



Council of the European Union
General Secretariat

Brussels, 28 May 2021

Interinstitutional files:
2020/0340(COD)

WK 7112/2021 INIT

REDACTED DOCUMENT ACCESSIBLE TO
THE PUBLIC (28.02.2025). ONLY MARGINAL
PERSONAL DATA HAVE BEEN REDACTED.

LIMITE

TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Data Governance Act : PL comments (doc. 8894/21)

Delegations will find in annex PL comments on the 3rd Presidency compromise text. (doc. 8894/21)



Council of the
European Union

Brussels, 19 May 2021
(OR. en)

8894/21

LIMITE

TELECOM 214
COMPET 372
MI 362
DATAPROTECT 132
JAI 564
CODEC 726

Interinstitutional File:
2020/0340(COD)

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	7111/21
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) - Presidency compromise text

I. INTRODUCTION

1. The proposal for a Regulation on European Data Governance (Data Governance Act) and the related Impact Assessment were presented by the Commission in the WP TELECOM towards the end of the DE Presidency. The proposal was also discussed during the informal video conference of Telecom Ministers on 7 December 2020.
2. Under the PT Presidency, several discussions on the proposal were held in the WP TELECOM throughout January and February, with the first compromise proposal presented in the WP TELECOM on 25 February 2021.
3. Based on the subsequent discussions in the Working Party, which took place throughout March and early April, the written comments received from the delegations, and the Joint Opinion of the EDPB-EDPS, the Presidency prepared the second compromise proposal, which was presented in the WP TELECOM meeting on 13 April.

4. Following another round of discussions in the Working Party, as well as based on the feedback received from the delegations in the written comments and during two workshops organised by the Presidency in April and May, the Presidency has prepared the third compromise proposal, contained in the Annex of this document. The Presidency invites the delegations to discuss the document in the WP TELECOM meeting on 20 May 2021.
5. Changes in the document as compared with the Commission's proposal are marked as follows: new text is indicated with **bold**, and deletions with ~~strike through~~. Changes as compared with the second Presidency compromise (doc. 7111/21) are underlined.

II. MAIN CHANGES

1. Scope and definitions (Chapter I)

- a) In **Article 1(2)** the reference to personal data was deleted because the text now contains a separate **Article 1(3)** where non-prejudice to personal data legislation is included.
- b) In **Article 2(2a)** the term 'data sharing service provider' was replaced with 'data intermediation service', and this change was applied throughout the whole text of the proposal. The definition was also further clarified. The purpose of this change is to make it clear that these new actors do not share data themselves but only provide an intermediation service to entities wishing to engage in data sharing. For further clarity on the scope, a non-exhaustive list of entities that are not considered to be data intermediation services for the purposes of the DGA was included.
- c) In **Article 2(3aa)** the definition of 'permission' was added to complement the definition of 'consent' and to account for situations where a legal person allows another natural or legal person to process non-personal data as well personal data insofar as there is an appropriate legal basis for such a permission.
- d) The definition in **Article 2(5)** has been modified to further clarify the characteristics of a data holder.

2. Reuse of certain categories of protected data held by public sector bodies (Chapter II)

- a) The previous **Article 5(5)** was split into a shorter **Article 5(5)** and the new **Article 5(5a)**, with the text of the previous **Article 5(5a)** moved up to the new **Article 5(5a)**. The aim is to separate clearly the provisions on the integrity of the functioning of the technical systems of the secure processing environment from the provisions on the requirement for the re-user to adhere to a confidentiality obligation and to assess on an on-going basis the risks of re-identification of any data subject.
- b) In **Article 5(10a)** an important clarification was made that the provision covers situations where there is a substantial number of cases across the Union concerning the re-use of non-personal data in specific third countries. Moreover, the reference to the examination procedure concerning implementing acts was corrected.
- c) In **Article 6(5)** the last sentence on the criteria and methodology for calculating fees was moved to **Article 6(6)**.

3. Requirements applicable to data sharing services (Chapter III)

- a) **Article 9(2)** was deleted because it was a duplication of non-prejudice provisions which are already included in **Article 1**.
- b) In **Article 11** a new **point (12)** was added in order to indicate that providers of data intermediation services are obliged to maintain a record of their intermediation activities.
- c) In **Article 12(3)** the last sentence was deleted and moved to **Recital 33**, due to the fact that non-prejudice provisions concerning the GDPR are already included in **Article 1(3)**.
- d) In **Article 13(3)** the reference to 'a reasonable time limit' was replaced with a deadline of 30 days to ensure consistency in the application of this provision, as well as consistency with the equivalent provision in **Article 21(3)**.
- e) **Article 14 point (b)** a reference to recognised data altruism organisations was added to make it clear that they are not covered by the provisions of Chapter III.

4. Data altruism (Chapter IV)

- a) In Chapter IV **Article 14a(1)** was modified to indicate the voluntary nature of national altruism policies, with the requirement added for the Member States to put in place organisational and/or technical arrangements to facilitate data altruism.
- b) The changes introduced in **Article 15(1), (2) and (3)** are meant to clarify the difference between the roles of the registers of recognised data altruism organisations maintained by the competent authorities for the registration of data altruism organisations and the respective Union register maintained by the Commission.
- c) In **Article 16** the requirement that a structure through which a data altruism organisation performs the activities related to data altruism should be legally separate from its other activities was replaced with the requirement for a functional separation.
- d) In **Article 20(3)** the last sentence was deleted and moved to **Recital 38a**, due to the fact that non-prejudice provisions concerning the GDPR are already included in **Article 1(3)**. This change mirrors the equivalent change introduced in **Article 12(3)**.

5. Competent authorities and procedural provisions (Chapter V)

- a) The previous **point (a)** in **Article 25(1)** was moved to the new **Article 25(3)** and it now contains a clarification on the right to an effective judicial remedy or access to review by an impartial body in cases where a competent authority referred to in Article 12 or 20 fails to act on a complaint.

6. European Data Innovation Board (Chapter VI)

- a) In **Article 26** a new point **(1a)** was added to indicate that the European Data Innovation Board should consist of at least one sub-group composed of the competent authorities and at least one sub-group responsible for technical discussions on standardisation and interoperability.

7. Final provisions (Chapter VIII)

- a) In **Article 30(3)** the last sentence was deleted because the requirement to provide an opinion on whether conditions concerning transfers of non-personal data to third countries are met would be too burdensome for the relevant competent bodies or authorities.
- b) In **Article 31** further clarification was provided on which infringements should be subject to penalties as provided for in this article.

6. Other changes (Recitals)

- a) In **Recital 3** it was clarified that in the case of mixed data sets, the provisions of the GDPR should prevail, in line with a similar provision in the Free Flow of Data Regulation.
- b) A new **Recital 18a** was added in order to indicate that adequate safeguards for strategic and sensitive data should be provided, inter alia, through adherence to the relevant technical standards, codes of conduct and certifications at Union level.
- c) The new text at the end of **Recital 22** was added to provide further clarification on the characteristics of data intermediation services.
- d) The new **Recital 22a** was split from the previous **Recital 22** for greater clarity. Consequently there is now a separate recital that lists clearly which entities are covered by the provisions of Chapter III of the proposal and which ones are not.
- e) The new text in **Recitals 25 and 36** was added to indicate that the Commission should encourage and facilitate the development of self-regulatory codes of conduct at Union level, respectively for data intermediation services and for data altruism organisations.
- f) In **Recital 26** some examples were added of ancillary services facilitating the sharing of data that may be provided by data intermediation service providers.
- h) In **Recital 35** it was clarified that in certain data altruism situations compensation for data subjects may be envisaged, namely when they incur costs while making their data available for objectives of general interest.
- i) In **Recital 40** some more clarifications concerning the composition of the European Data Innovation Board were added.

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 Committee¹,

Having regard to the opinion of the Committee of the Regions²,

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.

¹ OJ C , , p. .

² OJ C , , p. .

- (2) Over the last few years, 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 for citizens **and the economy**, for example through improved personalised medicine, new mobility, and its contribution to the European Green Deal³. In its Data Strategy⁴, 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. 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 European Union, in line with international obligations. 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**.
- (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 requirements for data governance**. 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 space⁵ 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 data⁶. This Regulation is therefore without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council⁽⁷⁾, and in particular the implementation of this Regulation shall not prevent cross border transfers of data in accordance with Chapter V of Regulation (EU) 2016/679 from taking place, Directive (EU) 2016/680 of the European Parliament and of the Council⁽⁸⁾, Directive (EU) 2016/943 of the European Parliament and of the Council⁽⁹⁾, Regulation (EU) 2018/1807 of the European Parliament and of the Council⁽¹⁰⁾,

³ Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Green Deal. Brussels, 11.12.2019. (COM(2019) 640 final)

⁴ COM (2020) 66 final.

⁵ 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).

⁶ 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.

⁷ 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)

⁸ 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)

⁹ 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)

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

Regulation (EC) No 223/2009 of the European Parliament and of the Council⁽¹¹⁾, Directive 2000/31/EC of the European Parliament and of the Council⁽¹²⁾, Directive 2001/29/EC of the European Parliament and of the Council⁽¹³⁾, Directive (EU) 2019/790 of the European Parliament and of the Council⁽¹⁴⁾, Directive 2004/48/EC of the European Parliament and of the Council⁽¹⁵⁾, Directive (EU) 2019/1024 of the European Parliament and of the Council⁽¹⁶⁾, as well as Regulation 2018/858/EU of the European Parliament and of the Council⁽¹⁷⁾, Directive 2010/40/EU of the European Parliament and of the Council⁽¹⁸⁾ and Delegated Regulations adopted on its basis, **Directive 2007/2/EC of the European Parliament and of the Council¹⁹, Directive (EU) 2017/1132 of the European Parliament and of the Council²⁰**, 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 international cooperation in the context 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 is not covered by this Regulation. This includes 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 sharing 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 sharing intermediation services or

- ¹¹ 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)
- ¹² 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)
- ¹³ 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)
- ¹⁴ 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)
- ¹⁵ 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).
- ¹⁶ 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).
- ¹⁷ 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).
- ¹⁸ 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)
- ¹⁹ **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).**
- ²⁰ **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).**

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, to Directive 2002/58/EC of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and of the Council ⁽²¹⁾. 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. 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 on the protection of personal data, the latter should prevail. Data protection authorities may be competent authorities under this Regulation. Where other organisations 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 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 over data and** in order to address ~~the other~~ barriers to a well-functioning data-driven economy and to create a Union-wide governance framework for data access, **control** and use, in particular regarding the re-use of certain types of data held by the public sector, the provision of services by data ~~sharing~~ **intermediation service** providers 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. **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** ~~generated~~ 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 not accessible on the basis of specific national or Union legislation, such as Regulation (EU) 2016/679 and Directive (EU) 2016/680) in public databases is often not made available, not even for research or innovative activities. Due to the sensitivity of this data, certain technical and legal procedural requirements must be met before they are made available, in order to ensure the respect of rights others have over such data. 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.

²¹ 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)

- (6) There are techniques enabling privacy-friendly analyses on databases that contain personal data, such as anonymisation, pseudonymisation, differential privacy, generalisation, or suppression, ~~and~~ randomisation, and use of synthetic data or other such methods. Application of these privacy-enhancing technologies, together with comprehensive data protection approaches, **in line with the rules on personal data processing**, should ensure the safe re-use of **certain categories of protected data, for example** personal data and 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 ⁽²²⁾. **The public sector body may impose a condition whereby the re-use is restricted to machine-processing of data or to processing with limited human involvement. ~~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. ~~This Regulation should not be read as creating a new legal basis for the processing of personal data.~~
- (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 for 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 applies to p**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) 2016/943²³, which sets the framework for the lawful acquisition, use or disclosure of trade secrets. **This Regulation does not create an obligation to allow re-use of public sector data. This Regulation**It is 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.
- (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, ~~for which intellectual property rights are not incidental, but which are predominantly contained in works and other documents protected by such intellectual property rights~~, are not covered by this Regulation **since the works and other documents they hold are predominantly covered by third party**

²² 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).

²³ OJ L 157, 15.6.2016, p. 1–18.

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 are also not covered by this Regulation. Where relevant, Member States may decide to apply the requirements of this Regulation to public undertakings or private undertakings, such as those that exercise public sector duties or provide services of general interest. The exchange of data between public sector bodies and public sector bodies in third countries or international organizations, purely in pursuit of their public tasks, 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 as far as possible 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 an advanced digital service in the general interest. Such arrangements should, however, be concluded in compliance with public procurement 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 three years. In order to ensure transparency, such exclusive agreements should be published online **two months before entry into force**, regardless of a possible publication of an award of a public procurement contract. **Where an exclusive right to re-use data does not meet the conditions set out in this Regulation, the exclusive right shall be invalid.**
- (10) Prohibited exclusive agreements and other practices or arrangements between data **subjects and data holders on the one hand**, and data re-users **on the other hand**, 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 three years from the date of entry into force of this Regulation.
- (11) Conditions for re-use of protected data that apply to public sector bodies 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, proportionate and objectively justified, while not restricting competition. **The conditions for re-use should be designed in a manner promoting scientific research, e.g. privileging research should be considered non-discriminatory. In particular, 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. 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 ~~effort-burden~~ for the public sector. Depending on the case at hand, before its transmission, personal data should be fully anonymised, so as to definitively 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~~ **Alternatively**, on-premise or remote re-use of the data within a secure processing environment could be permitted. 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 the Regulation (EU) 2016/679 allows such transmission. **This also applies to pseudonymised data which remain personal data in the sense of Regulation (EU) 2016/679. In the event of reidentification of data subjects, the obligation to ~~report~~ notify such a data breach to the public sector body should apply in addition to the obligation to ~~report~~ notify such a data breach to a supervisory authority and to the data subject in accordance with Regulation (EU) 2016/679.** ~~The public sector body could make the use of such secure processing environment conditional on the signature by the re-user of a confidentiality agreement 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.~~ 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~~ **could** support 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 companies 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 such a request.**

- (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 ~~beyond the boundaries set by this Regulation~~. 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 rightholder. 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 ⁽²⁴⁾ 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 take fully into account the rights and interests of natural and legal persons (in particular the protection of personal data, commercially sensitive data and the protection of intellectual property rights) in case such data is transferred to third countries.
- (15) Furthermore, it is important to **safeguard** protected ~~commercially sensitive~~ data of non-personal nature, notably 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 fundamental rights or interests of **data subjects and 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, should be transferred only to third-countries where appropriate safeguards for the use of data are provided. Such appropriate safeguards should be considered to exist 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 or national 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 that declare that a third country provides a level of protection that is essentially equivalent to those provided by Union or national law. 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 concerning 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~~ **data subjects and data holders**, public sector bodies or ~~data sharing 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.
- (16) In cases where there is no implementing act adopted by the Commission in relation to a third country declaring that it provides a level of protection, in particular as regards the protection of commercially sensitive data and the protection of intellectual property rights, which is essentially equivalent to that provided by Union or national law, the public sector body should only transmit 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

²⁴ 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).

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.

- (17) Some third countries adopt laws, regulations and other legal acts which aim at directly transferring or providing access to non-personal data in the Union under the control of natural and legal persons under the jurisdiction of the Member States. **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 with the law of the Union or the law of the relevant Member State.** 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 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 under certain conditions, in particular that the third-country 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 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.
- (18) 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 ~~sharing~~ **intermediation service** providers and entities entered in the 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.
- (18a) To foster further trust in the data economy of the Union, it is essential that adequate safeguards are provided to Union citizens, the public sector and businesses that ensure that control over their strategic and sensitive data is guaranteed and that Union legislation, values and standards are upheld in terms of , but not limited to, security, data protection and consumer protection. To that end, 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 the 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 **will** have been identified as highly sensitive **in 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, telecommunications 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~~ **implementing** acts. Conditions should be proportionate, non-discriminatory and necessary to protect legitimate public policy objectives identified, such as the protection of public health, ~~public order~~, 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 ~~make the data available~~ **allow re-use** at lower or no cost, for example for certain categories of re-uses such as non-commercial re-use, ~~for scientific research purposes~~, or re-use by small and medium-sized enterprises, 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 reasonable, transparent, published online and non-discriminatory.
- (21) In order to incentivise the re-use of these categories of data, Member States should establish a single information point to act as the primary 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 may 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 may be used for this purpose.** 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 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 ~~holders~~ **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, d**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 in the sense 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 may act as competent bodies.**

- (22) Providers of data ~~sharing~~ **intermediation** services (data intermediaries) are expected to play a key role in the data economy, **in particular in supporting voluntary data sharing practices between companies or data sharing arrangements set by union or national law. They could become a** as a tool to facilitate the aggregation and exchange of substantial amounts of relevant data. Data intermediaries 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 intermediaries that are independent from both data **subjects and data** holders, and **from** data users, can have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power. **Data intermediation services may 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 a specific infrastructure for the interconnection of data holders and data users.**

- (22a)** This Regulation should only cover **entities that provide information society services within the meaning of Article 1(1)b of Directive (EU) 2015/1535 and which providers of data sharing services** that have as a main objective the establishment of a business, a legal and/or potentially also technical relation between ~~data holders, including data subjects and data holders~~, on the one hand, and potential users on the other hand, and assist both parties in a transaction of data assets between the two. It should only cover services aiming at intermediating between an ~~indefinite undefined~~ number of data **subjects and data holders, on the one hand, holders and data users on the other hand, excluding data sharing** **intermediation** services that are meant to be used by a closed group of data **subjects and data** holders, and users. Providers of cloud services should be excluded, as well as service providers that obtain data from data ~~holders subjects and data holders~~, aggregate, enrich or transform the data and licence the use of the resulting data to data users, without establishing a direct relationship between data ~~holders subjects and data holders, on the one hand,~~ and data users **on the other hand**, for example advertisement or data brokers, data consultancies, providers of data products resulting from value added to the data by the service provider. At the same time, data ~~sharing intermediation~~ service providers should be allowed to make adaptations to the data exchanged, to the extent that this improves the usability of the data by the data user, where the data user desires this, such as to convert it into specific formats. In addition, services that focus on the intermediation of content, in particular on 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. Data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms, developed **and exclusively offered by manufacturers in the context** of objects and devices connected to the Internet-of-Things, ~~which that~~ have as their main objective to ensure functionalities of the connected object or device and ~~to~~ allow value added services, should not be covered by this Regulation. ‘Consolidated tape providers’ in the sense of Article 4 (1) point 53 of Directive 2014/65/EU of the European Parliament and of the Council²⁵ as well as ‘account information service providers’ in the sense of Article 4 point 19 of Directive (EU)

²⁵ 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 173/349.

2015/2366 of the European Parliament and of the Council²⁶ should not be considered as data sharing intermediation service providers for the purposes of this Regulation. **Public sector bodies that offer data sharing intermediation service facilities on a non-commercial basis are not covered by Chapter III of this Regulation.** Entities which restrict their activities to facilitating use of data made available on the basis of data altruism and that operate on a not-for-profit basis should not be covered by Chapter III of this Regulation, as this activity serves objectives of general interest by increasing the volume of data available for such purposes.

- (23) A specific category of data intermediaries includes providers of data sharing intermediation services that offer their services to data subjects in the sense of Regulation (EU) 2016/679. Such providers ~~focus exclusively on personal data and~~ seek to enhance individual agency, and **in particular** the individuals' control over the data ~~pertaining~~ **relating** to them. They would assist individuals in exercising their rights under Regulation (EU) 2016/679, in particular managing 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 make more data 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.
- (24) Data cooperatives seek 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 or potentially solving disputes between members of a group on how data can be used when such data pertain to several data subjects within that group. In this context it is important to acknowledge that the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data cooperative. Data cooperatives could also provide a useful means for one-person companies, micro, small and medium-sized enterprises that in terms of knowledge of data sharing, are often comparable to individuals.
- (25) In order to increase trust in such data sharing intermediation services, in particular related to the use of data and the compliance with the conditions imposed by data ~~holders~~ **subjects and data holders**, it is necessary to create a Union-level regulatory framework, which would set out highly harmonised requirements related to the trustworthy provision of such data sharing intermediation services, **and which would be implemented by the national competent authorities.** This will contribute to ensuring that data **subjects and data holders, as well as** ~~and~~ data users, have better control over the access to and use of their data, in accordance with Union law. **The Commission should also encourage and facilitate the development of self-regulatory codes of conduct at Union level, involving relevant stakeholders.** Both in situations where data sharing occurs in a business-to-business context and where it occurs in a business-to-consumer context, data sharing intermediation service providers should offer a novel, 'European' way of data governance,

²⁶ 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.

by providing a separation in the data economy between data provision, intermediation and use. Providers of data sharing intermediation services may also make available specific technical infrastructure for the interconnection of data ~~holders~~ **subjects and data holders** ~~and with~~ data users.

- (26) A key element to bring trust in data sharing intermediation services and more control for data ~~holder~~ **subjects and data holders**, ~~as well as for and~~ data users, in data sharing services is the neutrality of data sharing intermediation service providers as regards the data exchanged between data ~~holders~~ **subjects and data holders**, ~~on the one hand~~, and data users ~~on the other hand~~. It is therefore necessary that data sharing intermediation service providers act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose. This will also require structural separation between the data sharing intermediation service and any other services provided, so as to avoid issues of conflict of interest. This means that the data sharing intermediation service should be provided through a legal ~~entity~~ **person** that is separate from the other activities of that data sharing intermediation service provider. ~~As an exception to this, the data sharing intermediation service providers may use the data for which they provide sharing services for the improvement of their services provided by the data holder for the improvement of their data intermediation services.~~ In addition to that the providers may offer additional specific services to improve the usability of the data and ancillary services that facilitate the sharing of data, such as storage, aggregation, curation, pseudonymisation and anonymisation. Data sharing intermediation service providers that intermediate the exchange of data between individuals as data ~~holders~~ **subjects** and legal ~~persons~~ **entities as data users** should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data ~~holders~~ **subjects**. Questions of liability for all material and immaterial damages and detriments resulting from any conduct of the data sharing intermediation service provider should be addressed in the relevant contract, based on the national liability regimes.
- (26a) Data sharing 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 the data service provider operates. The European Data Innovation Board should facilitate the emergence of additional industry standards, where necessary. Data sharing intermediation service providers should implement in due time the measures for interoperability between the data sharing intermediation services set out by the European Data Innovation Board.
- (27) In order to ensure the compliance of the providers of data sharing intermediation services with the conditions set out in this Regulation, such providers should have a place of establishment in the Union. Alternatively, where a provider of data sharing intermediation services not established in the Union offers services within the Union, it should designate a representative. Designation of a representative is necessary, given that such providers of data sharing intermediation services handle personal data as well as commercially confidential data, which necessitates the close monitoring of the compliance of such service providers with the conditions laid out in this Regulation. In order to determine whether such a provider of data sharing intermediation services is offering services within the Union, it should be ascertained whether it is apparent that the provider of data sharing 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 sharing intermediation services, or the use of a language generally used in the third country where the provider of data sharing 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, may make it apparent that the provider of data sharing intermediation services is planning to offer services within the Union. The representative should act on behalf of the provider of data sharing intermediation services and it should be possible for competent authorities to contact the representative. The representative should be designated by a written mandate of the provider of data sharing 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 sharing 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 sharing intermediation services process personal data, this Regulation does not affect the protection of personal data.** Where the data sharing intermediation service providers are data controllers or processors in the sense of Regulation (EU) 2016/679 they are bound by the rules of that Regulation. This Regulation should be also without prejudice to the application of competition law.
- (29) Providers of data sharing intermediation services should also take measures to ensure compliance with competition law **and have procedures in place to this effect.** Data sharing may generate various types of efficiencies but may also lead to restrictions of competition, in particular where it includes the sharing of competitively sensitive information. 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.
- (30) A notification procedure for data sharing 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 sharing intermediation services, but without requiring any explicit decision or administrative act by the competent authority for the provision of such services.
- (31) In order to support effective cross-border provision of services, the data sharing intermediation service provider 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 the information set out in this Regulation.
- (32) The main establishment of a provider of data sharing 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 sharing 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 sharing 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 sharing 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 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 are 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 ~~sharing~~ **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 consent or, where it concerns non-personal data, made available by legal persons, for ~~purposes~~ **objectives** of general interest. Such ~~purposes~~ **objectives** would include healthcare, combating climate change, improving mobility, facilitating **the development, production and dissemination of European statistics** ~~the establishment of official statistics~~ or improving the provision of public services. Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well ~~purposes~~ **objectives** of general interest. This Regulation aims 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. ~~Data subjects may receive compensation related to the necessary costs they incur making their data available for objectives of general interest.~~
- (36) Legal entities that seek to support ~~purposes~~ **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, and this should facilitate cross-border data use within the Union and the emergence of data pools covering several Member States. Data subjects in this respect would consent to specific purposes of data processing, but could also consent to data processing in certain areas of research or parts of research projects as it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. 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 ~~voluntary~~ 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 to ensure that the data controller maintains high standards of scientific ethics, effective 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 encourage and facilitate the development of self-regulatory codes of conduct at Union level, involving relevant stakeholders.**

Commented [1]: Although the added sentence does not entail an obligation to compensate but only creates such a possibility, its absence would not change the legal situation in this respect. Crossing out this clarification still means both directions (with or without payment) are allowed.
On the other hand, keeping this addition may generate far-reaching implications as far as data holders' requests are concerned and may affect future EU legal regulations regarding access to data from private sources, in particular Data Act. This situation in relation to data used "for public good" is not the desired effect.

- (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 in this Regulation should be able to use the title of ‘Data Altruism Organisations recognised in the Union’.
- (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. **Where Data Altruism Organisations are data controllers or processors in the sense 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) and in compliance with requirements for lawful consent in accordance with Article 7 of Regulation (EU) 2016/679. 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 in this Regulation should be chosen on the basis of their capacity and expertise, and they should be independent 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 are 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 bring additional legal certainty 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 could also 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 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 relevant data spaces and specific sectors (such as health, **environment**, agriculture, ~~and~~ **transport and statistics**), **as well as representatives of academia, research, and standard setting organisations and bodies with specific expertise such as national statistical offices, where relevant. Balanced representation of different geographical areas should be ensured. The determination of the membership should also aim to ensure the efficient functioning of the Board.** The European Data Protection Board should be invited to appoint a representative to the European Data Innovation Board.

- (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 standards and specifications (such as the Core Vocabularies²⁷ and the CEF Building Blocks²⁸), without prejudice to 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 without making recourse to an intermediary. 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.
- (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. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council²⁹.
- (43) In order to take account of the specific nature of certain categories of data, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to lay 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 through a legislative procedure. 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 of the Treaty on the Functioning of the European Union. The measures provided for in this Regulation should not be used to restrict competition in a manner contrary to the Treaty on the Functioning of the European Union. This concerns in particular the rules on the exchange of competitively sensitive information between actual or potential competitors through data sharing 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 Council³⁰ and delivered an opinion on **10 March 2021**³¹[...].

²⁷ <https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies>

²⁸ <https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef>

²⁹ 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).

³⁰ 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).

³¹ **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).**

- (46) This Regulation respects the fundamental rights and observes 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) 2019/882³² and Directive (EU) 2016/2102³³. 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;**

HAVE ADOPTED THIS REGULATION:

³² 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).

³³ 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).

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 ~~sharing~~ **intermediation** services;
 - (c) a framework for voluntary registration of entities which collect and process data made available for altruistic purposes.
- (2) This Regulation is without prejudice to specific provisions in other Union legal acts or **national law** regarding access to or re-use of certain categories of data, or requirements related to processing of ~~personal or~~ non-personal data. Where a sector-specific Union legal act or **national law** requires public sector bodies, providers of data ~~sharing~~ **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.**
- (3) **Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation. In particular, this Regulation shall be without prejudice to Regulation (EU) 2016/679 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 law on the protection of personal data, the latter prevails. 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 the data protection legislation.**
- (4) 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 purpose of this Regulation, the following definitions apply:

- (1) 'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording;
- (2) 're-use' means the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks;

Commented [2]: PL deems this addition important as it further clarifies the relation between DGA and GDPR.

(2a) **'data sharing-intermediation service provider' means a service provider of a commercial service, which, through the provision of technical, legal and other services means establishes relationships between an undefined undetermined number of data holders subjects and data holders, on the one hand and data users on the other hand, for the exchange purpose of data sharing, pooling or trade of data as well as the exercise of data subjects' rights. The following shall, inter alia, not be considered to be data intermediation services for the purposes of this Regulation:**

Commented [3]: PL endorses this new definition, especially underlining the intermediation aspect of the service, deletion of "exchange, pooling and trade of data" and enumeration of services that are not considered data intermediation services under the DGA

(a) services that obtain data from data holders, aggregate, enrich or transform the data and license the use of the resulting data to data users, without establishing a direct relationship between data holders and data users;

(b) cloud infrastructure services;

(c) services that focus on the intermediation of content, in particular on copyright-protected content;

(d) services of data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed and exclusively offered by manufacturers of objects and devices connected to the Internet-of-Things, which have as their main objective to ensure functionalities of the connected object or device and to allow value added services;

(e) services of 'consolidated tape providers' as defined in point (53) of Article 4(1) of Directive 2014/65/EU; and

(f) services of 'account information service providers' as defined in point 19 of Article 4 of Directive(EU) 2015/2366;

(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 of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;**

(3aa) 'permission' means the right given by a legal person to another natural or legal person to process non-personal data as well personal data insofar as there is a legal basis that allows the legal person to grant such a permission;

(3b) **'data subject' means data subject as referred to an identified or identifiable natural person in point (1) of Article 4 of Regulation (EU) 2016/679; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;**

(4) **'metadata' means data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service;**

Commented [4]: This definition refers to both non-personal and personal data creating confusion with the notion of "consent" and introducing into the regime of personal data protection terms that do not exist in Regulation 2016/679.

- (5) 'data holder' means a legal ~~person or a natural person who is not a data subject for the purpose of a specific data processing operation~~ person or data subject who which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control;
- (6) 'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and ~~is authorised~~ has the right, including under Regulation (EU) 2016/679 in the case of personal data, the right to use that data for commercial or non-commercial purposes;
- (6a) 'data re-user' is a natural or legal person who re-uses data as defined in point (2);
- (7) 'data sharing' means the provision of data by a data holder subject or a data holder of data to a data user for the purpose of joint or individual use of ~~the shared~~ such data, based on voluntary agreements or Union or national law, directly or through an intermediary, under open data 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 ~~any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction~~;
- (8) 'access' means data processing use by a data user of data that has been provided by a data holder, 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 ~~entity~~ person means the place of its central administration in the Union;
- (9a) 'data cooperative' means an organisation supporting its members, who are data subjects or small ~~and medium-sized enterprises or one-person companies~~, in making informed choices before consenting to data processing, or in negotiating terms and conditions for data processing ~~or one-person companies or micro, small and medium-sized enterprises, who are members of the cooperative or who confer the power to the cooperative to negotiate terms and conditions for data processing before they consent, in making informed choices before consenting to data processing, and allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the interests of data subjects or legal persons~~;
- (10) 'data altruism' means voluntary sharing of data by data holders subjects or data holders without seeking ~~or receiving~~ a reward, for purposes objectives of general interest ~~the 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 a reward, for purposes of general interest defined in accordance with the national legislation where applicable, such as scientific research purposes, evidence-based policy making or improving public services~~;
- (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:
- they are established for the specific purpose of meeting needs in the general interest, and do not have an industrial or commercial character;

Commented [5]: This definition creates similar problems as described above (see our comment to the definition of "permission").

Commented [6]: It is not clear what is meant by this addition – is it a reference to open data as in Open Data Directive or a broader concept of making data (not limited to data held by public bodies) available unconditionally for everybody and free of charge?

Commented [7]: General interest should be defined in DGA (solely for the purpose of this regulation) not in national legislation. Otherwise, the term will be defined multiple times in MS national laws, which means regulatory fragmentation. Data altruism organizations will operate under different national legal conditions. Such fragmentation will not encourage the organisations to undergo notification process, which is already an additional burden in itself.
The same comment refers to art. 16(a).
PL would welcome the discussion on this issues, especially on the possible list of purposes to be included into the definition.

- (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 provide the opportunity to re-use data in **a manner preserving data subject all rights and obligations under the Regulation (EU) 2016/679, in particular data subjects' rights, intellectual property rights, and commercial and statistical confidentiality** ~~privacy preserving way, ensuring compliance with applicable legislation, a manner that allows for the operator of the~~ **and allowing the entity providing operator of 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) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of a provider of data ~~sharing~~ **intermediation** services 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 ~~sharing~~ **intermediation** services or entity with regard to the obligations of that provider of data ~~sharing~~ **intermediation** services or entity set up by this Regulation.



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;
 - (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 of secondary level and below;
 - (d) data protected for reasons of national security, defence or public security;
 - (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) The provisions of this Chapter do not create any obligation on public sector bodies to allow re-use of data nor do they 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 and to obligations of public sector bodies under Union and national law to allow the re-use of data.

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 have otherwise not be possible.**

Commented [8]: In light of the recent EDPB statement that upholds previously expressed reservations regarding statistical information (see below), PL would like to ask the EC for confirmation that our application is correct and there is no conflict between DGA and provisions on European statistics (Reg. 223/2009). DGA does not change the confidentiality status of data protected by statistical confidentiality as it directly assumes the priority of relevant EU and national regulations in this respect and underlines the need to maintain appropriate data security standards.

The EDPB further recalls that the inclusion of data held by public sector bodies which are protected on grounds of statistical confidentiality in the scope of Chapter II of the DGA, according to Article 3(1)(b), risks to contradict the principle according to which personal data collected for statistical purpose shall only be used for that purpose²⁸. Respect of this principle is key not to undermine trust of the person concerned when she or he provides her or his personal data for statistical purposes.

Commented [9]: As there is no definition of “educational establishment” in DGA, this addition makes sure universities’ research data is cover by the regulation.

- (3) ~~Such~~ **An exclusive right according to paragraph 2** shall be granted ~~in the context of a relevant service or concession contract in compliance with applicable Union and national public procurement and concession award rules, or, in the case of a contract of a value for which neither Union nor national public procurement and concession award rules are applicable, in compliance with~~ the principles of transparency, equal treatment and non-discrimination on grounds of nationality.
- (4) ~~In all cases not covered by paragraph 3 and where the general interest purpose cannot be fulfilled without granting an exclusive right, the principles of transparency, equal treatment and non-discrimination on grounds of nationality shall apply.~~
- (5) The period of exclusivity of the right to re-use data shall not exceed three years. 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 reasons why it is necessary to grant such a right, shall be transparent and be made publicly available online **two months before entry into force**, regardless of a possible publication of an award of a public procurement and concessions contract.
- (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 three years after the date of entry into force of this Regulation.
- (8) ~~Where an exclusive right to re-use data does not meet the conditions set out in paragraphs 2, 3 and 4, the exclusive right shall be void.~~

Article 5
Conditions for re-use

- (1) Public sector bodies which are competent under national law to grant or refuse access for the re-use of one or more of the categories of data referred to in Article 3 (1) shall make publicly available the conditions for allowing such re-use. 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, 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. These conditions shall not be used to restrict competition.
- (3) Public sector bodies ~~may~~ **shall, in accordance with Union and national law, impose the conditions necessary for preserving the protected nature of the data. Such conditions may consist of the requirement for re-users:**
- (a) ~~a condition whereby an obligation to re-use reuse is subject to only pre-processed data where such pre-processing aims to~~ **to use data that the public sector body or the competent body has anonymized or pseudonymised of in the case of personal data, or deletion, modification, or aggregated, or treated by any other method of disclosure control ion of in the case of commercially confidential information, including trade secrets and confidential statistical data, or content protected by intellectual property rights;-**
- (4) ~~Public sector bodies may impose a obligations condition~~

- (ba) to access and re-use the data **remotely** within a secure processing environment provided and controlled by the public sector; or
- (cb) to access and re-use the data within the physical premises in which the secure processing environment is located, 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 (b) and (c) t**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 be able 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.**
- (5a) The public sector body shall make the use of data provided in accordance with Article 5(3) ~~such secure processing environment~~ conditional on the ~~signature~~ adherence by the re-user to of a confidentiality agreement 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. Public sector bodies shall prohibit the re-users from re-identifying any data subject to whom the data relates and shall oblige the re-users to assess on an on-going basis the risks of re-identification and to notify any data breach resulting in the re-identification of the individuals concerned to the public sector body concerned.**
- ~~(5a) Public sector bodies shall prohibit the re-users from re-identifying any data subject to whom the data relates and shall oblige the re-users to assess on an on-going basis the risks of re-identification and to report any data breach resulting in the re-identification of the individuals concerned to the public sector body concerned.~~
- (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 other legal basis for transmitting the data under Regulation (EU) 2016/679, the public sector body shall may support provide assistance to potential re-users in seeking consent of the data subjects and/or permission from the data holders legal entities whose rights and interests may be affected by such re-use, where it is feasible without disproportionate cost burden for the public sector. In that task they 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 confidentiality~~, the public sector bodies shall ensure that the confidential information is not disclosed as a result of the re-use.
- (9) ~~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.~~

Commented [10]: PL maintains reservations regarding the re-use of personal data held by public bodies expressed in our comments to the second compromised proposal.

Although we appreciate the efforts to align the public sector obligation in this paragraph to the personal data protection regime, we still find the practicalities and the legal basis under the GDPR of the public sector bodies "providing assistance to potential re-users in seeking consent of the data subjects" unclear, therefore Poland would like this part (referring to personal data) to be removed

~~Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29 (2).~~

- (10) Public sector bodies shall ~~oblige the re-user only not to transmit~~ **transfer non-personal data protected on grounds set out in Article 3** ~~confidential data or data protected by intellectual property rights to a re-user which intends to transfer the data to a third country other than a country designated in accordance with paragraph 9~~**10a unless** if the re-user undertakes:

- (a) to comply with the obligations imposed in accordance with paragraphs 7 to 8 even after the data is transferred to the third country; and
- (b) to accept the jurisdiction of the courts of the Member State of the public sector body as regards any dispute related to the compliance with the obligation in point a).

- (10a) **When justified by a substantial number the volume of cases 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 advisory examination procedure referred to in Article 29 (23).~~

- (11) ~~Where S~~specific Union acts adopted in accordance with a legislative procedure ~~may establish that deem~~ certain non-personal data categories held by public sector bodies ~~shall be deemed~~ 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 anonymised data. Where such an act is adopted, t~~**the Commission shall lay down conditions applicable to the transfer to third-countries of such data by be empowered to adopt delegated implementing acts adopted in accordance with the examination procedure referred to in Article 29(23) in accordance with Article 28 supplementing this Regulation by laying down special conditions applicable for transfers to third countries.**

~~The Those~~ conditions ~~for the transfer to third countries~~ shall be based on the nature of data categories identified in the 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 ~~for data subjects~~, in accordance with the Union's international obligations.

The conditions ~~They~~ 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 9 to 11 are met.

- (13) Where the re-user intends to transfer non-personal data **protected on the grounds set out in Article 3(1)** to a third country, the public sector body shall inform the **legal entity person to which the data relates** ~~data holder~~ about the **intention to transfer of the data to that third country before the permission is given.**

*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 shall be non-discriminatory, proportionate and objectively justified and shall not restrict competition.
- (3) Public sector bodies shall ensure that any fees can 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 small and medium-sized enterprises in line with State aid rules. **This may include allowing re-use at lower or no cost fee.**
- (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, costs for anonymisation or other forms or preparation of personal and confidential data as provided in Article 5(3), costs for the maintenance of the secure processing environment, as well as any costs in relation to supporting re-users in seeking consent of from data subjects and permission from data holders whose rights and interests may be affected by such re-use. The criteria and methodology for calculating fees shall be laid down by the Member States and published in advance.**
- (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 shall be allowed may either to establish one or more new competent bodies or to rely on existing ones 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 8 (3) shall apply in regard to such competent bodies.

- (1b) **The competent body or bodies shall have adequate legal, financial and technical resources capacities and expertise 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;
 - (b) providing technical support ~~for in the application of tested techniques~~ ensuring data processing in a manner that preserves privacy **and confidentiality** of the information contained in the data for which re-use is allowed, ~~including techniques for pseudonymisation, anonymisation, generalisation, suppression and randomisation of personal data;~~
 - (c) **where relevant**, assisting the public sector bodies **to support re-users, where relevant**, in obtaining consent **for re-use from data subjects** or permission **from data holders** ~~by re-users for re-use for altruistic and other purposes~~ in line with **their** specific decisions ~~of data holders~~, including on the jurisdiction or jurisdictions in which the data processing is intended to take place;
 - (d) providing public sector bodies with assistance on the adequacy of undertakings made by a re-user, pursuant to Article 5 (10).
- ~~(3) 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 8 (3) shall apply in regard to such competent bodies.~~
- ~~(4) The competent body or bodies shall have adequate legal, financial and technical resources capacities and expertise 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).~~
- (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 through a single information point **which may be linked to sectoral information points. Functions of a single information point may be automated provided that adequate support by a public sector body is ensured. Member States shall be allowed either to establish a new information point or to rely on an existing structure.**
- (2) The single information point shall receive **enquiries or** requests for the re-use of the categories of data referred to in Article 3 (1) and shall transmit them to the competent public sector bodies, or the competent bodies referred to in Article 7 (1), where relevant, **and where possible and appropriate, by automated means.** The single information point shall make available by electronic means a register an asset list containing of all available data resources, **including where relevant those available at sectoral**

information points, containing with relevant information describing the nature of available data.

Article 8a
Processing of requests for re-use

- (1) (3) Requests for the re-use of the categories of data referred to in Article 3 (1) shall be granted or refused by the competent public sector bodies or the competent bodies referred to in Article 7 (1) ~~within a reasonable time, and in any case~~ within two months from the date of ~~the receipt of the~~ request.
- (2) **In the case of exceptionally extensive and complex requests this period may be extended by 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.**
- (3) (4) Any natural or legal person affected by a decision of a public sector body or of a competent body, as the case may be, shall have **an effective right of redress** ~~the right to an effective judicial remedy against such decision before the courts in~~ of 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 SHARING INTERMEDIATION SERVICES

Article 9

Providers of data sharing intermediation services

- (1) The provision of the following data sharing intermediation services **shall comply with the requirements of Article 11** and shall be subject to a notification procedure:
- (a) intermediation services between data holders which are legal ~~persons~~ **persons entities** 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 ~~exploitation use~~ of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users;
 - (b) intermediation services between data subjects that seek to make their **personal and non-personal** ~~other personal~~ data available and potential data users, including making available the technical or other means to enable such services, **including** in the exercise of the rights provided in Regulation (EU) 2016/679;
 - (c) services of data cooperatives, ~~that is to say services supporting data subjects or one person companies or micro, small and medium-sized enterprises, who are members of the cooperative or who confer the power to the cooperative to negotiate terms and conditions for data processing before they consent, in making informed choices before consenting to data processing, and allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the interests of data subjects or legal persons.~~
- ~~(2) This Chapter shall be without prejudice to the application of other Union and national law to providers of data sharing services, including powers of supervisory authorities to ensure compliance with applicable law, in particular as regard the protection of personal data and competition law.~~

Article 10

Notification of data sharing intermediation service providers

- (1) Any provider of data sharing intermediation services who intends to provide the services referred to in Article 9 (1) shall submit a notification to the competent authority **for data sharing intermediation services** referred to in Article 12.
- (2) For the purposes of this Regulation, a provider of data sharing 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.
- (3) A provider of data sharing intermediation services that is not established in the Union, but offers the services referred to in Article 9 (1) within the Union, shall appoint a legal representative in one of the Member States in which those services are offered. The provider shall be deemed to be under the jurisdiction of the Member State in which the legal representative is ~~established~~ **located**. **The representative shall be mandated by the provider of data sharing intermediation services to be addressed in addition to or instead of it by, in particular, competent authorities, ~~and~~ data holders subjects and**

data holders as well as data users, on all issues related to the service, for the purposes of ensuring compliance with this Regulation. The designation of a representative by the provider of data sharing intermediation services shall be without prejudice to legal actions which could be initiated against the provider of data sharing intermediation services themselves.

- (4) Upon notification, the provider of data sharing intermediation services may start the activity subject to the conditions laid down in this Chapter.
- (5) The notification shall entitle the provider to provide data sharing intermediation services in all Member States.
- (6) The notification shall include the following information:
 - (a) the name of the provider of data sharing intermediation services;
 - (b) the provider's legal status, form and registration number, where the provider is registered in trade or in another similar public register;
 - (c) the address of the provider'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;
 - (d) a website where information on the provider and the activities can be found, ~~where applicable, including as a minimum the information as referred to in letters a, b, c and f of this paragraph;~~
 - (e) the provider's contact persons and contact details;
 - (f) a description of the service the provider intends to provide **and indicate under which of the categories under Article 9 (1) such services fall, and how the conditions set in Article 11 are fulfilled;**
 - (g) the estimated date for starting the activity;
 - ~~(h) the Member States where the provider intends to provide services.~~
- (7) At the request of the provider, the competent authority **for data sharing intermediation services** shall, within one week **of duly and fully completed notification**, issue a standardised declaration, confirming that the provider has submitted the notification referred to in paragraph 4.
- ~~(8) The competent authority shall forward each notification to the national competent authorities of the Member States by electronic means, without delay.~~
- (9) The competent authority **for data sharing intermediation services** shall notify the Commission of each new notification. The Commission shall keep a **public register of all providers of data sharing intermediation services providing services in the Union, which shall make available the information referred to in points (a), (b), (c) and (d).**
- (10) The competent authority **for data sharing 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 sharing intermediation services.
- (11) Where a provider of data sharing intermediation services ceases its activities, it shall notify the relevant competent authority **for data sharing intermediation services** determined pursuant to paragraphs 1, 2 and 3 within 15 days. The competent authority

shall ~~forward~~ **inform the Commission by electronic means without delay** of each such notification **without delay, to the national competent authorities in the Member States and to the Commission by electronic means.**

Article 11

Conditions for providing data ~~sharing~~ **intermediation** services

The provision of data ~~sharing~~ **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 **provide data ~~sharing~~ intermediation services through a legally independent structure shall be placed in a separate legal entity**;
- (2) the ~~metadata~~ **data** collected **on any activity of a natural or legal person for the purposes of the provision of a data ~~sharing~~ intermediation service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service from the provision of the data sharing service** may be used only for the **purpose of** development of that service;
- ~~(3) the provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards prices;~~
- (4) the provider shall facilitate the exchange of the data in the format in which it receives it from ~~the a data holder~~ **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, **unless the data subject or data holder expressly disagrees**;
- (4a) the provider may offer additional specific services to data ~~holders~~ **subjects and data holders** facilitating the exchange of the data, such as storage, aggregation, curation, pseudonymisation and anonymisation;
- (4b) the provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data ~~holders~~ **subjects and data holders**, as well as for ~~and~~ data users, including as regards prices;
- (5) the provider shall have procedures in place to prevent fraudulent or abusive practices in relation to ~~access to data from~~ parties seeking access through their services;
- (6) the provider 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~~ **subjects and data holders**, as well as ~~and~~ data users, to obtain access to their data in case of insolvency **of the provider**;
- (6a) the provider shall take reasonable measures to ensure interoperability with other data ~~sharing~~ **intermediation services, among others, by means of commonly-used standards in the sector in which the data ~~sharing~~ intermediation service providers operate**;

- (7) the provider 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~~ and national law or the law of the relevant Member State;
- (8) the provider shall take measures to ensure a high level of security for the storage and transmission of non-personal data;
- (9) ~~the provider shall have procedures in place to ensure compliance with the Union and national rules on competition and it shall notify them to the relevant competent authority for evaluation, where relevant;~~
- (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 supporting data subjects to better understand advising data subjects on potential data uses by third parties and standard terms and conditions attached to such uses;
- (11) where a provider provides tools for obtaining consent from data subjects or permissions to process data made available by **data holders** ~~legal persons~~, 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**;
- (12) the provider shall maintain a record of intermediation activity, including the name and contact details of the intermediation parties and categories of data that were subject of intermediation procedure.**

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 sharing 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 sharing intermediation services** shall comply with Article 23.
- (3) **The powers of the designated competent authorities are without prejudice to the powers** ~~The designated competent authorities, of the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities. These authorities shall exchange the information which is necessary for the exercise of their tasks and cooperate in view of enforcement in relation to data sharing intermediation service providers. In particular, for any question requiring an assessment of compliance with Regulation (EU) 2016/679, the competent authority shall first seek an opinion or decision by the competent supervisory authority established pursuant to that Regulation and comply with that opinion or decision.~~

Article 13 *Monitoring of compliance*

- (1) The competent authority **for data sharing intermediation services** shall monitor and supervise compliance with this Chapter. **The competent authority may also monitor and**

supervise the compliance of such data sharing intermediation services based on the request of natural or legal persons.

- (2) The competent authority **for data sharing intermediation services** shall have the power to request from providers of data sharing intermediation services all the information that is necessary to verify compliance with the requirements ~~laid down in Articles 10 and 11 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 sharing intermediation services** finds that a provider of data sharing intermediation services does not comply with one or more of the requirements ~~laid down in Article 10 or 11 of this Chapter~~, it shall notify that provider of those findings and give it the opportunity to state its views, within ~~a reasonable time limit~~ **30 days**.
- (4) The competent authority **for data sharing intermediation services** 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. In this regard, the competent authorities shall be able, where appropriate:
- (a) to impose dissuasive financial penalties which may include periodic penalties **and penalties** with retroactive effect;
 - (b) to require cessation ~~or postponement~~ of the provision of the data sharing intermediation service **due to serious or substantial breaches that have not been corrected despite prior notification or warning or postponement suspension of the provision of such a service until modifications of its conditions, as requested by the competent authority, are made. The competent authority for data sharing intermediation services shall request the Commission to remove the provider of the data sharing intermediation service from the register of providers of data sharing intermediation services once it has ordered the cessation ~~or postponement~~ of the service.**
- (5) The competent authorities **for data sharing intermediation services** shall communicate the measures imposed pursuant to paragraph 4 and the reasons on which they are based to the entity concerned without delay and shall stipulate a reasonable period, **and in any event not longer than 30 days**, for the entity to comply with the measures.
- (6) If a provider of data sharing 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 purpose of their tasks under this Regulation** and requests to take the measures referred to in this Article. **Where a competent authority for data sharing intermediation services in one Member State requests assistance from another Member State, it shall submit a duly justified request. The competent authority for data sharing 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:

- (a) **public sector bodies that offer data sharing intermediation facilities on a non-commercial basis;**
- (b) **recognised data altruism organisations and other** not-for-profit entities whose activities consist only in seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism.

CHAPTER IV DATA ALTRUISM

Article 14a

National ~~arrangements Policies~~ for ~~dData a~~Altruism

- (1) Member States ~~shall define national policies for data altruism and~~ **shall** put 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 shall may in particular support data subjects in making personal data related to them held by public sector bodies available voluntarily for data altruism.~~
- (2) The European Data Innovation Board shall advise and assist in developing a consistent practice throughout the Union.

Commented [11]: PL would like these to remain voluntary facultative. It is worth considering to expand this article with some more guidelines for the scope of the policies in order to maintain uniformity across MS

Article 15

Register of recognised data altruism organisations

- (1) Each competent authority for the registration of data altruism organisations designated pursuant to Article 20 shall keep a public register of recognised data altruism organisations ~~that has legal effect.~~
- (2) ~~An entity registered in the register referred to in paragraph 1 and in accordance with Article 16 may refer to itself as a 'data altruism organisation recognised in the Union' in its written and spoken communication. The Commission shall maintain a public Union register of recognised data altruism organisations for information purposes.~~
- (3) ~~The Commission shall maintain a public Union register of recognised data altruism organisations for information purposes. An entity registered in the register in accordance with Article 16 may refer to itself as a 'data altruism organisation recognised in the Union' in its written and spoken communication.~~

Article 16

General requirements for registration

In order to qualify for registration, the data altruism organisation shall:

- (a) be a legal ~~entity~~ **person** constituted to meet objectives of ~~general interest, in line with national law;~~
- (b) operate on a not-for-profit basis and be independent from any entity that operates on a for-profit basis;
- (c) perform the activities related to data altruism ~~take place through a~~ **structure that is legally functionally independent separate structure, separate from its other activities it has undertaken.**

Commented [12]: General interest should be defined in DGA (solely for the purpose of this regulation) not in national legislation. Otherwise, the term will be defined multiple times in MS national laws, which means regulatory fragmentation. Data altruism organizations will operate under different national legal conditions. Such fragmentation will not encourage the organisations to undergo notification process, which is already an additional burden in itself.

Article 17

Registration of recognised data altruism organisations

- (1) Any entity which meets the requirements of Article 16 may request to be entered in the register of recognised data altruism organisations referred to in Article 15 (1).
- (2) For the purposes of this Regulation, an entity engaged in activities based on data altruism with establishments in more than one Member State, shall register in the Member State in which it has its main establishment.
- (3) An entity that is not established in the Union, but meets the requirements in Article 16, shall appoint a legal representative in one of the Member States where it intends to collect data based on data altruism. For the purpose of compliance with this Regulation, that entity shall be deemed to be under the jurisdiction of the Member State where the legal representative is located.
- (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 ~~main~~ 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 website where information on the entity and the activities can be found, **including as a minimum the information as referred to in letters a, b, d, e and h of this paragraph;**
 - (g) the entity's contact persons and contact details;
 - (h) the ~~purposes~~ **objectives** of general interest it intends to promote when collecting 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 the competent authority **for the registration of data altruism organisations** considers that the entity complies with the requirements of Article 16, it shall register the entity in the register of recognised data altruism organisations within twelve weeks from the date of application. The registration shall be valid in all Member States. Any registration shall be communicated to the Commission, for inclusion 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 national register of recognised data altruism organisations.
- (7) Any entity entered in the register of recognised data altruism organisations shall ~~submit~~ **notify the competent authority for the registration of data altruism organisations of** any changes of the information provided pursuant to paragraph 4 ~~to the competent authority~~ within 14 calendar 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.**

Article 18
Transparency requirements

- (1) Any entity entered in the 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;
 - (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 the register of recognised data altruism organisations shall draw up and transmit to the 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 use process data it holds, including a summary description of the general interest purposes pursued by such data use 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 uses 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 ~~legal entities~~ as regards their data

- (1) Any entity entered in the register of recognised data altruism organisations shall inform data subjects and data holders **prior to any processing of their data**:
 - (a) about the ~~purposes objectives~~ of general interest (and in case of personal data – about the purpose of the processing which shall be specified, explicit and legitimate) for which it permits the processing of their data by a data user in an easy-to-understand manner;
 - (b) about **the location of any processing performed outside the Union, in case the processing is performed by the entity entered in the register of recognised data altruism organisations itself**.
- (2) The entity shall ~~also~~ ensure that the data is not be used for other ~~purposes objectives~~ than those of general interest for which it permits the processing.
- (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. ~~also ensure that consent from data~~**

Commented [13]: In case of personal data processing based on consent (what is the case of data altruism) the purpose of the processing of personal data should be clearly defined. "General interest" is the notion which is too broad and undefined and cannot be used to describe the purpose of the processing within the meaning of GDPR. (purpose limitation).

See the opinion of EDPS/EDPB: point 172 "the requirement for the data altruism organization to inform the data holder (including the data subject) "about the purposes of general interest for which it permits the processing of their data by a data user" shall be in line with the principle according to which data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (principle of purpose limitation, under Article 5(b) of the GDPR".

~~subjects or permissions to process data made available by legal persons can be easily withdrawn.~~

- (2b) The entity shall take measures to ensure an appropriate ~~high~~ level of security for the storage and processing of data that it has collected based on data altruism.
- (3) Where an entity entered in the register of recognised data altruism organisations provides tools for obtaining consent ~~by third parties~~ from data subjects or permissions to process data made available by ~~data holders legal persons~~, it shall, **where relevant**, specify the jurisdiction or jurisdictions **outside the Union** in which the data use is intended to take place.

Article 20

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

- (1) Each Member State shall designate one or more competent authorities responsible for the 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 the designated authorities.
- (3) The competent authority **for the registration of data altruism organisations** shall undertake its tasks in cooperation with the data protection authority, where such tasks are related to processing of personal data, and with relevant sectoral bodies of the same Member State. ~~For any question requiring an assessment of compliance with Regulation (EU) 2016/679, the competent authority shall first seek an opinion or decision by the competent supervisory authority established pursuant to that Regulation and comply with that opinion or decision.~~

Article 21

Monitoring of compliance

- (1) The competent authority shall monitor and supervise compliance of entities entered in the register of recognised data altruism organisations with the conditions laid down in this Chapter. **The competent authority 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 the 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 a reasonable time limit**.
- (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:

PUBLIC

- (a) lose its right to refer to itself as a 'data altruism organisation recognised in the Union' in any written and spoken communication;
 - (b) be removed from the register of recognised data altruism organisations, **including at Union level.**
- (6) If an entity included in the 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 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 ~~so requested~~ shall, upon such a request, provide a response 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 22

European data altruism consent form

- (1) In order to facilitate the collection of data based on data altruism, the Commission ~~may~~ **shall** adopt implementing acts **establishing and** developing a European data altruism consent form, **after consultation of the European Data Protection 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 (~~232~~).
- (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 read by humans 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 sharing intermediation services or entity included in the 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 shall be allowed may either to establish one or more new entities or to rely on existing ones.**
- (2) Competent authorities shall exercise their tasks in an impartial, transparent, consistent, reliable and timely manner.
- (3) The top-management and the personnel responsible for carrying out the relevant tasks of the competent authority provided for in this Regulation cannot be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the services which they evaluate, nor the authorised representative of any of those parties 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 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) **Any affected ~~N~~natural and legal persons shall have the right to lodge a complaint with the relevant national competent authority against a provider of data sharing intermediation services or an entity entered in the register of recognised data altruism organisations **in relation to any matter pertaining to this Regulation**.**
- (2) The 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 right to an effective judicial~~ 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:
- ~~(a) a failure to act on a complaint lodged with the competent authority referred to in Articles 12 and 20;~~
- ~~(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 ~~sharing~~ **intermediation** services and the monitoring of entities entered into the register of recognised data altruism organisations.
- (2) Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority against which the judicial remedy is sought is located **individually or, where relevant, by the representatives of one or more natural or legal persons.**
- (3) When a competent authority referred to in Article 12 or 20 fails to act on a complaint, any affected natural and legal persons shall 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 expert Group group~~, consisting of the representatives of competent authorities of all the Member States **pursuant to Article 12 and Article 20**, the European Data Protection Board, the Commission, relevant data spaces and other representatives of ~~competent authorities~~ **relevant bodies** in specific sectors **as well as bodies with specific expertise such as national statistical offices**.
- (1a) The Board shall consist of at least one 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 (a), (b), (e) and (f), as well as at least one sub-group for technical discussions on standardisation and interoperability pursuant to Article 27 (c) and (d).**
- (2) Stakeholders and relevant third parties ~~may~~ **shall** be invited to attend meetings of the Board and to participate in its work, **where relevant**.
- (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 European Data Innovation Board

The Board shall have the following tasks:

- (a) to advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies referred to in Article 7 (1) processing requests for the re-use of the categories of data referred to in Article 3 (1);
- (b) to advise and assist the Commission in developing a consistent practice of the competent authorities in the application of requirements applicable to data ~~sharing~~ **intermediation service providers and entities performing activities related to data altruism**;
- (c) to advise **and assist** the Commission on the prioritisation of cross-sector 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;
- (d) to **advise and** assist the Commission in enhancing the interoperability of data as well as data ~~sharing~~ **intermediation** services between different sectors and domains, building on existing European, international or national standards;
- (e) to facilitate the cooperation between national competent authorities under this Regulation 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 ~~sharing~~ **intermediation** service providers and the registration and monitoring of recognised data altruism organisations, **including the coordination and harmonisation regarding the setting of fees or penalties:-**

- (f) to facilitate the cooperation between national competent authorities on the application of Article 30.

CHAPTER VII

COMMITTEE PROCEDURE ~~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) shall be conferred on the Commission for an indeterminate period of time from [...].~~
- (3) ~~The delegation of power referred to in Article 5 (11) 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) 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 within the meaning of Regulation (EU) No 182/2011.
- (2) Where reference is made to this paragraph, Article ~~4 5~~ of Regulation (EU) No 182/2011 shall apply.
- (3) **Where reference is made to this paragraph, Article ~~4 5~~ of Regulation (EU) No 182/2011 shall apply.**
- ~~(34) Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests. In such a case, the chair shall convene a committee meeting within a reasonable time.~~

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 sharing intermediation service provider or the entity entered in the 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 access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the law of the relevant Member State, ~~unless the transfer or access are in line with~~ **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 sharing intermediation service provider or entity entered in the register of recognised data altruism organisations to transfer from or give access to non-personal data subject to 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 concluded before [the entry into force of this Regulation].
- (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 sharing intermediation service provider or entity entered in the 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 held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the 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) in that context, the competent court issuing the order or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by Union law or the applicable Member State law.

~~The addressee of the decision shall may ask the opinion of the relevant competent bodies or authorities, pursuant to this Regulation, in order to determine if these conditions are met. The relevant competent bodies shall exchange information on international access requests in the framework of the European Data Innovation Board.~~

- (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 sharing

Commented [14]: PL has reservations to Art. 30 (3). Data transfer, including non-personal data, in relations with third countries should be based on international agreements. DGA should not duplicate the same uncertainties that are associated with personal data transfer under GDPR. PL is considering, therefore, whether to introduce additional guarantees to the catalog of 'safety valves' (Article 30 (3) (a) - (c)), in which the EU courts grant authorization for data transfer/check the legality of such access based on EU rules and transfer. It should not be the case that in the absence of an international agreement regulating the transfer of data, the guarantees related to access to data are in fact decided by the third country court at its discretion, and the entity that has the rights to this data can at most count on the fact that the technology company the manager of such data will challenge requests for access to the data.

intermediation service provider or the entity entered in the 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.

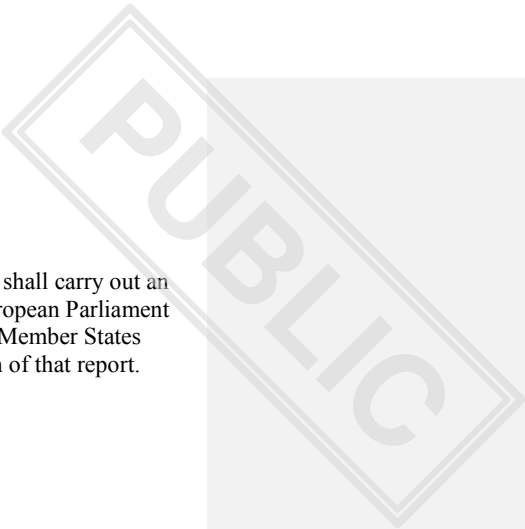
- (5) The public sector body, the natural or legal person to which the right to re-use data was granted under Chapter 2, the data ~~sharing~~ intermediation service provider and the entity providing data altruism shall inform the data ~~holder~~ subject or the data holder about the existence of a request of an administrative authority in a third-country to access its data, 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 of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by [date of application of the Regulation] and shall notify the Commission without delay of any subsequent amendment affecting them.~~

Commented [15]: PL notes that in order to maintain the uniformity of regulations at the EU level, it is worth considering the introduction of rules for determining penalties. GDPR regulations concerning this topic can be used as a model for this.

- (1) Each competent authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation shall in each individual case be effective, proportionate and dissuasive.
- (2) When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
 - (a) Infringements of the following provisions shall be subject to administrative fines up to [...], or in the case of an undertaking, up to [...] % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (b) the obligations regarding transfers of non-personal data to third countries pursuant to Article 5 (12) and Article 30,
 - (c) the obligation of data intermediation service providers to notify pursuant to Article 10,
 - (d) the conditions for providing services pursuant to Article 11,
 - (e) conditions for the registration as a recognised data altruism organisation pursuant to Articles 18 and 19.
- (3) The exercise by the competent authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
- (4) Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by competent authorities.



Article 32
Evaluation and review

By [four years after the data 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. Member States shall provide the Commission with the information necessary for the preparation of that report.

Article 33
Amendment to Regulation (EU) No 2018/1724

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

Starting, running and closing a business	Notification as a provider of data sharing intermediation services	Confirmation of the receipt of notification
	Registration as a European Data Altruism Organisation	Confirmation of the registration

Article 34
Transitional arrangements

Entities providing the data ~~sharing~~ **intermediation** services provided in Article 9(1) on the date of entry into force of this Regulation shall comply with the obligations set out in Chapter III by [date - 2 years after the start date of the application of the Regulation] at the latest.

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 [182 months after its entry into force].

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

Done at Brussels,

For the European Parliament
The President

For the Council
The President