Council of the European Union

Brussels, 10 December 2021
(OR. en)

14606/21

Interinstitutional File:
2020/0340(COD)

LIMITE

TELECOM 451
COMPET 884
MI 911
DATAPROTECT 275
JAI 1331
CODEC 1583

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	14021/21
No. Cion doc.:	13351/20
Subject:	Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Analysis of the final compromise text in view to agreement

I. INTRODUCTION

1. The Commission adopted the proposal for a Regulation on European data governance (Data Governance Act, DGA) on 25 November 2020[1]. It is the first of a set of measures announced by the Commission in the 2020 European strategy for data[2].

2. The mandate for opening negotiations with the European Parliament on the DGA was granted by Coreper on 1 October. After the opening trilogue on 20 October, during which the work on all issues was delegated to the technical level, the Slovenian Presidency held 12 technical meetings with the European Parliament.

[1] doc. 13351/20.
[2] COM/2020/66 final.

3. On 24 November, Coreper granted the Presidency a revised mandate to continue the negotiations.

4. The second trilogue was held on 30 November. During this trilogue the Council and the European Parliament came to an agreement on all political issues and successfully closed the negotiations.

5. In the Annex to this document delegations will find the Proposal for a Regulation on European data governance updated according to the provisional political agreement reached at the second trilogue.

II. MAIN ELEMENTS OF THE COMPROMISE

1. **Period of exclusivity for the re-use of public sector data - Articles 4(5) and 4(7) and Recitals 9 and 10**

   As regards the length of the exclusivity period that can be granted for the re-use of public sector data, both for potential new exclusive arrangements and for those that would be concluded before the date of entry into force of the DGA, the draft agreement provides that the maximum length of existing exclusive arrangements will be two and a half years, while in the case of new exclusive arrangements it will be 12 months.

2. **Support by public sector bodies for for re-users - Articles 5(6) and Recital 11**

   On the support by public sector bodies for potential re-users in seeking consent or permission for the re-use of certain protected public sector data, the agreement provides that public sector bodies will be under no hard obligation to support re-users in this respect. Instead, there is softer language in the text stipulating that they will have to make the best effort to do so.

3. **Implementing and delegated acts**

During the second trilogue, a compromise was also reached with regard to the use of delegated and implementing acts in four cases:

- adequacy decisions for transfers of non-personal data to third countries **(Article 5(10b))**;
- conditions for transfers of highly sensitive public sector data to third countries **(Article 5(11))**;
- model contractual clauses to support public sector bodies and re-users in their compliance with conditions for re-use **(Article 5(10a))**; and
- rulebook for data altruism organisations **(Article19a(1))**.

The draft agreement provides for the use of implementing acts with examination procedure for adequacy decisions and model contractual clauses. In these cases the future provisions will remain in line with the equivalent procedures for personal data under the GDPR.

With regard to the remaining two cases, namely conditions for transfers of highly sensitive public sector data to third countries and the rulebook for data altruism organisations, the co-legislators agreed to use delegated acts for secondary legislation.

4. **Date of application - Article 35**

The draft agreement also contains a revised date of application of the DGA, which has been extended from 12 to 15 months from entry to force, in order to allow Member States sufficient preparation time for the implementation of the DGA.

III. CONCLUSION

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

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

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

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European data governance

(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[3],

Having regard to the opinion of the Committee of the Regions[4],

Acting in accordance with the ordinary legislative procedure,

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.

[3] OJ C , , p. .
[4] OJ C , , p. .

(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 this transformation: data-driven innovation will bring enormous benefits both for citizens and the economy, for example through improved personalised medicine, new mobility, and its contribution to the communication of the Commission of 11 December 2019 on the European Green Deal. In order to make this data-driven economy inclusive for all Europeans, special attention must be paid to reducing 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 to enable businesses, in particular micro, small and medium sized enterprises (SMEs) as defined in the annex to Commission Recommendation 2003/361/EC[5] and start-ups to thrive, ensuring data access neutrality, portability and interoperability, and avoiding lock-in effects. In its communication of 19 February 2020 on a European Strategy for data, the Commission described the vision of a common European data space, a Single Market for data in which data could be used irrespective of its physical location of storage in the Union in compliance with applicable law, which inter alia can be pivotal for the rapid development of artificial intelligence technologies. It 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, it proposes to establish domain-specific common European data spaces, as the concrete arrangements in which data sharing and data pooling can happen. As foreseen in that strategy, such common European data spaces can cover areas such as health, mobility, manufacturing, financial services, energy, or agriculture or thematic areas, such as the European green deal or European data spaces for public administration or skills, as well as a combination of these areas, e.g. energy and climate. In accordance with the FAIR data principles, common European data spaces should make data findable, accessible, interoperable and re-usable, while ensuring a high level of cybersecurity. When there is a level playing field in the data economy, businesses 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, a sound governance is needed, in which relevant stakeholders of a common European data space need to be represented and engaged.

(2d) In order to facilitate and encourage the use of public sector data for the purposes of scientific research, public sector bodies are encouraged to develop a harmonized approach and processes to make public sector data easily accessible for the purposes of scientific research in the public interest. This could mean, inter alia, creating streamlined administrative procedures, standardized data formatting, informative metadata on the methodological and data collection choices, and standardized data-fields that enable the easy joining of data-sets from different public sector data sources where relevant for the purposes of analysis. These practices should have as its objective the promotion of 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'.

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

(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 a borderless digital internal market and a human-centric, trustworthy and secure data society and economy. Sector-specific legislation can develop, adapt and propose new and complementary elements, depending on the specificities of the sector, such as the envisaged legislation on the European health data space[6] and on access to vehicle data. Moreover, certain sectors of the economy are already regulated by sector-specific Union law that include rules relating to cross-border or Union wide sharing or access to data[7]. This Regulation should therefore be without prejudice to Directive (EU) 2016/943 of the European Parliament and of the Council ([8]), Regulation (EU) 2018/1807 of the European Parliament and of the Council ([9]), Regulation (EC) No 223/2009 of the European Parliament and of the Council ([10]), Directive 2000/31/EC of the European Parliament and of the Council ([11]), Directive 2001/29/EC of the European Parliament and of the Council ([12]), Directive (EU) 2019/790 of the European Parliament and of the Council ([13]), Directive 2004/48/EC of the European Parliament and of the Council ([14]), Directive (EU) 2019/1024 of the European Parliament and of the Council ([15]), as well as Regulation 2018/858/EU of the European Parliament and of the Council ([16]), Directive 2010/40/EU of the European Parliament and of the Council ([17]) , Directive 2007/2/EC of the

---

6 See: Annexes to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Commission Work Programme 2021, (COM(2020) 690 final).

7 For example Directive 2011/24/EU in the context of the European Health Data Space, and relevant transport legislation such as Directive 2010/40/EU, Regulation 2019/1239 and Regulation (EU) 2020/1056 in the context of the European Mobility Data Space.

8 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).

9 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).

10 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, 31.03.2009, p. 164).

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, 17.07.2000, 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 (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).

14 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).

15 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).

16 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).

17 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).

European Parliament and of the Council[18], Directive (EU) 2017/1132 of the European Parliament and of the Council[19], Directive (EU) 2015/849 of the European Parliament and of the Council[20] and any other sector-specific Union legislation that organises the access to and re-use of data. This Regulation should be without prejudice to Union and national law on the access and use of data for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as international cooperation in this context. This Regulation should be without prejudice to the competences of the Member States regarding activities concerning public security, defence and national security. Re-use of data protected for such reasons and held by public sector bodies should not be covered by this Regulation. This should include data from procurement procedures falling within the scope of Directive 2009/81/EC. 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. Where a sector-specific Union legal act requires public sector bodies, providers of data intermediation services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act should also apply.

(3a) This Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council**[21]** and to Directives 2002/58/EC**[22]** and (EU) 2016/680**[23]** of the European Parliament and of the Council, and the corresponding provisions of national law. This Regulation should in particular not be read as creating a new legal basis for the processing of personal data for any of the regulated activities, or as modifying information requirements under Regulation (EU) 2016/679. Its implementation should not prevent cross-border transfers of data in accordance with Chapter V of Regulation (EU) 2016/679 from taking place. In the event of conflict between the provisions of this Regulation and Union law or national law on the protection of personal data adopted in accordance with Union law, the latter should prevail. It should be possible to consider data protection authorities competent authorities under this Regulation. Where other entities function as competent authorities under this Regulation, it should be without prejudice to the supervisory powers and competences of data protection authorities under Regulation (EU) 2016/679. Where

---

18 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).

19 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).

20 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.

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 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).

23 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).

personal and non-personal data in a data set are inextricably linked, this Regulation should not prejudice the application of Regulation (EU) 2016/679.

(4) Action at Union level is necessary to increase trust in data sharing by establishing proper mechanisms for control by data subjects and data holders over the data that relates to them, and in order to address other barriers to a well-functioning and competitive data-driven economy. A Union-wide governance framework should have the objective of building trust among individuals and businesses for data access, control, sharing, use and re-use, in particular by establishing proper mechanisms for data subjects to know and meaningfully exercise their rights, as well as regarding the re-use of certain types of data held by the public sector, the provision of services by providers of data intermediation services to business users and to data subjects, 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 businesses can help increase trust. This action is without prejudice to obligations and commitments in the international trade agreements concluded by the Union.

(5) 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 as well as sector-specific legislation ensure that the public sector makes more of the data it produces easily available for use and re-use. However, certain categories of data (commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties, including trade secrets and personal data) in public databases is often not made available, despite this being possible in accordance with the applicable Union law, in particular Regulation (EU) 2016/679 and Directives 2002/58/EC and (EU) 2016/680, not even for research or innovative activities in the public interest. Due to the sensitivity of those 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 limit negative impact on fundamental rights, the principle of non-discrimination and data protection. Such requirements are usually time- and knowledge-intensive to fulfil. This has led to the underutilisation of such data. While some Member States are setting up structures, processes and sometimes legislate to facilitate this 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.

(6) There are techniques enabling analyses on databases that contain personal data, such as anonymisation, differential privacy, generalisation, or suppression, and randomisation, use of synthetic data or other such 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 these 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 this implies that the data use and re-use in this context can only be done in a secure processing environment set in place and supervised by the public sector. 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)

557/2013[24]. In general, insofar as personal data are concerned, the processing of personal data should rely upon one or more of the grounds for processing provided in Articles 6 and 9 of Regulation (EU) 2016/679.

(6a) 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 purposes of ensuring information security, improving existing anonymisation techniques and contributing to the overall robustness of anonymisation, undertaken in accordance with Regulation (EU) 2016/679.

(6b) 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 authorities to create and make available data in accordance with the principle of 'open by design and by default' as referred to in Recital (16) of Directive (EU) 2019/1024 and promote the creation and the procurement of data in formats and structures that facilitates anonymisation in that regard.

(7) 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 business. 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[25], which sets the framework for the lawful acquisition, use or disclosure of trade secrets. This Regulation should not create an obligation to allow re-use of public sector data. 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. It should be without prejudice and complementary 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 is also without prejudice to 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.

---

[24] Commission Regulation (EU) 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).

[25] OJ L 157, 15.6.2016, p. 1–18.

(8) 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, as defined by law or by 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 they hold should not be subject to this Regulation. Data held by cultural establishments, such as libraries, archives and museums, as well as orchestras, operas, ballets, and theatres, and 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 and/or bodies governed by public law. This Regulation should apply to such hybrid organisations only in their capacity as research performing organisations. If such a research performing organisation holds data as a part of a specific public-private association with private sector organisations or other public bodies, bodies governed by public law or hybrid research performing organisations (i.e. organised as both public sector bodies or public undertakings) with the main purpose of pursuing research, these data should also not be covered by this Regulation. Where relevant, Member States should be able to apply the requirements of this Regulation to public undertakings or private undertakings that exercise public sector duties or provide services of general interest. The exchange of data among public sector bodies, or between public sector bodies and public sector bodies in third countries or international organizations, purely in pursuit of their public tasks, in particular 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.

(9) 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 agreement should be only possible when justified and necessary for the provision of a service of general interest. This may be the case when 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 delivering the service or the product which allows the public sector body to provide service in the general interest. Such arrangements should, however, be concluded in compliance with public procurement and concession award rules 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 period, which should not exceed 12 months. In order to ensure transparency, such exclusive agreements should be published online, in a form that is in accordance with Union law on public procurement, where relevant. Where an exclusive right to re-use data does not meet the conditions set out in this Regulation, the exclusive right should be invalid.

(10) 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 have been already in place before the entry into force of this Regulation should not be renewed after the expiration of their term. In the case of indefinite or longer-term agreements, they should be terminated within thirty months from the date of entry into force of this Regulation.

(11) Conditions for re-use of protected data that apply to public sector bodies, which are designated as competent under national law to allow re-use, and which should be without prejudice to rights or obligations concerning access to such data, should be laid down. 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 reuse should be designed in a manner promoting scientific research. e.g. privileging scientific research should as a rule be considered 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 others 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 for the public sector. Conditions should be designed to ensure effective safeguards with regard to the protection of personal data. Before its transmission, personal data should be anonymised, so as to not allow the identification of the data subjects, or data containing commercially confidential information modified in such a way that no confidential information is disclosed. Where provision of anonymised or modified data would not respond to the needs of the re-user, and where any requirements of completing a data protection impact assessment and consulting the supervisory authority pursuant to Articles 35 and 36 of Regulation (EU) 2016/679 have been fulfilled and the risks for 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 permitted. This could be a suitable arrangement for the reuse 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 others. In particular, personal data should only be transmitted for re-use to a third party where a legal basis under data protection legislation allows such transmission. Non-personal data should only be transmitted when 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 remain personal data within the meaning of Regulation (EU) 2016/679. In the event of reidentification of data subjects, the obligation to notify such a data breach to the public sector body should apply in addition to the obligation to notify such a data breach to a supervisory authority and to the data subject in accordance with Regulation (EU) 2016/679. The public sector bodies, where relevant, should facilitate the re-use of data on the basis of consent of data subjects or permissions of legal persons on the re-use of data pertaining to them through adequate technical means. In this respect, the public sector body should make best efforts to provide assistance to potential re-users in seeking such consent by establishing technical mechanisms that permit transmitting requests for consent from re-users, where practically feasible. No contact information should be given that allows re-users to contact data subjects or data holders directly. When transmitting the request to consent, the public sector body should ensure that the data subject is clearly informed of the possibility to refuse to give consent.

(12) 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 should it limit the exercise of these 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 WIPO Copyright Treaty (WCT) and Union or national law governing intellectual property. Public sector bodies should, however, exercise their copyright in a way that facilitates re-use.

(13) Data subject to intellectual property rights as well as trade secrets should only be transmitted to a third party where such transmission is lawful by virtue of Union or national law or with the agreement of the right holder. Where public sector bodies are holders of the right 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.

(14) Companies and data subjects should be able to trust that the re-use of certain categories of protected data, which are held by the public sector, will take place in a manner that respects their rights and interests. Additional safeguards should thus be put in place for situations in which the re-use of such public sector data is taking place on the basis of a processing of the data outside the public sector. Such an additional safeguard could be found in the requirement that public sector bodies should 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 when such data is transferred to third countries. Public sector bodies should not permit re-use of information stored in e-health applications by insurance companies 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.

(15) Furthermore, in order to preserve fair competition and an 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 IP theft or industrial espionage. In order to ensure the protection of rights or interests of data holders, non-personal data which is to be protected from unlawful or unauthorised access under Union or national law, and which is held by public sector bodies, can be transferred to third-countries only when appropriate safeguards for the use of data are provided. Such appropriate safeguards should include the public sector body only transmitting protected data to a re-user, if the re-user undertakes obligations in the interest of the protection of the data. The re-user that intends to transfer the data to such third country should commit to comply with the obligations laid out 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. In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to establish model contractual clauses for the transfer by re-users of non-personal data to a third country.

---

[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).

(16) Appropriate safeguards should also be considered to be implemented when in that third-country there are equivalent measures in place which ensure that non-personal data benefits from a level of protection similar to that applicable by means of Union law in particular as regards the protection of trade secrets and the protection of intellectual property rights. To that end, the Commission may adopt implementing acts, when justified by a substantial number of requests, across the Union, concerning the re-use of non-personal data in specific third countries, that declare that a third country provides a level of protection that is essentially equivalent to those provided by Union or national law. The Commission should assess the necessity of the adoption of such implementing acts based on the information provided by the Member States through the European Data Innovation Board. Such implementing acts would reassure public sector bodies that re-use of publicly held data in the concerned third-country would not compromise the protected nature of the data. The assessment of the level of protection afforded in such third-country should, in particular, take into consideration the relevant legislation, both general and sectoral, including on public security, defence, national security and criminal law concerning the access to and protection of non-personal data, any access by the public authorities 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, or the third countries' international commitments regarding the protection of data the third country concerned has entered into, 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 service 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 are 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 public sector bodies' right to oblige re-users to comply with conditions for re-use, in accordance with this Regulation.

(17) Some third countries adopt laws, regulations and other legal acts which aim at directly transferring or providing governmental access to non-personal data in the Union under the control of natural and legal persons under the jurisdiction of the Member States. Judgments of courts or tribunals or decisions of administrative authorities in third countries requiring such transfer or access to non-personal data should be enforceable when based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. In 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 as regards the protection of fundamental rights of the individual or 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, and including its contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, transfer or access should only be allowed if, in particular it has been verified that the third-country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent court in the third country, which is empowered to take duly into account the relevant legal interests of the provider of such data.

Moreover, public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation service providers and entities entered in the register of recognised data altruism organisations should ensure, when signing contractual agreements with other private parties, that non-personal data held in the Union are only accessed in or transferred to third countries in compliance with the law of the Union or the law of the relevant Member State.

(18a) 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 businesses that ensure that 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 service providers and entities entered in a national register of 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 these ends, it has to be ensured that public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation service providers and entities entered in the register of recognized data altruism organisations should adhere to all relevant technical standards, codes of conduct and certifications at Union level.

(19) 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 acts adopted in accordance with a legislative procedure, as regards the transfer to third countries, if such transfer could jeopardise 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 could be 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 legislation. The 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 public policy objectives identified, such as the protection of public health, safety, the environment, public morals, 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. These conditions could include terms applicable for the transfer or technical arrangements, such as the requirement of using a secure processing environment, limitations as regards the re-use of data in third-countries or categories of persons which are entitled to transfer such data to third countries or who can access the data in the third country. In exceptional cases they could also include restrictions on transfer of the data to third countries to protect the public interest.

(20) Public sector bodies should be able to charge fees for the re-use of data but should also be able to decide to allow re-use at lower or no cost, for example for certain categories of re-uses such as non-commercial re-use or scientific research purposes, or re-use by SMEs and start-ups, civil society and educational establishments, so as to incentivise such re-use in order to stimulate research and innovation and support companies that are an important source of innovation and typically find it more difficult to collect relevant data themselves, in line with State aid rules. In this specific context, scientific research purposes should be understood to include any type of research related purpose regardless of the organizational or financial structure of the research institution in question, with the exception of research that is being conducted by a company aiming at the development, enhancement or optimisation of products or services. Such fees should be proportionate to the costs incurred, transparent, published online non-discriminatory 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.

(21) In order to incentivise the re-use of these categories of data, Member States should establish a single information point to act as an interface for re-users that seek to re-use such data held by the public sector bodies. 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 when transmitting enquiries or requests for the re-use. Sufficient human oversight should be ensured in the transmission process. Already existing practical arrangements such as Open Data Portals could be used for this purpose. It should have an asset list containing all available data sources, including, where relevant, those available at sectoral, regional and local information points, with relevant information describing the 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 in sectoral Union or Member States legislation. Those competent bodies should provide support to public sector bodies with state-of-the-art techniques, including how to best structure and store data to make data easily accessible, in particular through application programming interfaces, as well as 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 and act in accordance with the instructions received from the public sector body. Such support structure could support the data subjects and data holders with management of the consent or permission to re-use, including consent to certain areas of scientific research when 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 performed under the responsibility of the public sector body responsible for the register containing the data, who remains a data controller within the meaning of Regulation (EU) 2016/679 insofar as personal data are concerned. Member States may have in place one or several competent bodies, which could act in different sectors. Internal services of public sector bodies could act as competent bodies. A competent body can be a public sector body supporting other public sector bodies in allowing re-use of data, where relevant, or a public sector body allowing re-use itself. Supporting other public sector bodies entails informing them, upon request, about best practices on how to fulfil the requirements established by this Regulation such as the technical means to make a secure processing environment available or the technical means to ensure privacy and confidentiality when providing access to data within the scope of this Regulation.

(22) 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 companies or facilitating data sharing obligations set by Union or national law. They could become a tool to facilitate the exchange of substantial amounts of relevant data. Providers of data intermediation services, which can also include public sector bodies, offering 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 both data subjects and data holders, and from 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 actors 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, meaning purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives. Data intermediation services could include inter alia 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 holders, data subjects and data users.

(22a) This Regulation should cover services which aim at the establishment of commercial relationships for the purpose of data sharing between an undetermined number of data subjects and data holders, on the one hand, and data users on the other hand, through technical, legal or other means, including for the exercise of data subjects' rights in relation to personal data. Where businesses and other actors offer multiple data-related services, only the activities which directly concern the provision of data intermediation services are covered by this Regulation. The provision of cloud storage, analytics or of data sharing software, the provision of web browsers or browser plug-ins, or an email service should not be considered data intermediation services in the sense of this Regulation, as long as such services only provide technical tools for data subjects or data holders to share data with others, but are neither used for aiming to establish a commercial relationship between data holders and data users, nor allow the provider to acquire information on the establishment of commercial relationships for the purpose of data sharing, through the provision of such services. Examples of data intermediation services would include, inter alia, data marketplaces on which companies could make available data 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 pool to all interested parties in a manner that all participants contributing to the pool would receive a reward for their contribution to the pool. This would exclude value-added data services, that obtain data from data holders, 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 data intermediation services, exclusively used by one data holder in order to enable the use of data they hold, or used by multiple legal entities in a closed group, including supplier or customer relationships or contractually-defined collaborations, in particular those that have as a main objective the ensuring of functionalities of objects and devices connected to the internet-of-things.

(22b) Services that focus on the intermediation of copyright-protected content, such as online content sharing service providers in the meaning of Article 2(6) of Directive (EU) 2019/790 should not be covered by this Regulation. 'Consolidated tape providers' as defined in Article 4 (1) point 53 of Directive 2014/65/EU of the European Parliament and of the Council[27] fall outside the scope of the definition of data intermediation services. Additionally, '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 as data intermediation service providers for the purposes of this Regulation. This Regulation should also not apply to services established by the public sector in order to facilitate either the re-use of protected data held by different public sector bodies in accordance with Chapter II of this Regulation or any other data, insofar as they do not aim to establish commercial relationships. Data altruism organisations regulated by Chapter IV of this Regulation should not be considered offering data intermediation services, as long as they do not establish a commercial relationship between potential data users, on the one hand, and data subjects and data holders who make data available on altruistic motives, on the other hand. Other services that do not aim to establish commercial relationships, such as repositories aimed at enabling re-use of scientific research data in accordance with Open Access principles should not be considered data intermediation services in the sense of this Regulation.

(23) A specific category of data intermediation services includes providers of services that offer their services to data subjects within the meaning of Regulation (EU) 2016/679. Such providers seek to enhance individual agency, and in particular the individuals' control over the data relating to them. They 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 data portability right, which allows data subjects to move their personal data from one controller to the other. In this context, it is important that their business model 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 what is in the individuals' own interest. This could include advising individuals on uses of their data they could allow 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 storage space, or '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 data spaces' may contain static personal data such as name, address or date of birth as well as dynamic data that an individual generates e.g. through the use of an online service or an object connected to the Internet-of-Things. They may also be used to store verified identity information (passport number, social security information) as well as proof of personal attributes (e.g. driving licence, diplomas or bank account information).

---

[27] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, (OJ L 173, 12.6.2014, p. 349).

[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)

(24) 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 when such data relates to several data subjects within that group. In this 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 companies and SMEs that in terms of knowledge of data sharing, are often comparable to individuals.

(25) In order to increase trust in such data intermediation services, in particular related to the use of data and the compliance with the conditions imposed by data subjects and data holders, it is necessary to create a Union-level regulatory framework, which sets out highly harmonised requirements related to the trustworthy provision of such data intermediation services, and which is implemented by the national competent authorities. This will contribute to ensuring that data subjects and data holders, as well as data users, have better control over the 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 service providers should offer a novel, 'European' way of data governance, by providing a separation in the data economy between data provision, intermediation and use. Providers of data intermediation services 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 service 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, 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, providers of data intermediation services should be allowed to make adaptations to the data exchanged, in order to improve the usability of the data by the data user, where the data user so desires, or improve interoperability such as to convert it into specific formats.

(25a) Providers of data intermediation services which meet the requirements laid down in this Regulation should be able to use the title 'providers of data intermediation services recognised in the Union'. In order to assist data subjects and legal entities to easily identify, and thereby increase their trust in, providers of data intermediation services recognised in the Union, a common logo that is recognisable throughout the Union should be established. In order to ensure uniform conditions for the application of that logo, implementing powers should be conferred on the Commission to establish a design for that common logo.

(26) It is important to enable a competitive environment for data sharing. A key element to bring trust and more control for data holders, data subjects and data users in data intermediation services is the neutrality of providers of data intermediation services as regards the data exchanged between data holders or data subjects and data users. It is therefore necessary that providers of data intermediation services act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose. The pricing and terms of data intermediation services should not be made dependent on whether or to what extent 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 provider or a related entity. This will also require structural separation between the data intermediation service and any other services provided, so as to avoid issues of conflict 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 provider of data intermediation services. As an exception to this, the data intermediation service providers should be able to use the data provided by the data holder for the improvement of their data intermediation services. Providers of data intermediation services 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 shall not use data for purposes other than those related to data intermediation services. Providers of data intermediation services 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 damages and detriments resulting from any conduct of the data intermediation service provider could be addressed in the relevant contract, based on the national liability regimes.

(26a) Data intermediation service providers should take reasonable measures to ensure interoperability within a sector and between different sectors to ensure the proper functioning of the market. Reasonable measures could include following the existing, commonly-used standards in the sector where the data service provider operates. The European Data Innovation Board should facilitate the emergence of additional industry standards, where necessary. Data intermediation service providers should implement in due time the measures for interoperability between the data intermediation services set out by the European Data Innovation Board.

(27) In order to ensure the compliance of data intermediation services with the conditions set out in this Regulation, providers of such services should have a place of establishment in the Union. Where a provider of data intermediation services not established in the Union offers services within the Union, it should designate a legal representative. Designation of a legal representative in such cases is necessary, given that such providers of data intermediation services handle personal data as well as commercially confidential data, which necessitates the close monitoring of the compliance of providers of data intermediation services with the conditions laid out in this Regulation. In order to determine whether such a provider of data intermediation services is offering services within the Union, it should be ascertained whether it is apparent that the provider of data intermediation services 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 of other contact details of the provider of data intermediation services, or the use of a language generally used in the third country where the provider of data intermediation services is established, should be considered 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 other language, or the mentioning of users who are in the Union, could make it apparent that the provider of data intermediation services is planning to offer services within the Union. The designated legal representative should act on behalf of the provider of data intermediation services and it should be possible for competent authorities to contact the legal representative, including in the case of an infringement, to initiate enforcement proceeding against a non-compliant provider of data intermediation services not established in the Union. The legal representative should be designated by a written mandate of the provider of data intermediation services to act on the latter's behalf with regard to the latter's obligations under this Regulation.

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

(28a) Providers of data intermediation services are expected to have in place procedures and measures to sanction fraudulent or abusive practices in relation to access to data from parties seeking access through their services, including through measures such as the exclusion of data users that breach the terms of service or infringe existing legislation.

(29) This Regulation should be also without prejudice to the application of competition law. Providers of data intermediation services should also take measures to ensure compliance with competition law and have procedures in place to this effect. This applies in particular in situations where data sharing enables businesses 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.

(29a) Member States should lay down rules on penalties for the infringements of this Regulation. Those penalties should be effective, proportionate and dissuasive. Large discrepancies between rules on penalties could lead to distortion of competition in the Digital Single Market. Harmonisation of such rules could be of benefit in this regard.

(30) A notification procedure for data intermediation services should be established in order to ensure a data governance within the Union 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 the provision of such services. The notification procedure should not impose undue obstacles for SMEs, start-ups and civil society organisations and follow the principle of non-discrimination.

(31) In order to support effective cross-border provision of services, the provider of data intermediation services should be requested to send a notification only to the designated competent authority 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 provider of data intermediation services should be able to start operating in other Member States without further notification obligations.

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

(33) The competent authorities designated to monitor compliance of data intermediation services with the requirements in this Regulation should be chosen on the basis of their capacity and expertise regarding horizontal or sectoral data sharing, and they should be independent of any provider of data intermediation services as well as transparent and impartial in the exercise of their tasks. Member States should notify the Commission of the identity of the designated competent authorities. The powers and competences of the designated competent authorities 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 should seek, where relevant, an opinion or decision by the competent supervisory authority established pursuant to that Regulation.

(34) The notification framework 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 legislation.

(35) There is a strong potential in the use of data made available voluntarily by data subjects based on their informed consent or, where it concerns non-personal data, made available by legal persons, for objectives of general interest. Such objectives would include healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of European statistics or improving the provision of public services. Support to scientific research should be considered as well an objective of general interest. This Regulation should aim at contributing to the emergence of pools of data made available on the basis of data altruism that have a sufficient size in order to enable data analytics and machine learning, including across borders in the Union. In order to achieve this objective, Member States could have organizational or technical arrangements in place, 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 organization of awareness campaigns, or a structured exchange between public authorities on how public policies benefit from data altruism (e.g. improving traffic, public health, combating climate change). In support of this, Member States could also define national policies for data altruism. Data subjects should be able to receive compensation related only to the costs they incur making their data available for objectives of general interest.

(36) Legal entities that seek to support objectives of general interest by making available relevant data based on data altruism at scale and meet certain requirements, should be able to register as 'data altruism organisations recognised in the Union'. This could lead to the establishment of data repositories. As registration in a Member State would be valid across the Union, this should facilitate cross-border data use within the Union and the emergence of data pools covering several Member States. Legal persons could give permission to the processing of their non-personal data for a range of purposes not defined at the moment of giving the permission. The compliance of such registered entities with a set of requirements should bring trust that the data made available on altruistic purposes is serving a general interest purpose. Such trust should result in particular from a place of establishment or a legal representative within the Union, as well as from the requirement that registered entities have a not-for-profit character, from transparency requirements and from specific safeguards in place to protect rights and interests of data subjects and companies. Further safeguards should include making it possible to process relevant data within a secure processing environment operated by the registered entity, 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, based on 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 way of delegated acts, adopt a rulebook developed in close cooperation with data altruism organisations and relevant stakeholders, making compliance with this rulebook a requirement for registration as a recognised data altruism organisations in accordance with this Regulation.

(37) This Regulation is without prejudice to the establishment, organisation and functioning of entities that seek to engage in data altruism pursuant to national law. It builds on national law requirements to operate lawfully in a Member State as a not-for-profit organisation. Entities which meet the requirements laid down in this Regulation should be able to use the title 'data altruism organisations recognised in the Union'. In order to assist data subjects and legal entities to easily identify, and thereby to increase their trust in, data altruism organisations recognised in the Union, a common logo that is recognisable throughout the Union should be established. In order to ensure uniform conditions for the application of that logo, implementing powers should be conferred on the Commission to establish a design for that common logo. The common logo should be accompanied by a QR code with a link to the Union register of data altruism organisations recognised in the Union.

(37a) This Regulation is 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 includes open collaborative knowledge sharing platforms, open access scientific and academic repositories, open source software development platforms and Open Access content aggregation platforms.

(38) Data altruism organisations recognised in the Union should be able to collect relevant data directly from natural and legal persons or to process data collected by others. Processing of collected data can be done by data altruism organisations for purposes which they define themselves or where relevant they can permit the processing by third parties for these purposes. Where recognised data altruism organisations are data controllers or processors within the meaning of Regulation (EU) 2016/679 they are bound by the rules of that Regulation. Typically, data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(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 can be supported by consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects. Article 5(1)(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.

(38a) The competent authorities 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, and 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 the designated competent authorities. The powers and competences of the designated competent authorities 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 should seek, where relevant, an opinion or decision by the competent supervisory authority established pursuant to that Regulation.

(39) To promote trust and bring additional legal certainty and user-friendliness to granting and withdrawing of 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 performed by companies and provide a mechanism allowing such companies 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, there should be a possibility for sectoral adjustments of the European data altruism consent form.

(40) In order to successfully implement the data governance framework, a European Data Innovation Board (the 'Board') should be established, in the form of an expert group. The Board should consist of representatives of the Member States, the Commission and representatives of common European data spaces and specific sectors (such as health, environment, agriculture, transport, health, energy, industrial manufacturing, media, cultural and creative sectors, and statistics), as well as representatives of academia, research, standard setting organisations and bodies with specific expertise such as national statistical offices, where relevant.

(41) The Board should support 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 (EIF) principles and through the utilisation of European and international standards and specifications (including through the EU Multi-Stakeholder Platform for ICT Standardisation, the Core Vocabularies[29] and the CEF Building Blocks[30]), and should take into account standardisation work taking place in specific sectors or domains. Work on technical standardisation may 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 in clarifying and distinguishing which standards and practices are cross-sectoral and which are sectoral. The Board should cooperate with sectoral bodies, networks or expert groups, or other cross-sectoral organisations dealing with re-use of data. Regarding data altruism, the Board should assist the Commission in the development of the data altruism consent form, in consultation with the European Data Protection Board. By proposing guidelines on common European data spaces, the Board should support the development of a functioning European data economy based on those data spaces, as set out in the European data strategy.

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

(42a) In order to provide for an efficient enforcement of this Regulation and to ensure that providers of data intermediation services as well as entities who wish to register as recognised data altruism organisations can 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[32]. These procedures should be added to the list of procedures included in Annex II of Regulation (EU) 2018/1724.

---

29 https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies

30 https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef

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 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 2014/2012 (OJ L 295, 21.11.2018, p.1).

(43) 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 for transfers to third-countries of certain non-personal data categories deemed to be highly sensitive in specific Union acts adopted though a legislative procedure and by establishing a rulebook for recognised data altruism organisations that provides for information, technical and security requirements as well as communication roadmaps and interoperability standards with which those organisations are to comply. 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. 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.

(44) 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.

(45) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council [33] and delivered an opinion on 10 March 2021[34].

(46) This Regulation uses as its guiding principles the respect of the fundamental rights and observing the principles recognised in particular by the Charter, 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 Directive (EU) 2019/882[35] and Directive (EU) 2016/2102[36]. 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.

---

33 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).

34 EDPB-EDPS Joint Opinion on the proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act).

35 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).

36 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).

(46a) 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 establishing a notification and supervisory framework for the provision of data intermediation services and a framework for voluntary registration of entities which make data available for altruistic purposes, 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,

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;

   (ca) 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 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 specific provisions in Union or national law regarding access to or re-use of certain categories of data, in particular regarding granting of access to and disclosure of official documents. This Regulation is also without prejudice to obligations of public sector bodies under Union and national law to allow the re-use of data or to requirements related to processing of non-personal data. Where a sector-specific Union legal act or national law requires public sector bodies, providers of data intermediation services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act or national law shall also apply. Any additional requirements shall be non-discriminatory, proportionate and objectively justified.

2a. 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 shall be without prejudice to Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive 2002/58/EC, including the powers and competences of supervisory authorities. In the event of conflict between the provisions of this Regulation and Union or national law on the protection of personal data adopted in accordance with Union law, Union or national law should prevail. This Regulation does not create a legal basis for the processing of personal data and does not alter any obligations and rights set out in Regulation (EU) 2016/679 or Directive 2002/58/EC.

2b. This Regulation shall be without prejudice to the application of competition law.

2d. This Regulation is without prejudice to the competences of the Member States regarding 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 audio-visual 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;

(2c) 'data intermediation service' means a service, which aims to establish commercial relationships for the purpose of data sharing between an undetermined number of data subjects and data holders, on the one hand, and data users on the other hand, through technical, legal or other means, including for the exercise of data subjects' rights in relation to personal data. The following shall, inter alia, not be considered to be data intermediation services:

(a) services that obtain data from data holders, 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, exclusively used by one data holder in order to enable the use of data they hold, or used by multiple legal entities in a closed group, including supplier or customer relationships or contractually-defined collaborations, in particular those that have as a main objective the ensuring of functionalities of objects and devices connected to the internet-of-things;

(d) public sector bodies that offer data sharing intermediation services without aiming to establish commercial relationships for the purpose of data sharing;

(2b) 'personal data' means data as defined in point (1) of Article 4 of Regulation (EU) 2016/679;

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

(3a) ‘consent’ means consent as defined in point (11) of Article 4 of Regulation (EU) 2016/679;

(3b) 'permission' means giving data users the right to the processing of non-personal data;

(3c) 'data subject' means data subject as referred to in point (1) of Article 4 of Regulation (EU) 2016/679;

(5) ‘data holder’ means a legal person, public body, international organisation, 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;

(6) ‘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;

(7) ‘data sharing’ means the provision of data by a data subject or a data holder to a data user for the purpose of 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 licenses, for free or against remuneration;

(7a) ‘processing’ means processing as defined in point (2) of Article 4 of Regulation (EU) 2016/679;

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

(9) ‘main establishment’ of a legal person means the place of its central administration in the Union;

(9a) 'services of data cooperatives' means data intermediation services offered by an organizational structure constituted by data subjects or small and medium-sized enterprises or one-person undertakings, who are members of that structure, having as its principal object to support its members in the exercise of their rights with respect to certain data, including in making informed choices before consenting to data processing and exchanging views on data processing purposes and conditions that would best represent the interests of members in relation to their data, or in negotiating 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;

(10) ‘data altruism’ means voluntary sharing of data based on consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond a compensation related to the costs they incur making their data available, for purposes of general interest, defined in accordance with national law where applicable, such as healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics, improving public services, public policy making or scientific research purposes in the general interest;

(11) ‘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;

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

(13) ‘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 purpose 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;

(14) ‘secure processing environment’ means the physical or virtual environment and organisational means to ensuring compliance with the requirements of Regulation (EU) 2016/679, in particular data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, ensuring compliance with applicable Union and national law, and allowing the entity providing the secure processing environment to determine and supervise all data processing actions, including to display, storage, download, export of the data and calculation of derivative data through computational algorithms;

(15) 'legal representative' means a natural or legal person established in the Union explicitly designated to act on behalf of a provider of data intermediation service 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 a national competent authority instead of the provider of data intermediation service or entity with regard to the obligations of that provider of data intermediation service or entity set up under this Regulation, including to initiate enforcement proceeding against a non-compliant provider of data intermediation services or a data altruism organisation 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) protection of intellectual property rights of third parties; or

   (d) 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 national security, defence or public 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 does not create any obligation on public sector bodies to allow re-use of data nor does it release public sector bodies from their confidentiality obligations under Union or national law. This Chapter is without prejudice to Union and national law or international agreements to which the Union or Member States are parties on the protection of categories of data provided in paragraph 1. This Chapter is without prejudice to 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 object 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 otherwise not be possible.

3. An exclusive right according to 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.

5. The period of exclusivity of the right to re-use data shall not exceed 12 months. Where a contract is concluded, the duration of the contract awarded shall be as aligned with the period of exclusivity.

6. The award of an exclusive right pursuant to paragraphs (2) to (5), including the reasoned justification why it is necessary to grant such a right, shall be transparent and be made publicly available online, where relevant, in a form that is in accordance with Union law on public procurement.

7. Agreements or other practices falling within the scope of the prohibition in paragraph 1, which do not meet the conditions set out in paragraphs 2 and 3, and which were concluded before the date of entry into force of this Regulation shall be terminated at the end of the contract and in any event at the latest within thirty months after the date of entry into force of this Regulation.

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 be equipped with the necessary resources and 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. In that task, they may be assisted by the competent bodies referred to in Article 7 (1).

2. Conditions for re-use shall be non-discriminatory, transparent, proportionate and objectively justified with regard to categories of data and 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, which may include providing for the following requirements:

   (a) to only grant access to re-use data where the public sector body or the competent body, following the request to re-use, has ensured that data has been anonymised in the case of personal data, and that data has been 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 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, if remote access cannot be allowed without jeopardising the rights and interests of third parties.

5. In the case of re-use allowed according to 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 reuse of the result shall be comprehensible and transparent to the re-user.

5a. Unless national law includes specific safeguards on applicable confidentiality obligations relating to the re-use of data covered in Article 3(1), the public sector body shall make the use of data provided in accordance with paragraph 3 conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties 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. The re-user shall without undue delay, where appropriate with the assistance of the public sector body, inform the legal persons whose rights may be affected in case an unauthorised re-use of non-personal data occurs.

6. Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no legal basis for transmitting the data under Regulation (EU) 2016/679, the public sector body shall make best efforts, insofar as allowed by 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 disproportionate burden for the public sector body. In that task it may be assisted by the competent bodies referred to in Article 7 (1).

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

8a. 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 as well as of the purpose of the transfer at the time of requesting the re-use. In the case of re-use in accordance with paragraph 6, 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, and the public sector body shall not allow the re-use unless the legal person gives the 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 10b only if the re-user contractually commits to:

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

(b) accept the jurisdiction of the courts of the Member State of the transmitting public sector body as regards any dispute related to compliance with paragraphs 7 and 8.

10a. Public sector bodies shall, where relevant and to the extent of their capabilities, provide guidance and support to re-users in complying with the obligations referred to in paragraph 10. In order to support public sector bodies and re-users, the Commission may adopt implementing acts providing model contractual clauses for complying with the obligations referred to in paragraph (10) points (a) and (b). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 29 (2a)

10b. When justified by a 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 29 (2a).

11. Specific Union acts adopted in accordance with a legislative procedure 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 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 28 supplementing this Regulation by laying down special conditions applicable to the transfers to third-countries of such data.

Those conditions shall be based on the nature of non-personal data categories identified in the specific Union act and on the grounds for deeming them highly sensitive, non-discriminatory and limited to what is necessary to achieve the public policy objectives identified in the Union law act, such as safety and public health, as well as risks of re-identification of anonymized data, in accordance with the Union's international obligations.

If specific Union acts under the first subparagraph require so, such conditions may include terms applicable for the transfer or technical arrangements in this regard, limitations as regards the re-use of data in third-countries or categories of persons which are entitled to transfer such data to third countries or, in exceptional cases, restrictions as regards transfers to third-countries.

12. 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 and 11 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 they apply fees, public sector bodies shall take measures to incentivise 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 line 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 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. Fees shall be derived from the costs related to the processing of requests for re-use of the categories of data referred to in Article 3 (1). Any fees shall be limited to the necessary costs incurred for the reproduction, provision and dissemination of data, rights' clearance, costs for anonymisation or other forms or preparation of personal and confidential data as provided for in Article 5(3), costs for the maintenance of the secure processing environment, costs in relation to the acquisition of the right to permit re-use in accordance with this Chapter from third parties outside the public sector, as well as any costs in relation to supporting 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 in advance. 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 tasks mentioned in this Article, Member States shall designate one or more competent bodies, which may be sectoral, to support the public sector bodies which grant access to the re-use of the categories of data referred to in Article 3(1) in the exercise of that task. 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 set out by this Regulation.

1a. The competent bodies may also be entrusted, pursuant to Union or national law which provides for such access to be given, to grant access for the re-use of the categories of data referred to in Article 3(1). While performing their function to grant or refuse access for re-use, Articles 4, 5, 6 and 8a shall apply in regard to such competent bodies.

1b. 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).

2. The support 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;

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

(b) 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, 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;

(c) where relevant, assisting the public sector bodies to provide assistance 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 or jurisdictions 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 from re-users, where practically feasible;

(d) providing public sector bodies with assistance on the adequacy of undertakings made by a re-user, pursuant to Article 5(10).

5. The Member States shall communicate to the Commission the identity of the competent bodies designated pursuant to paragraph 1 by [date of application of this Regulation]. They shall also communicate to the Commission any subsequent modification of the identity of those bodies.

Article 8

Single information point

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 which may be linked to sectoral, regional or local information points. Functions of a single information point may be automated provided that adequate support by a public sector body is ensured. Member States may either establish a new information point or rely on an existing structure.

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 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 its re-use.

2b. 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).

2c. 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 single information points.

Article 8a

Processing of requests for re-use

1. Unless shorter time limits have been established in accordance with national law, a decision on the requests for the re-use of the categories of data referred to in Article 3(1) shall be adopted by the competent public sector bodies or the competent bodies referred to in Article 7 (1) within two months from the date of receipt of the request. In case of exceptionally extensive and complex requests this period may be extended by no more than 30 days. In such cases the applicant shall be notified as soon as possible that more time is needed to process the request and the reasons why.

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

CHAPTER III

REQUIREMENTS APPLICABLE TO DATA INTERMEDIATION SERVICES

Article 9

Data intermediation services

1. The provision of the following data intermediation services shall comply with the requirements of Article 11 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 and data users;

   (b) intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make other 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 10

Notification by data intermediation service providers

1. Any provider of data intermediation services who intends to provide the services referred to in Article 9 (1) shall submit a notification to the competent authority for data intermediation services referred to in Article 12.

2. For the purposes of this Regulation, a provider of data intermediation services 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 provider of data intermediation services that is not established in the Union, but offers the services referred to in Article 9(1) within the Union, shall designate a legal representative in one of the Member States in which those services are offered. For the purposes of ensuring compliance with this Regulation, the legal representative shall be mandated by the provider of data intermediation services to be addressed in addition to or instead of it by competent authorities 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, upon request, the actions taken and provisions put in place by the provider to ensure compliance with this Regulation. The provider of data intermediation services shall be deemed to be

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

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

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

6. The notification shall include the following information:

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

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

(c) the address of the provider of data intermediation services' main establishment in the Union, if any, and, where applicable, any secondary branch in another Member State or that of the legal representative designated pursuant to paragraph 3;

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

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

(f) a description of the service the provider intends to provide, and an indication under which of the categories under Article 9 (1) such services fall;

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

6a. The competent authority shall ensure that the notification procedure is non-discriminatory and does not distort competition.

7. At the request of the provider of data intermediation services, the competent authority for data intermediation services shall, within one week of duly and fully completed notification, issue a standardised declaration, confirming that the provider of data intermediation services has submitted the notification referred to in paragraph 4 and that the notification contains the information referred to in paragraph 6.

7a. The competent authority referred to in Article 12 shall confirm, upon the request of a provider of data intermediation services, that the provider complies with Articles 10 and 11. Upon receipt of such a confirmation, that provider may use the title 'provider of data intermediation services recognised in the Union' in its written and spoken communication, as well as a common logo. In order to ensure that providers of data intermediation services 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. Providers of data intermediation services 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 29(2).

9. The competent authority for data intermediation services shall notify the Commission of each new notification without delay by electronic means. The Commission shall keep and regularly update a public register of all providers of data intermediation services providing services in the Union, which shall make available the information referred to in points (a), (b), (c), (d) and (g) of paragraph 6, as well as in point (f) with regard to the description of the service the provider intends to provide and the categories listed in Article 9 (1) under which such services fall.

10. The competent authority for data intermediation services may charge fees for the notification, as defined by 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 authorities in relation to notifications of data intermediation services. The competent authority may also charge discounted fees or allow free of charge notification for SMEs and start-ups.

10a. Providers of data intermediation services shall submit any changes of the information provided pursuant to paragraph 6 to the competent authority within 14 days from the day on which the change takes place.

11. Where a provider of data intermediation services 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. The competent authority shall inform the Commission by electronic means of each such notification without delay. The Commission shall update the public register of the providers of data intermediation services in the Union accordingly.

Article 11

Conditions for providing data intermediation services

The provision of data intermediation services referred in Article 9(1) shall be subject to the following conditions:

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

(1a) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user may not be made dependent upon whether or to what degree the data holder or data user uses other services provided by the same provider or a related entity;

(2) the data collected with respect to any activity of a natural or legal person for the purposes 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 service, may be used only for the development of that 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;

(4) the provider shall facilitate the exchange of the data in the format in which it receives it from a data subject or a data holder and 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. The provider shall offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law;

(4a) 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, pseudonymisation. Those tools and services shall be used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context shall not use data for other purposes;

(4b) the 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 as regards prices and terms of service;

(5) the provider shall have procedures in place to prevent fraudulent or abusive practices in relation to parties seeking access through their services;

(6) the provider of data intermediation service shall ensure a reasonable continuity of provision of its services and, in the case of services which ensure storage of data, shall have sufficient guarantees in place that allow data holders and data users to obtain access to, to transfer or to retrieve their data or, in the case of providing intermediation services between data subjects and data users, allow data subjects to exercise their rights, in the case of insolvency of the provider;

(6a) the provider shall take appropriate measures to ensure interoperability with other data intermediation services, among others, by means of commonly-used open standards in the sector in which the data intermediation service providers operate;

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

(7a) the provider shall without undue delay inform data holders in case of an unauthorised transfer, access or use of the non-personal data that it has shared;

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

(10) the provider offering services to data subjects shall act in the data subjects' best interest when facilitating the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible form about intended data uses by data users and standard terms and conditions attached to such uses, before data subjects give consent;

(11) where a provider of data intermediation services provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the jurisdiction or jurisdictions outside the Union 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;

(11a) the provider shall maintain a log record of the intermediation activity.

Article 12

Competent authorities

1. Each Member State shall designate in its territory one or more authorities competent to carry out the tasks related to the notification framework for data intermediation services and shall communicate to the Commission the identity of those designated authorities by [date of application of this Regulation]. It shall also communicate to the Commission any subsequent modification.

2. The designated competent authorities for data intermediation services shall comply with Article 23.

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

Article 13

Monitoring of compliance

1. The competent authority for data intermediation services shall monitor and supervise compliance with this Chapter. The competent authority may also monitor and supervise the compliance of such data intermediation services based on the request of natural or legal persons.

2. The competent authority for data intermediation services shall have the power to request from providers of data intermediation services 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 provider of data intermediation services does not comply with one or more of the requirements of this Chapter, it shall notify that provider of those findings and give it the opportunity to state its views, within 30 days.

4. The competent authority 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 aiming to ensure compliance. In that regard, the competent authorities 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, or to initiate legal proceedings for the imposition of fines, or both;

   (b) to require a postponement in the commencement or suspension of the provision of the data intermediation service until modifications of its conditions, as requested by the competent authority, are made; or to require the cessation of the provision of the data intermediation service, in case serious or repeated infringements have not been corrected despite the prior notification or warning in accordance with paragraph (3). The competent authority for data intermediation services shall request the Commission to remove the provider of the data intermediation service from the register of providers of data intermediation services once it has ordered the cessation of the service. If a provider of data intermediation service corrects the breaches, a provider shall re-notify the competent authority. The competent authority shall notify the Commission of each new re-notification.

4a. Where a provider of data intermediation services that is not established in the Union fails to designate a legal representative or the legal representative fails, upon request of the competent authority, to provide the necessary information that comprehensively demonstrates compliance with this Regulation, the competent authority shall have the power to postpone or suspend the provision of the data intermediation service until the legal representative is designated or the necessary information is provided.

5. The competent authorities shall communicate the measures imposed pursuant to paragraph 4, the reasons on which they are based as well as the necessary steps to be taken to rectify the relevant shortcomings to the provider of data intermediation services concerned without delay and shall stipulate a reasonable period, no longer than 30 days, for the provider to comply with the measures.

6. If a provider of data intermediation services has its main establishment or legal representative in a Member State, but provides services in other Member States, the competent authority of the Member State of the main establishment or where the legal representative is located and the competent authorities of those other Member States shall cooperate and assist each other. Such assistance and cooperation may cover information exchanges between the competent authorities concerned for the purposes of their tasks under this Regulation and 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 another Member State, it shall submit a duly justified request. The competent authority for data intermediation services so requested shall, without undue delay and within a timeframe proportionate to the urgency of the request, provide a response. 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 14

Exceptions

This Chapter shall not apply to recognised data altruism organisations and other not-for-profit entities insofar as their activities consist in seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism, unless those 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 hand.

CHAPTER IV

DATA ALTRUISM

Article 14a

National arrangements for data altruism

1. Member States may have in place organisational and/or technical arrangements to facilitate data altruism. In support of this Member States may define national policies for data altruism. These national policies may in particular support 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 inform the Commission.

Article 15

Public registers of recognised data altruism organisations

1. Each competent authority for the registration of data altruism organisations designated pursuant to Article 20 shall keep and regularly update a public national register of recognised data altruism organisations.

3. The Commission shall maintain a public Union register of recognised data altruism organisations for information purposes. Only an entity registered in the public national register of recognised data altruism organisations in accordance with Article 16 may use the title 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as a common logo. In order to ensure that data altruism organisations 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 altruism organisations recognised in the Union 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 Union register of data altruism organisations recognised in the Union. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29(2).

Article 16

General requirements for registration

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

(-a) perform data altruism activities;

(a) be a legal person established pursuant to national law to meet objectives of general interest, in line with national law, where applicable;

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

(c) perform the activities related to data altruism through a structure that is functionally separate from its other activities;

(ca) comply with the rulebook adopted in accordance with Article 19a(1), at the latest by [date of entry into force of the delegated act + 18 months].

Article 17

Registration of recognised data altruism organisations

1. An entity which meets the requirements of Article 16 may request to be entered in the 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 16 and has establishments in more than one Member State, may request to be entered in the 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 in Article 16, but is not established in the Union, shall designate a legal representative in one of the Member States in which those services are offered. For the purposes 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 or data subjects and data holders, with regard to all issues related to entities. The legal representative shall cooperate with and comprehensively demonstrate to the competent authorities, upon request, the actions taken and provisions put in place by the entity 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. The designation of a representative by the entity shall be without prejudice to legal actions which could be initiated against the entity themselves. Such an entity may request to be entered in the national register of recognised data altruism organisations in that Member State.

4. Applications for registration shall contain the following information:

   (a) name of the entity;

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

   (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 designated pursuant to paragraph (3);

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

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

(i) any other documents which demonstrate that the requirements of Article 16 are met.

5. Where the entity has submitted all necessary information pursuant to paragraph 4 and after the competent authority has evaluated the application and has found that the entity complies with the requirements of Article 16, it shall register the entity in the public national register of recognised data altruism organisations within twelve weeks from the date of application. The registration shall be valid in all Member States. The competent authority for the registration of data altruism organisations shall communicate any registration to the Commission, which shall include that registration in the 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 public national register of recognised data altruism organisations.

7. Any entity entered in a national register of recognised data altruism organisations shall notify the competent authority for the registration of data altruism organisations of any changes of the information provided pursuant to paragraph 4 within 14 days from the day on which the change takes place. The competent authority shall inform the Commission by electronic means of each such notification without delay. Based on such notification, the Commission shall update the Union register of recognised data altruism organisations without delay.

Article 18

Transparency requirements

1. Any entity entered in a public national register of recognised data altruism organisations shall keep full and accurate records concerning:

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

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

(c) the purpose of such 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. Any entity entered in a public national register of recognised data altruism organisations shall draw up and transmit to the relevant competent national 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 entity;

(b) a description of the way in which the general interest purposes 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 general interest purposes 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 entity, where applicable;

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

Article 19

Specific requirements to safeguard rights and interests of data subjects and data holders as regards their data

1. Any entity entered in the public national register of recognised data altruism organisations shall inform data holders or data subjects prior to any processing of their data in a clear and easy-to-understand manner:

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

(b) about the location of and the objectives of general interest for which it permits any processing performed outside the Union, in case the processing is performed by the entity entered in a national register of recognised data altruism organisations itself.

2. The entity shall not use the data for other objectives than those of general interest for which the data subject or data holder permits the processing. The entity shall not use misleading marketing practices to solicit provision of data.

2a. The entity shall provide tools for obtaining consent from data subjects or permissions to process data made available by data holders. The entity shall also provide tools for easy withdrawal of such consent or permission.

2b. The entity 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.

2c. The entity shall without undue delay inform data holders in case of an unauthorised transfer, access or use of the non-personal data that it has shared.

3. Where the entity 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 jurisdiction or jurisdictions outside the Union in which the data use is intended to take place.

Article 19a

Rulebook

1. The Commission shall adopt delegated acts in accordance with Article 28, supplementing this Regulation by establishing a rulebook, laying down:

   (a) appropriate information requirements to ensure that data holders and data subjects 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 the giving and withdrawal of the consent, 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 obtaining and withdrawing consent and 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 20

Competent authorities for the registration of data altruism organisations

1. Each Member State shall designate one or more competent authorities responsible for the public national register of recognised data altruism organisations and for the monitoring of compliance with the requirements of this Chapter. The designated competent authorities for the registration of data altruism organisations shall meet the requirements of Article 23.

2. Each Member State shall inform the Commission of the identity of their designated competent authorities for the registration of data altruism organisations.

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 bodies of that Member State.

Article 21

Monitoring of compliance

1. The competent authority for the registration of data altruism organisations shall monitor and supervise compliance of entities entered in its public national register of recognised data altruism organisations with the conditions laid down in this Chapter. The competent authority for the registration of data altruism organisations may also monitor and supervise the compliance of such entities based on the request of natural or legal persons.

2. The competent authority shall have the power to request information from entities included in its public national register of recognised data altruism organisations that is necessary to verify compliance with the provisions 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 finds that an entity does not comply with one or more of the requirements of this Chapter it shall notify the entity of those findings and give it the opportunity to state its views, within 30 days.

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

5. If an entity 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, the entity shall:

   (a) lose its right to refer to itself as a 'data altruism organisation recognised in the Union' in any written and spoken communication, such decision shall be made public;

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

6. If an entity included in a public national register of recognised data altruism organisations has its main establishment or legal representative in a Member State but is active in other Member States, the competent authority of the Member State of the main establishment or where the legal representative is located and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and reasoned requests to take the supervisory measures referred to in this Article. Where a competent authority in one Member State requests assistance from another Member State, it shall submit a duly justified request. The competent authority shall, upon such a request, provide a response without undue 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 22

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 consultation of 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 across Member States in a uniform format. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29(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 23

Requirements relating to competent authorities

1. The competent authorities designated pursuant to Article 12 and Article 20 shall be legally distinct from, and functionally independent of any provider of data intermediation services or entity included in the public national register of recognised data altruism organisations. The functions of the competent authorities designated pursuant to Article 12 and Article 20 may be performed by the same entity. Member States may either establish one or more new entities or rely on existing ones.

2. Competent authorities shall exercise their tasks in an impartial, transparent, consistent, reliable, and timely manner and shall, in the exercise of their tasks, safeguard fair competition and non-discrimination.

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

4. Top-management and personnel of the competent authorities shall not engage in any activity that may conflict with their independence of judgment or integrity in relation to evaluation activities entrusted to them.

5. The competent authorities 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 of a Member State shall provide the Commission and competent authorities from other Member States, on reasoned request and without undue delay, with the information necessary to carry out their tasks under this Regulation. Where a national competent authority considers the information requested to be confidential in accordance with Union and national rules on commercial and professional confidentiality, the Commission and any other competent authorities concerned shall ensure such confidentiality.

Article 24

Right to lodge a complaint

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

2. The competent authority with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken, and shall inform the complainant of the remedies provided for in Article 25.

Article 25

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:

   (b) legally binding decisions of the competent authorities referred to in Articles 13, 17 and 21 taken in the management, control and enforcement of the notification regime for providers of data intermediation services and the monitoring of entities entered into a public national register of recognised data altruism organisations.

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

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

CHAPTER VI

EUROPEAN DATA INNOVATION BOARD

Article 26

European Data Innovation Board

1. The Commission shall establish a European Data Innovation Board ("the Board") in the form of an Expert-Group, consisting of representatives of the competent authorities of all Member States pursuant to Article 12 and Article 20, 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. When appointing individual experts the Commission shall aim to achieve a gender and geographical balance in the composition of the expert group.

1a. The Board shall consist of at least three sub-groups: a sub-group composed of the competent authorities referred to in Article 12 and Article 20, with a view of carrying out the tasks pursuant to Article 27 point (a), (b), (e) and (ea); a sub-group for technical discussions on standardisation, portability and interoperability pursuant to Article 27 point (c) and (d); a sub-group for stakeholder involvement composed of relevant representatives from industry, research, academia, civil society, standardisation organisations, relevant common European data spaces and other relevant stakeholders or third parties advising the Board on tasks (bc), (bd), (c), (d) and (da) pursuant to Article 27.

3. The Commission shall chair the meetings of the Board.

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

Article 27

Tasks of the Board

The Board shall have the following tasks:

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

(aa) advise and assist the Commission in developing a consistent practice for data altruism across the Union;

(b) advise and assist the Commission in developing a consistent practice of the competent authorities referred to in Article 12 and Article 20 in the application of requirements applicable to data intermediation service providers and entities performing activities related to data altruism, respectively;

(bc) advise and assist the Commission in 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 IP theft or industrial espionage;

(bd) advise and assist the Commission in developing consistent guidelines for cybersecurity requirements for the exchange and storage of data;

(c) 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 regards to sectoral requirements for security, access procedures, while taking into account sector-specific standardisations activities, and in particular in clarifying and distinguishing which standards and practices are cross-sectoral and which are sectoral;

(d) 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 and 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;

(da) propose guidelines for 'common European 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 regards to sectoral requirements for security, access procedures, while taking into account sector-specific standardisations activities, in particular in 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 legal data transfers outside the Union, including safeguards against any transfers prohibited by Union law;

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

(v) adherence to cybersecurity requirements in line with Union law.

These ‘common European data spaces’ mean purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives. Such common standards and practices shall take into account existing standards, comply with the competition rules and ensure non-discriminatory access for all participants, for the purpose of facilitating data sharing in the Union and reaping the potential of existing and future data spaces.

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

(e) facilitate cooperation between competent authorities referred to in Article 12 and Article 20 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 service providers and the registration and monitoring of recognised data altruism organisations, including coordination regarding the setting of fees or penalties, as well as facilitate cooperation between competent authorities regarding international access and transfer of data;

(eb) advise and assist the Commission in developing the European data altruism consent form in accordance with Article 22(1);

(ed) advise the Commission on improving the international regulatory environment for non-personal data including standardisation;

(ea) advise and assist the Commission in evaluating whether implementing acts in accordance with Articles 5(10a) and 5(10aa) should be adopted.

CHAPTER VII

COMMITTEE AND DELEGATION

Article 28

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(11) and Article 19a(1) shall be conferred on the Commission for an indeterminate period of time from […].

3. The delegation of power referred to in Article 5(11) and Article 19a(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(11) and Article 19a(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 29

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.

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

CHAPTER VIII

FINAL PROVISIONS

Article 30

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 2, the data intermediation service provider or the entity entered in a national register of recognised data altruism organisations, as the case may be, 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 governmental access would create a conflict with Union law or national law of the relevant Member State, without prejudice to paragraph 2 or 3.

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

3. In the absence of such an international agreement, where a public sector body, a natural or legal person to which the right to re-use data was granted under Chapter 2, a data intermediation service provider or entity entered in a national register of recognised data altruism organisations is the addressee of a decision of a court or of an administrative authority of a third country to transfer from 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 national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only:

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

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

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

4. If the conditions 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 2, the data intermediation service provider or the entity entered in a national register of recognised data altruism organisations, as the case may be, 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 2, the data intermediation service provider and the entity entered in a national register of recognised data altruism organisations shall inform the data holder about the existence of a request of an administrative authority in a third-country to access its data before complying with this request, except in cases where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

Article 31

Penalties

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 (12) and Article 30, the obligation of data intermediation service providers to notify pursuant to Article 10, the conditions for providing services pursuant to Article 11, conditions for the registration as a recognised data altruism organisation pursuant to Articles 18 and 19 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 … [date of application of this Regulation] notify the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.

Member States shall take into account the following non-exhaustive and indicative criteria for the imposition of penalties on providers of data intermediation services and 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 provider of data intermediation services or data altruism organisation to mitigate or remedy the damage caused by the infringement;
(c) any previous infringements by the provider of data intermediation services or data altruism organisation;
(d) the financial benefits gained or losses avoided by the provider of data intermediation services or data altruism organisation due to the infringement, insofar as such gains or losses can be reliably established;
(e) any other aggravating or mitigating factors applicable to the circumstances of the case.

Article 32

Evaluation and review

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

(a) the application and functioning of the rules on penalties laid down by the Member States pursuant to Article 31;
(b) the level of compliance of the legal representatives of providers of data intermediation services and data altruism organisations not established in the Union with this Regulation and the level of enforceability of penalties on those providers and organisations;
(c) the type of data altruism organisations registered under Chapter IV and overview of the purposes 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. The report shall be accompanied, where necessary, by legislative proposals.

Article 33

Amendment to Regulation (EU) No 2018/1724

In Annex II to Regulation (EU) No 2018/1724, the following information is added to "Starting, running and closing a business":

Starting, running and closing a business

Notification as a provider of data intermediation services

Confirmation of the receipt of notification

Registration as a data altruism organisation recognised in the Union

Confirmation of the registration

Article 34

Transitional arrangements

Entities providing the data intermediation services provided for in Article 9(1) on …[date of entry into force of this Regulation] shall comply with the obligations set out in Chapter III by [24 months after the date of application of this Regulation] .

Article 35

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

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

Done at Brussels,

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