management activities. Activities of a data intermediation services provider should comply with the national law of the Member State in which it has its main establishment.

(42) In order to ensure the compliance of data intermediation services providers with this Regulation, they should have their main establishment in the Union. Where a data intermediation services provider not established in the Union offers services within the Union, it should designate a legal representative. The designation of a legal representative in such cases is necessary, given that such data intermediation services providers handle personal data as well as commercially confidential data, which necessitates the close monitoring of the compliance of data intermediation services providers with this Regulation. In order to determine whether such a data intermediation services provider is offering services within the Union, it should be ascertained whether it is apparent that the data intermediation services provider is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the website or of an email address and other contact details of the data intermediation services provider, or the use of a language generally used in the third country where the data intermediation services provider is established, should be considered to be insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that language, or the mentioning of users who are in the Union, could make it apparent that the data intermediation services provider is planning to offer services within the Union.

A designated legal representative should act on behalf of the data intermediation services provider and it should be possible for competent authorities for data intermediation services to address the legal representative in addition to or instead of a data intermediation services provider, including in the case of an infringement, for the purpose of initiating enforcement proceedings against a non-compliant data intermediation services provider not established in the Union. The legal representative should be designated by a written mandate of the data intermediation services provider to act on the latter's behalf with regard to the latter's obligations under this Regulation.

(43) In order to assist data subjects and data holders to easily identify, and thereby increase their trust in, data intermediation services providers recognised in the Union, a common logo recognisable throughout the Union should be established, in addition to the label 'data intermediation services provider recognised in the Union'.

(44) The competent authorities for data intermediation services designated to monitor compliance of data intermediation services providers with the requirements of this Regulation should be chosen on the basis of their capacity and expertise regarding horizontal or sectoral data sharing They should be independent of any data intermediation services provider as well as transparent and impartial in the exercise of their tasks. Member States should notify the Commission of the identity of those competent authorities for data intermediation services. The powers and competences of the competent authorities for data intermediation services should be without prejudice to the powers of the data protection authorities. In particular, for any question requiring an assessment of compliance with Regulation (EU) 2016/679, the competent authority for data intermediation services should seek, where relevant, an opinion or decision of the competent supervisory authority established pursuant to that Regulation.

(45) There is a strong potential for objectives of general interest in the use of data made available voluntarily by data subjects on the basis of their informed consent or, where it concerns non-personal data, made available by data holders. Such objectives would include healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, or public policy making. Support to scientific research should also be considered to be an objective of general interest. This Regulation should aim to contribute to the emergence of sufficiently-sized data pools made available on the basis of data altruism in order to enable data analytics and machine learning, including across the Union. In order to achieve that objective, Member States should be able to have in place organisational or technical arrangements, or both, which would facilitate data altruism. Such arrangements could include the availability of easily useable tools for data subjects or data holders for giving consent or permission for the altruistic use of their data, the organisation of awareness campaigns, or a structured exchange between competent authorities on how public policies, such as improving traffic, public health and combating climate change, benefit from data altruism. To that end, Member States should be able to establish national policies for data altruism. Data subjects should be able to receive compensation related only to the costs they incur when making their data available for objectives of general interest.

(46) The registration of recognised data altruism organisations and use of the label 'data altruism organisation recognised in the Union' is expected to lead to the establishment of data repositories. Registration in a Member State would be valid across the Union and is expected to facilitate cross-border data use within the Union and the emergence of data pools covering several Member States. Data holders could give permission to the processing of their non-personal data for a range of purposes not established at the moment of giving the permission. The compliance of

such recognised data altruism organisations with a set of requirements as laid down in this Regulation should bring trust that the data made available for altruistic purposes is serving an objective of general interest. Such trust should result in particular from having a place of establishment or a legal representative within the Union, as well as from the requirement that recognised data altruism organisations are not-for-profit organisations, from transparency requirements and from specific safeguards in place to protect rights and interests of data subjects and undertakings.

Further safeguards should include making it possible to process relevant data within a secure processing environment operated by the recognised data altruism organisations, oversight mechanisms such as ethics councils or boards, including representatives from civil society to ensure that the data controller maintains high standards of scientific ethics and protection of fundamental rights, effective and clearly communicated technical means to withdraw or modify consent at any moment, on the basis of the information obligations of data processors under Regulation (EU) 2016/679, as well as means for data subjects to stay informed about the use of data they made available. Registration as a recognised data altruism organisation should not be a precondition for exercising data altruism activities. The Commission should, by means of delegated acts, prepare a rulebook in close cooperation with data altruism organisations and relevant stakeholders. Compliance with that rulebook should be a requirement for registration as a recognised data altruism organisation.

(47) In order to assist data subjects and data holders to easily identify, and thereby to increase their trust in, recognised data altruism organisations, a common logo that is recognisable throughout the Union should be established. The common logo should be accompanied by a QR code with a link to the public Union register of recognised data altruism organisations.

(48) This Regulation should be without prejudice to the establishment, organisation and functioning of entities that seek to engage in data altruism pursuant to national law and build on national law requirements to operate lawfully in a Member State as a not-for-profit organisation.

(49) This Regulation should be without prejudice to the establishment, organisation and functioning of entities other than public sector bodies that engage in the sharing of data and content on the basis of open licenses, thereby contributing to the creation of common resources available to all. This should include open collaborative knowledge sharing platforms, open access scientific and academic repositories, open source software development platforms and open access content aggregation platforms.

(50) Recognised data altruism organisations should be able to collect relevant data directly from natural and legal persons or to process data collected by others. Processing of collected data could be done by data altruism organisations for purposes which they establish themselves or, where relevant, they could allow the processing by third parties for those purposes. Where recognised data altruism organisations are data controllers or processors as defined in Regulation (EU) 2016/679, they should comply with that Regulation. Typically, data altruism would rely on consent of data subjects within the meaning of Article 6(1), point (a), and Article 9(2), point (a), of Regulation (EU) 2016/679 that should be in compliance with requirements for lawful consent in accordance with Articles 7 and 8 of that Regulation. In accordance with Regulation (EU) 2016/679, scientific research purposes could be supported by consent to certain areas of scientific research where in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects. Article 5(1), point (b), of Regulation (EU) 2016/679 specifies that further processing for scientific or historical research purposes or statistical purposes should, in accordance with Article 89(1) of Regulation (EU) 2016/679, not be considered to be incompatible with the initial purposes. For non-personal data the usage limitations should be found in the permission given by the data holder.

(51) The competent authorities for the registration of data altruism organisations designated to monitor compliance of recognised data altruism organisations with the requirements of this Regulation should be chosen on the basis of their capacity and expertise. They should be independent of any data altruism organisation as well as transparent and impartial in the exercise of their tasks. Member States should notify the Commission of the identity of those competent authorities for the registration of data altruism organisations. The powers and competences of the competent authorities for the registration of data altruism organisations should be without prejudice to the powers of the data protection authorities. In particular, for any question requiring an assessment of compliance with Regulation (EU) 2016/679, the competent authority for the registration of data altruism organisations should seek, where relevant, an opinion or decision of the competent supervisory authority established pursuant to that Regulation.

(52) To promote trust and bring additional legal certainty and user-friendliness to the process of granting and withdrawing consent, in particular in the context of scientific research and statistical use of data made available on an altruistic basis, a European data altruism consent form should be developed and used in the context of altruistic data sharing. Such a form should contribute to additional transparency for data subjects that their data will be accessed and used in accordance with their consent and also in full compliance with the data protection rules. It should also facilitate the granting and withdrawing of consent and be used to streamline data altruism carried out by undertakings and provide a mechanism allowing such undertakings to withdraw their permission to use the data. In order to take into account the specificities of individual sectors, including from a data protection perspective, the European data altruism consent form should use a modular approach allowing customisation for specific sectors and for different purposes.

(53) In order to successfully implement the data governance framework, a European Data Innovation Board should be established, in the form of an expert group. The European Data Innovation Board should consist of representatives of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations of all Member States, the European Data Protection Board, the European Data Protection Supervisor, the European Union Agency for Cybersecurity (ENISA), the Commission, the EU SME Envoy or a representative appointed by the network of SME envoys, and other representatives of relevant bodies in specific sectors as well as bodies with specific expertise. The European Data Innovation Board should consist of a number of subgroups, including a subgroup for stakeholder involvement composed of relevant representatives of industry, such as health, environment, agriculture, transport, energy, industrial manufacturing, media, cultural and creative sectors, and statistics, as well as of research, academia, civil society, standardisation organisations, relevant common European data spaces and other relevant stakeholders and third parties, *inter alia* bodies with specific expertise such as national statistical offices.

(54) The European Data Innovation Board should assist the Commission in coordinating national practices and policies on the topics covered by this Regulation, and in supporting cross-sector data use by adhering to the European Interoperability Framework principles and through the use of European and international standards and specifications, including through the EU Multi-Stakeholder Platform for ICT Standardisation, the Core Vocabularies and the CEF Building Blocks, and should take into account standardisation work taking place in specific sectors or domains. Work on technical standardisation could include the identification of priorities for the development of standards and establishing and maintaining a set of technical and legal standards for transmitting data between two processing environments that allows data spaces to be organised, in particular clarifying and distinguishing which standards and practices are cross-sectoral and which are sectoral. The European Data Innovation Board should cooperate with sectoral bodies, networks or expert groups, or other cross-sectoral organisations dealing with the re-use of data. Regarding data altruism, the European Data Innovation Board should assist the Commission in the development of the data altruism consent form, after consulting the European Data Protection Board. By proposing guidelines on common European data spaces, the European Data Innovation Board should support the development of a functioning European data economy on the basis of those data spaces, as set out in the European strategy for data.

(55) Member States should lay down rules on penalties applicable to infringements of this Regulation and should take all measures necessary to ensure that they are implemented. The penalties provided for should be effective, proportionate and dissuasive. Large discrepancies between rules on penalties could lead to distortion of competition in the digital single market. The harmonisation of such rules could be of benefit in that regard.

(56) In order to provide for an efficient enforcement of this Regulation and to ensure that data intermediation services providers and entities that wish to register as recognised data altruism organisations are able to access and complete the procedures of notification and registration fully online and in a cross-border manner, such procedures should be offered through the single digital gateway established pursuant to Regulation (EU) 2018/1724 of the European Parliament and of the Council ([29]). Those procedures should be added to the list of procedures included in Annex II to Regulation (EU) 2018/1724.

(57) Regulation (EU) 2018/1724 should therefore be amended accordingly.

([29]) Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, p. 1).

(58) In order to ensure the effectiveness of this Regulation, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission for the purpose of supplementing this Regulation by laying down special conditions applicable to transfers to third countries of certain non-personal data categories deemed to be highly sensitive in specific Union legislative acts and by establishing a rulebook for recognised data altruism organisations, with which those organisations are to comply, that provides for information, technical and security requirements as well as communication roadmaps and interoperability standards. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([30]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(59) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to assist public sector bodies and re-users in their compliance with conditions for re-use set out in this Regulation by establishing model contractual clauses for the transfer by re-users of non-personal data to a third country, to declare that the legal, supervisory and enforcement arrangements of a third country are equivalent to the protection ensured under Union law, to develop the design of the common logo for data intermediation services providers and of the common logo for recognised data altruism organisations, and to establish and develop the European data altruism consent form. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([31]).

(60) This Regulation should not affect the application of the rules on competition, and in particular Articles 101 and 102 TFEU. The measures provided for in this Regulation should not be used to restrict competition in a manner contrary to the TFEU. This concerns in particular the rules on the exchange of competitively sensitive information between actual or potential competitors through data intermediation services.

(61) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered their opinion on 10 March 2021.

(62) This Regulation uses as its guiding principles the respect for the fundamental rights and principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the right to privacy, the protection of personal data, the freedom to conduct a business, the right to property and the integration of persons with disabilities. In the context of the latter, the public service bodies and services under this Regulation should, where relevant, comply with Directives (EU) 2016/2102 ([32]) and (EU) 2019/882 ([33]) of the European Parliament and of the Council. Furthermore, Design for All in the context of information and communications technology, which is the conscious and systematic effort to proactively apply principles, methods and tools to promote universal design in computer-related technologies, including internet-based technologies, thus avoiding the need for a posteriori adaptations or specialised design, should be taken into account.

(63) Since the objectives of this Regulation, namely the re-use, within the Union, of certain categories of data held by public sector bodies as well as the establishment of a notification and supervisory framework for the provision of data intermediation services, a framework for voluntary registration of entities which make data available for altruistic purposes and a framework for the establishment of a European Data Innovation Board, cannot be sufficiently achieved by the Member States, but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives,

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

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

([32]) Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2.12.2016, p. 1).

([33]) Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

HAVE ADOPTED THIS REGULATION:

*CHAPTER I*

***General provisions***

*Article 1*

**Subject matter and scope**

1. This Regulation lays down:

(a) conditions for the re-use, within the Union, of certain categories of data held by public sector bodies;

(b) a notification and supervisory framework for the provision of data intermediation services;

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

(d) a framework for the establishment of a European Data Innovation Board.

2. This Regulation does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law.

This Regulation is without prejudice to:

(a) specific provisions in Union or national law regarding the access to or re-use of certain categories of data, in particular with regard to the granting of access to and disclosure of official documents; and

(b) the obligations of public sector bodies under Union or national law to allow the re-use of data or to requirements related to processing of non-personal data.

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, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.

3. Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation. In particular, this Regulation is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, including with regard to the powers and competences of supervisory authorities. In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data shall prevail. This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations (EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680.

4. This Regulation is without prejudice to the application of competition law.

5. This Regulation is without prejudice to the competences of the Member States with regard to their activities concerning public security, defence and national security.

*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 audiovisual recording;

(2) 're-use' means the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks;

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

(4) 'non-personal data' means data other than personal data;

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

(6) 'permission' means giving data users the right to the processing of non-personal data;

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

(8) 'data holder' means a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data;

(9) 'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non-commercial purposes;

(10) 'data sharing' means the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge;

(11) 'data intermediation service' means a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following:

   (a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;

   (b) services that focus on the intermediation of copyright-protected content;

   (c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things;

   (d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships;

(12) 'processing' means processing as defined in Article 4, point (2), of Regulation (EU) 2016/679 with regard to personal data or Article 3, point (2), of Regulation (EU) 2018/1807 with regard to non-personal data;

(13) 'access' means data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of data;

(14) 'main establishment' of a legal person means the place of its central administration in the Union;

(15) 'services of data cooperatives' means data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structure, having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data;

(16) '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 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;

(17) 'public sector body' means the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities, or one or more such bodies governed by public law;

(18) 'bodies governed by public law' means bodies that have the following characteristics:

(a) they are established for the specific purpose of meeting needs in the general interest, and do not have 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 other bodies governed by public law, 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;

(19) 'public undertaking' means any undertaking over which the public sector bodies 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; for the purposes of this definition, 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;

(20) 'secure processing environment' means the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, 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;

(21) 'legal representative' means a natural or legal person established in the Union explicitly designated to act on behalf of a data intermediation services provider or an entity that collects data for objectives of general interest made available by natural or legal persons on the basis of data altruism not established in the Union, which may be addressed by the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations in addition to or instead of the data intermediation services provider or entity with regard to the obligations under this Regulation, including with regard to initiating enforcement proceedings against a non-compliant data intermediation services provider or entity not established in the Union.

*CHAPTER II*

***Re-use of certain categories of protected data held by public sector bodies***

*Article 3*

**Categories of data**

1. This Chapter applies to data held by public sector bodies which are protected on 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 Directive (EU) 2019/1024.

2. This Chapter does not apply to:

(a) data held by public undertakings;

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

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

(d) data held by public sector bodies which are protected for reasons of public security, defence or national security; or

(e) data 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 concerned, or, in the absence of such rules, as defined in accordance with common administrative practice in that Member State, provided that the scope of the public tasks is transparent and subject to review.

3. This Chapter is without prejudice to:

(a) Union and national law and international agreements to which the Union or Member States are party on the protection of categories of data referred to in paragraph 1; and

(b) Union and national law on access to documents.

*Article 4*

**Prohibition of exclusive arrangements**

1. Agreements or other practices pertaining to the re-use of data held by public sector bodies containing categories of data referred to in Article 3(1) which grant exclusive rights or which have as their objective or effect to grant such exclusive rights or to restrict the availability of data for re-use by entities other than the parties to such agreements or other practices shall be prohibited.

2. By way of derogation from paragraph 1, an exclusive right to re-use data referred to in that paragraph may be granted to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible.

3. An exclusive right as referred to in paragraph 2 shall be granted through an administrative act or contractual arrangement in accordance with applicable Union or national law and in compliance with the principles of transparency, equal treatment and non-discrimination.

4. 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.

5. The grant of an exclusive right pursuant to paragraphs 2, 3 and 4, including the reasons as to why it is necessary to grant such a right, shall be transparent and be made publicly available online, in a form that complies with relevant Union law on public procurement.

6. Agreements or other practices falling within the scope of the prohibition referred to in paragraph 1 which do not meet the conditions laid down in paragraphs 2 and 3 and which were concluded before 23 June 2022 shall be terminated at the end of the applicable contract and in any event by 24 December 2024.

*Article 5*

**Conditions for re-use**

1. Public sector bodies which are competent under national law to grant or refuse access for the re-use of one or more of the categories of data referred to in Article 3(1) 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 8. Where they grant or refuse access for re-use, they may be assisted by the competent bodies referred to in Article 7(1).

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

2. Conditions for re-use shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed. Those conditions shall not be used to restrict competition.

3. Public sector bodies shall, in accordance with Union and national law, ensure that the protected nature of data is preserved. They may provide for the following requirements:

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

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

   (ii) 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 remotely within a secure processing environment that is provided or controlled by the public sector body;

(c) to access and re-use the data 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.

4. In the case of re-use allowed in accordance with paragraph 3, 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. The public sector body shall reserve the right to verify the process, the means and any results of processing of data undertaken by the re-user to preserve the integrity of the protection of the data and 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.

5. Unless national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of data referred to in Article 3(1), the public sector body shall make the re-use of data provided in accordance with paragraph 3 of this Article 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 that the re-user may have acquired despite the safeguards put in place. Re-users shall be prohibited from re-identifying any data subject to whom the data relates and shall take technical and operational measures to prevent re-identification and to notify any data breach resulting in the re-identification of the data subjects concerned to the public sector body. In the event of the unauthorised re-use of non-personal data, the re-user shall, without delay, where appropriate with the assistance of the public sector body, inform the legal persons whose rights and interests may be affected.

6. Where the re-use of data cannot be allowed in accordance with the obligations laid down in paragraphs 3 and 4 of this Article and there is no legal basis for transmitting the data under Regulation (EU) 2016/679, 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 it 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 7(1).

7. Re-use of data shall be allowed only in compliance with intellectual property rights. The right of the maker of a database as 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 or to restrict re-use beyond the limits set by this Regulation.

8. Where data requested is considered to be confidential, in accordance with Union or national law on commercial or statistical confidentiality, the public sector bodies shall ensure that the confidential data is not disclosed as a result of allowing re-use, unless such re-use is allowed in accordance with paragraph 6.

9. Where a re-user intends to transfer non-personal data protected on the grounds set out in Article 3(1) 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 such data. In the case of re-use in accordance with paragraph 6 of this Article, the re-user shall, where appropriate with the assistance of the public sector body, inform the 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 legal person gives permission for the transfer.

10. 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 12 only if the re-user contractually commits to:

(a) complying with the obligations imposed in accordance with paragraphs 7 and 8 even after the data is transferred to the third country; and

(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 paragraphs 7 and 8.

11. 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 10 of this Article.

In order to assist public sector bodies and re-users, the Commission may adopt implementing acts establishing model contractual clauses for complying with the obligations referred to in paragraph 10 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 33(3).

12. 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.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 33(3).

13. 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 32 supplementing this Regulation by laying down special conditions applicable to the transfers of such data to third countries.

Those special conditions shall be based on the nature of the non-personal data categories identified in the specific Union legislative act and on the grounds for deeming those categories to be highly sensitive, taking into account the risks of re-identification of non-personal, anonymised data. They shall be non-discriminatory and limited to what is necessary to achieve the Union public policy objectives identified in that act, in accordance with the Union's international obligations.

If required by specific Union legislative acts as 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.

14. The natural or legal person to which the right to re-use non-personal data was granted may transfer the data only to those third countries for which the requirements in paragraphs 10, 12 and 13 are met.

*Article 6*

**Fees**

1. Public sector bodies which allow re-use of the categories of data referred to in Article 3(1) may charge fees for allowing the re-use of such data.

2. Any fees charged pursuant to paragraph 1 shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition.

3. Public sector bodies shall ensure that any fees 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.

4. Where public sector bodies charge fees, they shall take measures to provide incentives for the re-use of the categories of data referred to in Article 3(1) for non-commercial purposes, such as scientific research purposes, and by SMEs and start-ups in accordance with 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 SMEs and start-ups, civil society and educational establishments. To that end, public sector bodies may establish a list of categories of re-users to which data 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.

5. Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of the categories of data referred to in Article 3(1) 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 5(3);

(d) the maintenance of the secure processing environment;

(e) the acquisition of the right to allow re-use in accordance with this Chapter by third parties outside the public sector; and

(f) 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.

6. 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.

*Article 7*

**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, which may be competent for particular sectors, to assist the public sector bodies which grant or refuse access for the re-use of the categories of data referred to in Article 3(1). 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 Regulation.

2. The competent bodies may be empowered to grant access for the re-use of the categories of data referred to in Article 3(1) pursuant to Union or national law which provides for such access to be granted. Where they grant or refuse access for the re-use, Articles 4, 5, 6 and 9 shall apply to those competent bodies.

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 data referred to in Article 3(1).

4. The assistance provided for 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;

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

(c) providing technical support for pseudonymisation and ensuring data processing in a manner that effectively preserves the privacy, confidentiality, integrity and accessibility of the information contained in the data for which re-use is allowed, including techniques for the anonymisation, generalisation, suppression and randomisation of personal data or other state-of-the-art privacy-preserving methods, and the deletion of 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 5(10).

5. Each Member State shall notify the Commission of the identity of the competent bodies designated pursuant to paragraph 1 by 24 September 2023. Each Member State shall also notify the Commission of any subsequent change to the identity of those competent bodies.

*Article 8*

**Single information points**

1. Member States shall ensure that all relevant information concerning the application of Articles 5 and 6 is available and easily accessible through a single information point. Member States shall establish a new body or designate an existing body or structure as the single information point. The single information point may be linked to sectoral, regional or local information points. The functions of the single information point may be automated provided that the public sector body ensures adequate support.

2. The single information point shall be competent to receive enquiries or requests for the re-use of the categories of data referred to in Article 3(1) and shall transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies referred to in Article 7(1), where relevant. The single information point shall make available by electronic means a searchable asset list containing an overview of all available data resources including, where relevant, those data resources that are available at sectoral, regional or local information points, with relevant information describing the available data, including at least the data format and size and the conditions for their re-use.

3. The single information point may establish a separate, simplified and well-documented information channel for SMEs and start-ups, addressing their needs and capabilities in requesting the re-use of the categories of data referred to in Article 3(1).

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

*Article 9*

**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 Article 7(1) shall adopt a decision on the request for the re-use of the categories of data referred to in Article 3(1) within two months of the date of receipt of the request.

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 Article 7(1) shall notify the applicant as soon as possible that more time is needed for conducting the procedure, together with the reasons for the delay.

2. 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 III*

***Requirements applicable to data intermediation services***

*Article 10*

**Data intermediation services**

The provision of the following data intermediation services shall comply with Article 12 and shall be subject to a notification procedure:

(a) intermediation services between data holders and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders with data users;

(b) intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users, including making available the technical or other means to enable such services, and in particular enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679;

(c) services of data cooperatives.

*Article 11*

**Notification by data intermediation services providers**

1. Any data intermediation services provider who intends to provide the data intermediation services referred to in Article 10 shall submit a notification to the competent authority for data intermediation services.

2. For the purposes of this Regulation, a data intermediation services provider with establishments in more than one Member State shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment, without prejudice to Union law regulating cross-border actions for damages and related proceedings.

3. A data intermediation services provider that is not established in the Union, but which offers the data intermediation services referred to in Article 10 within the Union, shall designate a legal representative in one of the Member States in which those services are offered.

For the purpose of ensuring compliance with this Regulation, the legal representative shall be mandated by the data intermediation services provider to be addressed in addition to or instead of it by competent authorities for data intermediation services or data subjects and data holders, with regard to all issues related to the data intermediation services provided. The legal representative shall cooperate with and comprehensively demonstrate to the competent authorities for data intermediation services, upon request, the actions taken and provisions put in place by the data intermediation services provider to ensure compliance with this Regulation.

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

4. After having submitted a notification in accordance with paragraph 1, the data intermediation services provider may start the activity subject to the conditions laid down in this Chapter.

5. The notification referred to in paragraph 1 shall entitle the data intermediation services provider to provide data intermediation services in all Member States.

6. The notification referred to in paragraph 1 shall include the following information:

(a) the name of the data intermediation services provider;

(b) the data intermediation services provider's legal status, form, ownership structure, relevant subsidiaries and, where the data intermediation services provider is registered in a trade or other similar public national register, registration number;

(c) the address of the data intermediation services provider's main establishment in the Union, if any, and, where applicable, of any secondary branch in another Member State or that of the legal representative;

(d) a public website where complete and up-to-date information on the data intermediation services provider and the activities can be found, including as a minimum the information referred to in points (a), (b), (c) and (f);

(e) the data intermediation services provider's contact persons and contact details;

(f) a description of the data intermediation service the data intermediation services provider intends to provide, and an indication of the categories listed in Article 10 under which such data intermediation service falls;

(g) the estimated date for starting the activity, if different from the date of the notification.

7. The competent authority for data intermediation services shall ensure that the notification procedure is non-discriminatory and does not distort the competition.

8. At the request of the data intermediation services provider, the competent authority for data intermediation services shall, within one week of a duly and fully completed notification, issue a standardised declaration, confirming that the data intermediation services provider has submitted the notification referred to in paragraph 1 and that the notification contains the information referred to in paragraph 6.

9. At the request of the data intermediation services provider, the competent authority for data intermediation services shall confirm that the data intermediation services provider complies with this Article and Article 12. Upon receipt of such a confirmation, that data intermediation services provider may use the label 'data intermediation services provider recognised in the Union' in its written and spoken communication, as well as a common logo.

In order to ensure that data intermediation services providers recognised in the Union are easily identifiable throughout the Union, the Commission shall, by means of implementing acts, establish a design for the common logo. Data intermediation services providers recognised in the Union shall display the common logo clearly on every online and offline publication that relates to their data intermediation activities.

Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 33(2).

10. The competent authority for data intermediation services shall notify the Commission of each new notification by electronic means without delay. The Commission shall keep and regularly update a public register of all data intermediation services providers providing their services in the Union. The information referred to in paragraph 6, points (a), (b), (c), (d), (f) and (g), shall be published in the public register.

11. The competent authority for data intermediation services may charge fees for the notification 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 and other market control activities of the competent authority for data intermediation services in relation to notifications of data intermediation services providers. In the case of SMEs and start-ups, the competent authority for data intermediation services may charge a discounted fee or waive the fee.

12. Data intermediation services providers shall notify the competent authority for data intermediation services of any changes to the information provided pursuant to paragraph 6 within 14 days of the date of the change.

13. Where a data intermediation services provider ceases its activities, it shall notify the relevant competent authority for data intermediation services determined pursuant to paragraphs 1, 2 and 3 within 15 days.

14. The competent authority for data intermediation services shall notify the Commission of each notification referred to in paragraphs 12 and 13 by electronic means without delay. The Commission shall update the public register of the data intermediation services providers in the Union accordingly.

*Article 12*

**Conditions for providing data intermediation services**

The provision of data intermediation services referred in Article 10 shall be subject to the following conditions:

(a) the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person;

(b) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user shall not be dependent upon whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services;

(c) the data collected 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, shall be used only for the development of that data intermediation service, which may entail the use of data for the detection of fraud or cybersecurity, and shall be made available to the data holders upon request;

(d) the data intermediation services provider shall facilitate the exchange of the data in the format in which it receives it from a data subject or a data holder, shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure harmonisation with international or European data standards and shall offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law;

(e) data intermediation services may include offering additional specific 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, anonymisation and pseudonymisation, such tools being used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context not being used for other purposes;

(f) the data intermediation services provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service;

(g) the data intermediation services provider shall have procedures in place to prevent fraudulent or abusive practices in relation to parties seeking access through its data intermediation services;

(h) the data intermediation services provider shall, in the event of its insolvency, ensure a reasonable continuity of the provision of its data intermediation services and, where such data intermediation services ensure the storage of data, shall have mechanisms in place to allow data holders and data users to obtain access to, to transfer or to retrieve their data and, where such data intermediation services are provided between data subjects and data users, to allow data subjects to exercise their rights;

(i) the data intermediation services provider shall take appropriate measures to ensure interoperability with other data intermediation services, *inter alia*, by means of commonly used open standards in the sector in which the data intermediation services provider operates;

(j) the data intermediation services provider shall put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal data that is unlawful under Union law or the national law of the relevant Member State;

(k) the data intermediation services provider shall without delay inform data holders in the event of an unauthorised transfer, access or use of the non-personal data that it has shared;

(l) the data intermediation services provider shall take necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data, and the data intermediation services provider shall further ensure the highest level of security for the storage and transmission of competitively sensitive information;

(m) the data intermediation services provider offering services to data subjects shall act 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;

(n) where a data intermediation services provider provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data;

(o) the data intermediation services provider shall maintain a log record of the data intermediation activity.

*Article 13*

**Competent authorities for data intermediation services**

1. Each Member State shall designate one or more competent authorities to carry out the tasks related to the notification procedure for data intermediation services and shall notify the Commission of the identity of those competent authorities by 24 September 2023. Each Member State shall also notify the Commission of any subsequent change to the identity of those competent authorities.

2. The competent authorities for data intermediation services shall comply with the requirements set out in Article 26.

3. The powers of the competent authorities for data intermediation services are without prejudice to the powers of the data protection authorities, national competition authorities, authorities in charge of cybersecurity and other relevant sectoral authorities. In accordance with their respective competences under Union and national law, those authorities shall establish strong cooperation and exchange information as is necessary for the exercise of their tasks in relation to data intermediation services providers, and shall aim to achieve consistency in the decisions taken in applying this Regulation.

*Article 14*

**Monitoring of compliance**

1. The competent authorities for data intermediation services shall monitor and supervise compliance of data intermediation services providers with the requirements of this Chapter. The competent authorities for data intermediation services may also monitor and supervise the compliance of data intermediation services providers, on the basis of a request by a natural or legal person.

2. The competent authorities for data intermediation services shall have the power to request from data intermediation services providers or their legal representatives all the information that is necessary to verify compliance with the requirements of this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

3. Where the competent authority for data intermediation services finds that a data intermediation services provider does not comply with one or more of the requirements of this Chapter, it shall notify that data intermediation services provider 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 for data intermediation services shall have the power to require the cessation of the infringement referred to in paragraph 3 within a reasonable time limit or immediately in the case of a serious infringement and shall take appropriate and proportionate measures with the aim of ensuring compliance. In that regard, the competent authority for data intermediation services shall have the power, where appropriate:

(a) to impose, through administrative procedures, dissuasive financial penalties, which may include periodic penalties and penalties with retroactive effect, to initiate legal proceedings for the imposition of fines, or both;

(b) to require a postponement of the commencement or a suspension of the provision of the data intermediation service until any changes to the conditions requested by the competent authority for data intermediation services have been made; or

(c) to require the cessation of the provision of the data intermediation service in the event that serious or repeated infringements have not been remedied despite prior notification in accordance with paragraph 3.

The competent authority for data intermediation services shall request the Commission to remove the data intermediation services provider from the register of data intermediation services providers once it has ordered the cessation of the provision of the data intermediation service in accordance with the first subparagraph, point (c).

If a data intermediation services provider remedies infringements, that data intermediation services provider shall re-notify the competent authority for data intermediation services. The competent authority for data intermediation services shall notify the Commission of each new re-notification.

5. Where a data intermediation services provider that is not established in the Union fails to designate a legal representative or the legal representative fails, upon request of the competent authority for data intermediation services, to provide the necessary information that comprehensively demonstrates compliance with this Regulation, the competent authority for data intermediation services shall have the power to postpone the commencement of or to suspend the provision of the data intermediation service until the legal representative is designated or the necessary information is provided.

6. The competent authorities for data intermediation services shall notify the data intermediation services provider concerned of the measures imposed pursuant to paragraphs 4 and 5 and the reasons on which they are based, as well as the necessary steps to be taken to rectify the relevant shortcomings, without delay, and shall stipulate a reasonable period, which shall not be longer than 30 days, for the data intermediation services provider to comply with those measures.

7. If a data intermediation services provider has its main establishment or its legal representative in a Member State but provides services in other Member States, the competent authority for data intermediation services of the Member State of the main establishment or where the legal representative is located and the competent authorities for data intermediation services of those other Member States shall cooperate and assist each other. Such assistance and cooperation may cover information exchanges between the competent authorities for data intermediation services concerned for the purposes of their tasks under this Regulation and reasoned requests to take the measures referred to in this Article.

Where a competent authority for data intermediation services in one Member State requests assistance from a competent authority for data intermediation services in another Member State, it shall submit a reasoned request. The competent authority for data intermediation services shall, upon such a request, provide a response without delay and within a timeframe proportionate to the urgency of the request.

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

*Article 15*

**Exceptions**

This Chapter shall not apply to recognised data altruism organisations or other not-for-profit entities insofar as their activities consist of seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism, unless those organisations and entities aim to establish commercial relationships between an undetermined number of data subjects and data holders on the one hand and data users on the other.

*CHAPTER IV*

***Data altruism***

*Article 16*

**National arrangements for data altruism**

Member States may have in place organisational or technical arrangements, or both, to facilitate data altruism. To that end, Member States may establish national policies for data altruism. Those national policies may, in particular, assist data subjects in making personal data related to them held by public sector bodies available voluntarily for data altruism, and set out the necessary information that is required to be provided to data subjects concerning the re-use of their data in the general interest.

If a Member State develops such national policies, it shall notify the Commission thereof.

*Article 17*

**Public registers of recognised data altruism organisations**

1. Each competent authority for the registration of data altruism organisations shall keep and regularly update a public national register of recognised data altruism organisations.

2. The Commission shall maintain a public Union register of recognised data altruism organisations for information purposes. Provided that an entity is registered in the public national register of recognised data altruism organisations in accordance with Article 18, it may use the label 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as a common logo.

In order to ensure that recognised data altruism organisations are easily identifiable throughout the Union, the Commission shall, by means of implementing acts, establish a design for the common logo. Recognised data altruism organisations shall display the common logo clearly on every online and offline publication that relates to their data altruism activities. The common logo shall be accompanied by a QR code with a link to the public Union register of recognised data altruism organisations.

Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 33(2).

*Article 18*

**General requirements for registration**

In order to qualify for registration in a public national register of recognised data altruism organisations, an entity shall:

(a) carry out data altruism activities;

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

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

(d) carry out its data altruism activities through a structure that is functionally separate from its other activities;

(e) comply with the rulebook referred to Article 22(1), at the latest 18 months after the date of entry into force of the delegated acts referred to in that paragraph.

*Article 19*

**Registration of recognised data altruism organisations**

1. An entity which meets the requirements of Article 18 may submit an application for registration in the public national register of recognised data altruism organisations in the Member State in which it is established.

2. An entity which meets the requirements of Article 18 and has establishments in more than one Member State may submit an application for registration in the public national register of recognised data altruism organisations in the Member State in which it has its main establishment.

3. An entity which meets the requirements of Article 18 but which is not established in the Union shall designate a legal representative in one of the Member States in which the data altruism services are offered.

For the purpose of ensuring compliance with this Regulation, the legal representative shall be mandated by the entity to be addressed in addition to or instead of it by competent authorities for the registration of data altruism organisations or data subjects and data holders, with regard to all issues related to that entity. The legal representative shall cooperate with and comprehensively demonstrate to the competent authorities for the registration of data altruism organisations, upon request, the actions taken and provisions put in place by the entity to ensure compliance with this Regulation.

The entity shall be deemed to be under the jurisdiction of the Member State in which the legal representative is located. Such an entity may submit an application for registration in the public national register of recognised data altruism organisations in that Member State. The designation of a legal representative by the entity shall be without prejudice to any legal actions which could be initiated against the entity.

4. Applications for registration referred to in paragraphs 1, 2 and 3 shall contain the following information:

(a) the name of the entity;

(b) the entity's legal status, form and, where the entity is registered in a public national register, registration number;

(c) the statutes of the entity, where appropriate;

(d) the entity's sources of income;

(e) the address of the entity's main establishment in the Union, if any, and, where applicable, any secondary branch in another Member State or that of the legal representative;

(f) a public website where complete and up-to-date information on the entity and the activities can be found, including as a minimum the information referred to in points (a), (b), (d), (e) and (h);

(g) the entity's contact persons and contact details;

(h) the objectives of general interest it intends to promote when collecting data;

(i) the nature of the data that the entity intends to control or process, and, in the case of personal data, an indication of the categories of personal data;

(j) any other documents which demonstrate that the requirements of Article 18 are met.

5. Where the entity has submitted all necessary information pursuant to paragraph 4 and after the competent authority for the registration of data altruism organisations has evaluated the application for registration and found that the entity complies with the requirements of Article 18, it shall register the entity in the public national register of recognised data altruism organisations within 12 weeks after the receipt of the application for registration. The registration shall be valid in all Member States.

The competent authority for the registration of data altruism organisations shall notify the Commission of any registration. The Commission shall include that registration in the public Union register of recognised data altruism organisations.

6. The information referred to in paragraph 4, points (a), (b), (f), (g) and (h), shall be published in the relevant public national register of recognised data altruism organisations.

7. A recognised data altruism organisation shall notify the relevant competent authority for the registration of data altruism organisations of any changes to the information provided pursuant to paragraph 4 within 14 days of the date of the change.

The competent authority for the registration of data altruism organisations shall notify the Commission of each such notification by electronic means without delay. Based on such a notification, the Commission shall update the public Union register of recognised data altruism organisations without delay.

*Article 20*

**Transparency requirements**

1. A recognised data altruism organisation shall keep full and accurate records concerning:

(a) all natural or legal persons that were given the possibility to process data held by that recognised data altruism organisation, and their contact details;

(b) the date or duration of the processing of personal data or use of non-personal data;

(c) the purpose of the processing as declared by the natural or legal person that was given the possibility of processing;

(d) the fees paid by natural or legal persons processing the data, if any.

2. A recognised data altruism organisation shall draw up and transmit to the relevant competent authority for the registration of data altruism organisations an annual activity report which shall contain at least the following:

(a) information on the activities of the recognised data altruism organisation;

(b) a description of the way in which the objectives of general interest for which data was collected have been promoted during the given financial year;

(c) a list of all natural and legal persons that were allowed to process data it holds, including a summary description of the objectives of general interest pursued by such data processing and the description of the technical means used for it, including a description of the techniques used to preserve privacy and data protection;

(d) a summary of the results of the data processing allowed by the recognised data altruism organisation, where applicable;

(e) information on sources of revenue of the recognised data altruism organisation, in particular all revenue from allowing access to the data, and on expenditure.

*Article 21*

**Specific requirements to safeguard rights and interests of data subjects and data holders with regard to their data**

1. A recognised data altruism organisation shall inform data subjects or data holders prior to any processing of their data in a clear and easily comprehensible manner of:

(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 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. The recognised data altruism organisation shall not use the data for other objectives than those 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. The recognised data altruism organisation shall provide tools for obtaining consent from data subjects or permissions to process data made available by data holders. The recognised data altruism organisation shall also provide tools for easy withdrawal of such consent or permission.

4. The recognised data altruism organisation shall take measures to ensure an appropriate level of security for the storage and processing of non-personal data that it has collected based on data altruism.

5. The recognised data altruism organisation 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.

6. Where the recognised data altruism organisation facilitates 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, it shall, where relevant, specify the third-country jurisdiction in which the data use is intended to take place.

*Article 22*

**Rulebook**

1. The Commission shall adopt delegated acts in accordance with Article 32, supplementing this Regulation by establishing a rulebook laying down:

(a) appropriate information requirements to ensure that data subjects and data holders are provided, before a consent or permission for data altruism is given, with sufficiently detailed, clear and transparent information regarding the use of data, the tools for giving and withdrawing consent or permission, and the measures taken to avoid misuse of the data shared with the data altruism organisation;

(b) appropriate technical and security requirements to ensure the appropriate level of security for the storage and processing of data, as well as for the tools for giving and withdrawing consent or permission;

(c) communication roadmaps taking a multi-disciplinary approach to raise awareness of data altruism, of the designation as a 'data altruism organisation recognised in the Union' and of the rulebook among relevant stakeholders, in particular data holders and data subjects that would potentially share their data;

(d) recommendations on relevant interoperability standards.

2. The rulebook referred to in paragraph 1 shall be prepared in close cooperation with data altruism organisations and relevant stakeholders.

*Article 23*

**Competent authorities for the registration of data altruism organisations**

1. Each Member State shall designate one or more competent authorities responsible for its public national register of recognised data altruism organisations.

The competent authorities for the registration of data altruism organisations shall comply with the requirements set out in Article 26.

2. Each Member State shall notify the Commission of the identity of their competent authorities for the registration of data altruism organisations by 24 September 2023. Each Member State shall also notify the Commission of any subsequent change to the identity of those competent authorities.

3. The competent authority for the registration of data altruism organisations of a Member State shall undertake its tasks in cooperation with the relevant data protection authority, where such tasks are related to processing of personal data, and with relevant sectoral authorities of that Member State.

*Article 24*

**Monitoring of compliance**

1. The competent authorities for the registration of data altruism organisations shall monitor and supervise compliance of recognised data altruism organisations with the requirements laid down in this Chapter. The competent authority for the registration of data altruism organisations may also monitor and supervise the compliance of such recognised data altruism organisations, on the basis of a request by a natural or legal person.

2. The competent authorities for the registration of data altruism organisations shall have the power to request information from recognised data altruism organisations that is necessary to verify compliance with the requirements of this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

3. Where the competent authority for the registration of data altruism organisations finds that a recognised data altruism organisation does not comply with one or more of the requirements of this Chapter, it shall notify the recognised data altruism organisation 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 for the registration of data altruism organisations shall have the power to require the cessation of the infringement 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 altruism organisation does not comply with one or more of the requirements of this Chapter even after having been notified in accordance with paragraph 3 by the competent authority for the registration of data altruism organisations, that recognised data altruism organisation shall:

(a) lose its right to use the label 'data altruism organisation recognised in the Union' in any written and spoken communication;

(b) be removed from the relevant public national register of recognised data altruism organisations and the public Union register of recognised data altruism organisations.

Any decision revoking the right to use the label 'data altruism organisation recognised in the Union' under the first subparagraph, point (a), shall be made public by the competent authority for the registration of data altruism organisations.

6. If a recognised data altruism organisation has its main establishment or its legal representative in a Member State but is active in other Member States, the competent authority for the registration of data altruism organisations of the Member State of the main establishment or where the legal representative is located and the competent authorities for the registration of data altruism organisations of those other Member States shall cooperate and assist each other. Such assistance and cooperation may cover information exchanges between the competent authorities for the registration of data altruism organisations concerned for the purposes of their tasks under this Regulation and reasoned requests to take the measures referred to in this Article.

Where a competent authority for the registration of data altruism organisations in one Member State requests assistance from a competent authority for the registration of data altruism organisations in another Member State, it shall submit a reasoned request. The competent authority for the registration of data altruism organisations shall, upon such a request, provide a response without delay and within a timeframe proportionate to the urgency of the request.

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

*Article 25*

**European data altruism consent form**

1. In order to facilitate the collection of data based on data altruism, the Commission shall adopt implementing acts establishing and developing a European data altruism consent form, after consulting the European Data Protection Board, taking into account the advice of the European Data Innovation Board and duly involving relevant stakeholders. The form shall allow the collection of consent or permission across Member States in a uniform format. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 33(2).

2. The European data altruism consent form shall use a modular approach allowing customisation for specific sectors and for different purposes.

3. Where personal data are provided, the European data altruism consent form shall ensure that data subjects are able to give consent to and withdraw consent from a specific data processing operation in compliance with the requirements of Regulation (EU) 2016/679.

4. The form shall be available in a manner that can be printed on paper and is easily understandable as well as in an electronic, machine-readable form.

*CHAPTER V*

***Competent authorities and procedural provisions***

*Article 26*

**Requirements relating to competent authorities**

1. The competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations shall be legally distinct from, and functionally independent of, any data intermediation services provider or recognised data altruism organisation. The functions of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations may be carried out by the same authority. Member States may either establish one or more new authorities for those purposes or rely on existing ones.

2. Competent authorities for data intermediation services and competent authorities for the registration of data altruism organisations shall exercise their tasks in an impartial, transparent, consistent, reliable and timely manner. Where they exercise their tasks, they shall safeguard fair competition and non-discrimination.

3. The top-level management and personnel responsible for carrying out the relevant tasks of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the services which they evaluate, nor the authorised representative of any of those parties. This shall not preclude the use of evaluated services that are necessary for the operations of the competent authority for data intermediation services and the competent authority for the registration of data altruism organisations or the use of such services for personal purposes.

4. The top-level management and personnel of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations shall not engage in any activity that may conflict with their independence of judgment or integrity in relation to evaluation activities assigned to them.

5. The competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations shall have at their disposal the adequate financial and human resources to carry out the tasks assigned to them, including the necessary technical knowledge and resources.

6. The competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations of a Member State shall provide the Commission and competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations from other Member States, on reasoned request and without delay, with the information necessary to carry out their tasks under this Regulation. Where a competent authority for data intermediation services or a competent authority for the registration of data altruism organisations considers the information requested to be confidential in accordance with Union and national law on commercial and professional confidentiality, the Commission and any other competent authorities for data intermediation services or competent authorities for the registration of data altruism organisations concerned shall ensure such confidentiality.

*Article 27*

**Right to lodge a complaint**

1. Natural and legal persons shall have the right to lodge a complaint in relation to any matter falling within the scope of this Regulation, individually or, where relevant, collectively, with the relevant competent authority for data intermediation services against a data intermediation services provider or with the relevant competent authority for the registration of data altruism organisations against a recognised data altruism organisation.

2. The competent authority for data intermediation services or the competent authority for the registration of data altruism organisations with which the complaint has been lodged shall inform the complainant of:

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

(b) the judicial remedies provided for in Article 28.

*Article 28*

**Right to an effective judicial remedy**

1. Notwithstanding any administrative or other non-judicial remedies, any affected natural and legal persons shall have the right to an effective judicial remedy with regard to legally binding decisions referred to in Article 14 taken by the competent authorities for data intermediation services in the management, control and enforcement of the notification regime for data intermediation services providers and legally binding decisions referred to in Articles 19 and 24 taken by the competent authorities for the registration of data altruism organisations in the monitoring of recognised data altruism organisations.

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

3. Where a competent authority for data intermediation services or a competent authority for the registration of data altruism organisations fails to act on a complaint, any affected natural and legal persons shall, in accordance with national law, either have the right to an effective judicial remedy or access to review by an impartial body with the appropriate expertise.

*CHAPTER VI*

***European Data Innovation Board***

*Article 29*

**European Data Innovation Board**

1. The Commission shall establish a European Data Innovation Board in the form of an expert group, consisting of representatives of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations of all Member States, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the Commission, the EU SME Envoy or a representative appointed by the network of SME envoys, and other representatives of relevant bodies in specific sectors as well as bodies with specific expertise. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the expert group.

2. The European Data Innovation Board shall consist of at least the following three subgroups:

(a) a subgroup composed of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations, with a view to carrying out the tasks pursuant to Article 30, points (a), (c), (j) and (k);

(b) a subgroup for technical discussions on standardisation, portability and interoperability pursuant to Article 30, points (f) and (g);

(c) a subgroup for stakeholder involvement composed of relevant representatives from industry, research, academia, civil society, standardisation organisations, relevant common European data spaces and other relevant stakeholders and third parties advising the European Data Innovation Board on tasks pursuant to Article 30, points (d), (e), (f), (g) and (h).

3. The Commission shall chair the meetings of the European Data Innovation Board.

4. The European Data Innovation Board shall be assisted by a secretariat provided by the Commission.

*Article 30*

**Tasks of the European Data Innovation Board**

The European Data Innovation Board shall have the following tasks:

(a) to advise and assist the Commission with regard to developing a consistent practice of public sector bodies and competent bodies referred to in Article 7(1) in handling requests for the re-use of the categories of data referred to in Article 3(1);

(b) to advise and assist the Commission with regard to developing a consistent practice for data altruism across the Union;

(c) to advise and assist the Commission with regard to developing a consistent practice of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations in the application of requirements applicable to data intermediation services providers and recognised data altruism organisations;

(d) to advise and assist the Commission with regard to developing consistent guidelines on how to best protect, in the context of this Regulation, commercially sensitive non-personal data, in particular trade secrets, but also non-personal data representing content protected by intellectual property rights from unlawful access that risks intellectual property theft or industrial espionage;

(e) to advise and assist the Commission with regard to developing consistent guidelines for cybersecurity requirements for the exchange and storage of data;

(f) to advise the Commission, in particular taking into account the input from standardisation organisations, on the prioritisation of cross-sector standards to be used and developed for data use and cross-sector data sharing between emerging common European data spaces, cross-sectoral comparison and exchange of best practices with regard to sectoral requirements for security and access procedures, taking into account sector-specific standardisation activities, in particular clarifying and distinguishing which standards and practices are cross-sectoral and which are sectoral;

(g) to assist the Commission, in particular taking into account the input from standardisation organisations, in addressing fragmentation of the internal market and the data economy in the internal market by enhancing cross-border, cross-sector interoperability of data as well as data sharing services between different sectors and domains, building on existing European, international or national standards, *inter alia* with the aim of encouraging the creation of common European data spaces;

(h) to propose guidelines for common European data spaces, namely purpose- or sector-specific or cross-sectoral interoperable frameworks of 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, such common standards and practices taking into account existing standards, complying with the competition rules and ensuring non-discriminatory access to all participants, for the purpose of facilitating data sharing in the Union and reaping the potential of existing and future data spaces, addressing, *inter alia*:

   (i) cross-sectoral standards to be used and developed for data use and cross-sector data sharing, cross-sectoral comparison and exchange of best practices with regard to sectoral requirements for security and access procedures, taking into account sector-specific standardisation activities, in particular clarifying and distinguishing which standards and practices are cross-sectoral and which are sectoral;

   (ii) requirements to counter barriers to market entry and to avoid lock-in effects, for the purpose of ensuring fair competition and interoperability;

(iii) adequate protection for lawful data transfers to third countries, including safeguards against any transfers prohibited by Union law;

(iv) adequate and non-discriminatory representation of relevant stakeholders in the governance of common European data spaces;

(v) adherence to cybersecurity requirements in accordance with Union law;

(i) to facilitate cooperation between Member States with regard to setting harmonised conditions allowing for the re-use of the categories of data referred to in Article 3(1) held by public sector bodies across the internal market;

(j) to facilitate cooperation between competent authorities for data intermediation services and competent authorities for the registration of data altruism organisations through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the notification procedure for data intermediation services providers and the registration and monitoring of recognised data altruism organisations, including coordination with regard to the setting of fees or penalties, as well as facilitate cooperation between competent authorities for data intermediation services and competent authorities for the registration of data altruism organisations with regard to international access and transfer of data;

(k) to advise and assist the Commission with regard to evaluating whether the implementing acts referred to in Article 5(11) and (12) are to be adopted;

(l) to advise and assist the Commission with regard to developing the European data altruism consent form in accordance with Article 25(1);

(m) to advise the Commission on improving the international regulatory environment for non-personal data, including standardisation.

*CHAPTER VII*

***International access and transfer***

*Article 31*

**International access and transfer**

1. The public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.

2. Any decision or judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a public sector body, a natural or legal person to which the right to re-use data was granted under Chapter II, a data intermediation services provider or recognised data altruism organisation to transfer or give access to non-personal data within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State.

3. In the absence of an international agreement as referred to in paragraph 2 of this Article, where a public sector body, a natural or legal person to which the right to re-use data was granted under Chapter II, a data intermediation services provider or 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 within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where:

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

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

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

4. If the conditions laid down in paragraph 2 or 3 are met, the public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation of the request.

5. The public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider and the recognised data altruism organisation shall inform the data holder about the existence of a request of a third-country administrative authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

*CHAPTER VIII*

***Delegation and committee procedure***

*Article 32*

**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 5(13) and Article 22(1) shall be conferred on the Commission for an indeterminate period of time from 23 June 2022.

3. The delegation of power referred to in Article 5(13) and Article 22(1) 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 5(13) or Article 22(1) 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 33*

**Committee procedure**

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

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

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

*CHAPTER IX*

***Final and transitional provisions***

*Article 34*

**Penalties**

1. Member States shall lay down the rules on penalties applicable to infringements of the obligations regarding transfers of non-personal data to third countries pursuant to Article 5(14) and Article 31, the notification obligation of data intermediation services providers pursuant to Article 11, the conditions for providing data intermediation services pursuant to Article 12 and the conditions for the registration as a recognised data altruism organisation pursuant to Articles 18, 20, 21 and 22, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. In their rules on penalties, Member States shall take into account the recommendations of the European Data Innovation Board. Member States shall, by 24 September 2023, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

2. Member States shall take into account the following non-exhaustive and indicative criteria for the imposition of penalties on data intermediation services providers and recognised data altruism organisations for infringements of this Regulation, where appropriate:

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

(b) any action taken by the data intermediation services provider or recognised data altruism organisation to mitigate or remedy the damage caused by the infringement;

(c) any previous infringements by the data intermediation services provider or recognised data altruism organisation;

(d) the financial benefits gained or losses avoided by the data intermediation services provider or recognised data altruism organisation due to the infringement, insofar as such benefits or losses can be reliably established;

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

*Article 35*

**Evaluation and review**

By 24 September 2025, the Commission shall carry out an evaluation of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee. The report shall be accompanied, where necessary, by legislative proposals.

The report shall assess, in particular:

(a) the application and functioning of the rules on penalties laid down by the Member States pursuant to Article 34;

(b) the level of compliance of the legal representatives of data intermediation services providers and recognised data altruism organisations that are not established in the Union with this Regulation and the level of enforceability of penalties imposed on those providers and organisations;

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

Member States shall provide the Commission with the information necessary for the preparation of that report.

*Article 36*

**Amendment to Regulation (EU) 2018/1724**

In the table in Annex II to Regulation (EU) 2018/1724, the entry 'Starting, running and closing a business' is replaced by the following:

| Life events | Procedures | Expected output subject to an assessment of the application by the competent authority in accordance with national law, where relevant |
|---|---|---|
| Starting, running and closing a business | Notification of business activity, permission for exercising a business activity, changes of business activity and the termination of a business activity not involving insolvency or liquidation procedures, excluding the initial registration of a business activity with the business register and excluding procedures concerning the constitution of or any subsequent filing by companies or firms within the meaning of the second paragraph of Article 54 TFEU | Confirmation of the receipt of notification or change, or of the request for permission for business activity |
| | Registration of an employer (a natural person) with compulsory pension and insurance schemes | Confirmation of registration or social security registration number |
| | Registration of employees with compulsory pension and insurance schemes | Confirmation of registration or social security registration number |
| | Submitting a corporate tax declaration | Confirmation of the receipt of the declaration |
| | Notification to the social security schemes of the end of contract with an employee, excluding procedures for the collective termination of employee contracts | Confirmation of the receipt of the notification |
| | Payment of social contributions for employees | Receipt or other form of confirmation of payment of social contributions for employees |
| | Notification of a data intermediation services provider | Confirmation of the receipt of notification |
| | Registration as a data altruism organisation recognised in the Union | Confirmation of the registration |

*Article 37*

**Transitional arrangements**

Entities providing the data intermediation services referred to in Article 10 on 23 June 2022 shall comply with the obligations set out in Chapter III by 24 September 2025.

*Article 38*

**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 24 September 2023.

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

Done at Brussels, 30 May 2022.

| *For the European Parliament* | *For the Council* |
| --- | --- |
| *The President* | *The President* |
| R. METSOLA | B. LE MAIRE |