EUROPEAN
COMMISSION

Brussels, 25.11.2020
COM(2020) 767 final

2020/0340 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European data governance
(Data Governance Act)

(Text with EEA relevance)

{SEC(2020) 405 final} - {SWD(2020) 295 final} - {SWD(2020) 296 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Regulation of the European Parliament and of the Council[1] on data governance. It is the first of a set of measures announced in the 2020 European strategy for data[2]. The instrument aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The instrument would address the following situations:

- Making public sector data available for re-use, in situations where such data is subject to rights of others[3].
- Sharing of data among businesses, against remuneration in any form.
- Allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).
- Allowing data use on altruistic grounds.

• Consistency with existing policy provisions in the policy area

The current initiative covers different types of data intermediaries, handling both personal and non-personal data. Therefore, the interplay with the legislation on personal data is particularly important. With the General Data Protection Regulation (GDPR)[4] and ePrivacy Directive[5], the EU has put in place a solid and trusted legal framework for the protection of personal data and a standard for the world.

The current proposal complements the 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 (Open Data Directive)[6]. This proposal addresses data held by public sector bodies that is subject to rights of others and therefore falls outside the scope of this Directive. The proposal has logical and coherent links with the other initiatives announced in the European strategy for data. It aims at facilitating data sharing including by reinforcing trust in data sharing intermediaries that are expected to be used in the different data spaces. It does not aim to grant, amend or remove the substantial rights on access and use of data. This type of measures is envisaged for a potential Data Act (2021)[7].

The instrument draws inspiration from the principles for data management and re-use developed for research data. The FAIR data principles[8] stipulate that such data should, in principle, be findable, accessible, interoperable and re-usable.

---

1 The final form of the legal act will be determined by the content of the instrument.

2 COM/2020/66 final.

3 "Data the use of which is dependent on the rights of others" or "data subject to the rights of others" covers data that might be subject to data protection legislation, intellectual property, or contain trade secrets or other commercially sensitive information.

4 OJ L 119, 4.5.2016, p. 1-88.

5 OJ L 201, 31.7.2002, p. 37-47.

6 OJ L 172, 26.6.2019, p. 56–83.

7 See COM/2020/66 final.

8 https://www.force11.org/group/fairgroup/fairprinciples

- **Consistency with other Union policies**

Sector-specific legislation on data access is in place and/or under preparation to address identified market failures in fields such as the automotive industry[9], payment service providers[10], smart metering information[11], electricity network data[12], intelligent transport systems[13], environmental information[14], spatial information[15], and the health sector[16]. The current proposal supports the use of data made available under existing rules without altering these rules or creating new sectoral obligations.

Similarly, the proposal is without prejudice to competition law, and it is designed in compliance with Articles 101 and 102 TFEU, and it is also without prejudice to the provisions of 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[17].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

Article 114 of the Treaty on the Functioning of the European Union (TFEU) is identified as the relevant legal basis for this Regulation. Pursuant to this Article, the EU has to adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market in the EU. This initiative is part of the 2020 European strategy for data that aims to strengthen the single market for data. With a growing digitalisation of the economy and society, there is a risk that Member States will increasingly legislate data-related issues in an uncoordinated way, which would intensify fragmentation in the single market. Setting up the governance structures and mechanisms that will create a coordinated approach to using data across sectors and Member States would help stakeholders in the data economy to capitalise on the scale of the single market. It will contribute towards the establishment of the single market for data, by ensuring the emergence and cross-border functioning of novel services through a set of harmonised provisions.

Digital policies are a shared competence between the EU and its Member States. Article 4(2) and (3) of the TFEU specifies that, in the area of the single market and technological development, the EU can carry out specific activities, without prejudice to the Member States' freedom to act in the same areas.

- **Subsidiarity (for non-exclusive competence)**

Businesses often need data from several Member States so they can develop EU-wide products and services, as data samples available in individual Member States often do not

9 OJ L 188 18.7.2009, p. 1 as amended by OJ L 151, 14.6.2018, p. 1.
10 OJ L 337, 23.12.2015, p. 35-127.
11 OJ L 158, 14.6.2019, p. 125-199; OJ L 211, 14.8.2009, p. 94-136.
12 OJ L 220, 25.8.2017, p. 1-120; OJ L 113, 1.5.2015, p. 13-26.
13 OJ L 207, 6.8.2010, p. 1-13.
14 OJ L 41, 14.2.2003, p. 26-32.
15 OJ L 108, 25.4.2007, p. 1-14.
16 A legislative proposal for the European health data space is envisaged for the fourth quarter of 2021. https://eur-lex.europa.eu/resource.html?uri=cellar%3A91ce5c0f-12b6-11eb-9a54-01aa75ed71a1.0001.02/DOC_2&format=PDF
17 OJ L 178, 17.7.2000, p. 1-16.

have the richness and diversity allowing 'Big Data' pattern detection or machine learning. In addition, data-based products and services developed in one Member State may need to be customised to suit the preferences of customers in another Member State, and this requires local data on the Member States' level. As such, data needs to be able to flow easily through EU-wide and cross-sector value chains, for which a highly harmonised legislative environment is essential. Furthermore, only action at Union level can ensure that a European model of data sharing, with trusted data intermediaries for B2B data sharing and for personal data spaces, takes off, given the cross-border nature of data sharing and the importance of such data sharing.

A single market for data should ensure that data from the public sector, businesses and citizens can be accessed and used in the most effective and responsible manner possible, while businesses and citizens keep control of the data they generate and the investments made into their collection are safeguarded. Increased access to data would have as a result that companies and research organisations would advance representative scientific developments and market innovation in the EU as a whole, which is particularly important in situations where EU coordinated action is necessary, such as the COVID-19 crisis.

- **Proportionality**

The initiative is proportionate to the objectives sought. The proposed legislation creates an enabling framework that does not go beyond what is necessary to achieve the objectives. It harmonises a series of data-sharing practices, while respecting the Member States' prerogative to organise their administration and legislate on access to public sector information. The notification framework for data intermediaries, as well as the mechanisms for data altruism serve to attain a higher level of trust in these services, without unnecessarily restricting these activities, and help develop an internal market for the exchange of such data. The initiative will also leave a significant amount of flexibility for application at sector-specific level, including for the future development of European data spaces.

The proposed Regulation will give rise to financial and administrative costs, which are to be borne mainly by national authorities, while some costs will also burden data users, and data sharing providers in order to ensure compliance with the obligations set in this Regulation. However, the exploration of different options and their expected costs and benefits led to a balanced design of the instrument. It will leave national authorities enough flexibility to decide on the level of financial investment and to consider possibilities to recover such costs through administrative charges or fees, while offering overall coordination at EU level. Similarly, the costs to data users and sharing providers will be counterbalanced by the value emanating from broader access and use of data, as well as the market uptake of novel services.

- **Choice of the instrument**

The choice of a regulation as the legal instrument is justified by the predominance of elements that require a uniform application that does not leave margins of implementation to the Member States and that creates a fully horizontal framework. These elements include the notification for data sharing service providers, the mechanisms for data altruism, the basic principles that apply to the re-use of public sector data that cannot be available as open data or are not subject to sector-specific EU legislation, and the set-up of coordination structures at European level. The direct applicability of the Regulation would avoid an implementation

period and process for the Member States, enabling at the same time the establishment of the common European data spaces in the near future, in line with the EU recovery plan.[18]

At the same time, the provisions of the Regulation are not overly prescriptive and leave room for different levels of Member State action for elements that do not undermine the objectives of the initiative, in particular the organisation of the competent bodies supporting public sector bodies with their tasks relating to the re-use of certain categories of public sector data.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

An online public consultation was launched on 19 February 2020 on the day the European strategy for data[19] was adopted, and was closed on 31 May 2020. The consultation explicitly indicated it was launched in order to prepare the current initiative, and it addressed the items covered in the initiative with relevant sections and questions. It targeted all types of stakeholders.

In total, the Commission received 806 contributions, of which 219 were from a company, 119 from a business association, 201 from EU citizens, 98 from academic / research institutions, and 57 from public authorities. Consumers' voices were represented by 7 respondents, and 54 respondents were non-governmental organisations (including 2 environmental organisations). Among the 219 companies / business organisations, 43.4% were SMEs. Overall, 92.2% of the replies came from the EU-27. Very few respondents indicated whether their organisation had a local, regional, national or international scope.

230 position papers were submitted, either attached to questionnaire answers (210) or as stand-alone contributions (20). The papers provided different views on the topics covered by the online questionnaire, in particular in relation to the governance of common data spaces. They provided opinions on the key principles for those spaces, and expressed a high level of support for the prioritisation of standards as well as the data altruism concept. They also indicated the need for safeguards in developing measures related to data intermediaries.

- **Collection and use of expertise**

In order to explore with the relevant experts the framework conditions for creating common European data spaces in the identified sectors, a series of 10 workshops on common European data spaces took place in 2019 and an additional workshop was organised in May 2020. Gathering a total of more than 300 stakeholders, mainly from the private and public sectors, the workshops covered different sectors (agriculture, health, finance/banking, energy, transport, sustainability/environment, public services, smart manufacturing) and more cross-cutting aspects (data ethics, data market places). The Commission departments dealing with these areas participated in the workshops. The sectoral workshops helped to identify the common elements across the sectors, which need to be addressed by way of laying down a horizontal governance framework.

[18] COM(2020) 456 final.
[19] COM/2020/66 final.

- **Impact assessment**

An impact assessment was carried out for this proposal. On 9 September 2020, the Regulatory Scrutiny Board issued a negative opinion. On 5 October 2020 the Board delivered a positive opinion subject to reservations.

The impact assessment examines the baseline scenarios, policy options and their impacts for four intervention areas, namely (a) mechanisms for the enhanced use of public sector data that cannot be available as open data, (b) a certification or labelling framework for data intermediaries, (c) measures facilitating data altruism, and (d) mechanisms to coordinate and steer horizontal aspects of governance in the form of an EU-level structure.

For all intervention areas, policy option 1 of having coordination at EU level with soft regulatory measures was found to be insufficient, since it would not significantly change the situation compared to the baseline scenario. Thus, the main analysis concentrated on policy options 2 and 3, which involved a low and high intensity regulatory intervention respectively. The preferred option turned out to be a combination of regulatory interventions of lower and higher intensity, in the following manner:

Regarding mechanisms to enhance the use of certain public sector data, the use of which is subject to the rights of others, both the low and high intensity options would introduce EU-wide rules for re-using such information (in particular non-exclusivity). The low intensity regulatory intervention would require that individual public sector bodies allowing this type of re-use to be technically equipped to ensure that data protection, privacy and confidentiality are fully preserved. It would also contain an obligation for Member States to provide for at least a one-stop shop mechanism for the requests to access such data, without determining its exact institutional and administrative form. The high intensity option would have prescribed the establishment of one single data authorisation body per Member State. Given the costs and issues of feasibility related to the latter, the preferred option is the lower intensity regulatory intervention.

For the certification or labelling of trusted data intermediaries, a lower intensity regulatory intervention was envisaged to consist in a softer, voluntary labelling mechanism, where a fitness check of the compliance with the requirements for acquiring the label as well as awarding the label would be carried out by competent authorities designated by Member States (which can also be the one-stop shop mechanisms also established for the enhanced re-use of public sector data). The high intensity regulatory intervention consisted of a compulsory certification scheme managed by private conformity assessment bodies. As a compulsory scheme would generate higher costs, this could potentially have a prohibitive impact on SMEs and startups, and the market is not mature enough for a compulsory certification scheme; therefore the lower intensity regulatory intervention was identified as the preferred policy option. However, the higher intensity regulatory intervention in the form of a compulsory scheme was also identified as a feasible alternative, as it would bring significantly higher trust to the functioning of data intermediaries, and would establish clear rules for how these intermediaries are supposed to act in the European data market. After further discussions in the Commission, an intermediate solution was retained. It consists of a notification obligation with ex post monitoring of compliance with the requirements to exercise the activities by the competent authorities of the Member States. The solution has the advantages of a compulsory regime, while limiting the regulatory burden on the market players.

In the case of data altruism, the low intensity regulatory intervention consisted in a voluntary certification framework for organisations seeking to offer such services, while the high intensity regulatory intervention envisaged a compulsory authorisation framework. As the latter would ensure a higher level of trust in making data available, which could contribute to more data being made available by data subjects and companies and result in a higher level of development and research, while generating a similar amount of costs, it was flagged in the Impact Assessment as the preferred option for this intervention area. However, the further discussions within the Commission revealed additional concerns around the potential administrative burden on organisations engaging in data altruism, and the relation of the obligations with future sectoral initiatives on data altruism. For this reason an alternative solution was retained, giving organisations engaging in data altruism the possibility to register as a 'Data Altruism Organisation recognised in the EU'. This voluntary mechanism will contribute to increase trust, while presenting a lower administrative burden than both a compulsory authorisation framework and a voluntary certification framework.

Finally, for the European horizontal governance mechanism, the low intensity regulatory intervention referred to the creation of an expert group, while the high intensity regulatory intervention consisted in the creation of an independent structure with legal personality (similar to the European Data Protection Board). Given the high costs and the low level of political feasibility surrounding the inception of the higher intensity option, the low intensity policy option was chosen.

The impact assessment support study[20] indicated that, while under the baseline scenario the data economy and the economic value of data sharing are expected to grow to an estimated EUR 533 to 510 billion (3.87% of the GDP), this would increase to between EUR 540.7 and EUR 544.4 billion (3.92% to 3.95% of the GDP) under the preferred, packaged option. These amounts take into account only in a limited way the downstream benefits, in terms of better products, higher productivity and new ways for tackling societal challenges (e.g. climate change). Indeed, these benefits are likely to be considerably higher than the direct benefits.

At the same time, this packaged policy option would make it possible to create a European model for data sharing that would offer an approach that is alternative to the current business model for integrated tech platforms through the emergence of neutral data intermediaries. This initiative can make the difference for the data economy by creating trust in data sharing and incentivising the development of common European data spaces, where natural and legal persons are in control of the data they generate.

- **Fundamental rights**

Since personal data falls within the scope of some elements of the Regulation, the measures are designed in a way that fully complies with the data protection legislation, and actually increases in practice the control that natural persons have over the data they generate.

Regarding the enhanced re-use of public sector data, both the fundamental rights of data protection, privacy and property (concerning proprietary rights in certain data, which is e.g. commercially confidential or protected by intellectual property rights) will be respected. Similarly, data sharing service providers offering services to data subjects will have to comply with the applicable data protection rules.

[20] European Commission (2020, *forthcoming*). *Support Study to this Impact Assessment*, SMART 2019/0024, prepared by Deloitte.

The notification framework for data intermediaries would touch on the freedom to conduct a business, as it would place certain restrictions in the form of different requirements as a pre-requisite for the functioning of such entities.

4. BUDGETARY IMPLICATIONS

This proposal will not have any budgetary implications.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

Due to the dynamic nature of the data economy, monitoring of the evolution of impacts constitutes a key part of the intervention in this domain. To ensure that the selected policy measures actually deliver the intended results and to inform possible future revisions, it is necessary to monitor and evaluate the implementation of this Regulation.

Monitoring the specific objectives and the regulatory obligations will be achieved through representative surveys of stakeholders, through the work of the Support Centre for Data Sharing, via records of the European Data Innovation Board on the different intervention areas reported by the dedicated national authorities and through an evaluation study to support the instrument's review.

- **Detailed explanation of the specific provisions of the proposal**

Chapter I defines the subject matter of the regulation and sets out the definitions used throughout the instrument.

Chapter II creates a mechanism for re-using certain categories of protected public sector data which is conditional on the respect of the rights of others (notably on grounds of protection of personal data, but also protection of intellectual property rights and commercial confidentiality).This mechanism is without prejudice to sector-specific EU legislation on access to and the re-use of this data. The re-use of such data falls outside the scope of Directive (EU) 2019/1024 (Open Data Directive). Provisions under this Chapter do not create the right to re-use such data, but provide for a set of harmonized basic conditions under which the re-use of such data may be allowed (e.g. the requirement of non-exclusivity). Public sector bodies allowing this type of re-use would need to be technically equipped to ensure that data protection, privacy and confidentiality are fully preserved. Member States will have to set up a single contact point supporting researchers and innovative business in identifying suitable data, and are required to put structures in place to support public sector bodies with technical means and legal assistance.

Chapter III aims to increase trust in sharing personal and non-personal data and lower transaction costs linked to B2B and C2B data sharing by creating a notification regime for data sharing providers. These providers will have to comply with a number of requirements, in particular the requirement to remain neutral as regards the data exchanged. They cannot use such data for other purposes. In the case of providers of data sharing services offering services for natural persons, the additional criterion of assuming fiduciary duties towards the individuals using them will also have to be met.

The approach is designed to ensure that data sharing services function in an open and collaborative manner, while empowering natural and legal persons by giving them a better

overview of and control over their data. A competent authority designated by the Member States will be responsible for monitoring compliance with the requirements attached to the provision of such services.

Chapter IV facilitates data altruism (data voluntarily made available by individuals or companies for the common good). It establishes the possibility for organisations engaging in data altruism to register as a 'Data Altruism Organisation recognised in the EU' in order to increase trust in their operations. In addition, a common European data altruism consent form will be developed to lower the costs of collecting consent and to facilitate portability of the data (where the data to be made available is not held by the individual).

Chapter V sets out the requirements for the functioning of the competent authorities designated to monitor and implement the notification framework for data-sharing service providers and entities engaged in data altruism. It also contains provisions on the right to lodge complaints against the decisions of such bodies and on the means of judicial redress.

Chapter VI creates a formal expert group (the 'European Data Innovation Board') which will facilitate the emergence of best practices by Member States' authorities in particular on processing requests for the re-use of data which is subject to the rights of others (under Chapter II), on ensuring a consistent practice regarding the notification framework for data sharing service providers (under Chapter III), and for data altruism (Chapter IV). In addition, the formal expert group will support and advise the Commission on the governance of cross-sectoral standardisation and the preparation of strategic cross-sector standardisation requests. This chapter establishes also the composition of the Board and organises its functioning.

Chapter VII allows the Commission to adopt implementing acts concerning the European data altruism consent form.

Chapter VIII contains transitional provisions for the functioning of general authorisation scheme for data sharing providers and provides for final provisions.

2020/0340 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European data governance (Data Governance Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[21],

Having regard to the opinion of the Committee of the Regions[22],

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.

(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, for example through improved personalised medicine, new mobility, and its contribution to the European Green Deal[23]. In its Data Strategy[24], 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

[21] OJ C , , p. .

[22] OJ C , , p. .

[23] 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)

[24] COM (2020) 66 final.

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.

(3) It is necessary to improve the conditions for data sharing in the internal market, by creating a harmonised framework for data exchanges. Sector-specific legislation can develop, adapt and propose new and complementary elements, depending on the specificities of the sector, such as the envisaged legislation on the European health data space[25] and on access to vehicle data. Moreover, certain sectors of the economy are already regulated by sector-specific Union law that include rules relating to cross-border or Union wide sharing or access to data[26]. This Regulation is therefore without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council ([27]), 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 ([28]), Directive (EU) 2016/943 of the European Parliament and of the Council ([29]), Regulation (EU) 2018/1807 of the European Parliament and of the Council ([30]), Regulation (EC) No 223/2009 of the European Parliament and of the Council ([31]), Directive 2000/31/EC of the European Parliament and of the Council ([32]), Directive 2001/29/EC of the European Parliament and of the Council ([33]), Directive (EU) 2019/790 of the European Parliament and of the Council ([34]), Directive 2004/48/EC of

---

25 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).

26 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.

27 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)

28 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)

29 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)

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

31 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)

32 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)

33 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)

34 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)

the European Parliament and of the Council ([35]), Directive (EU) 2019/1024 of the European Parliament and of the Council ([36]), as well as Regulation 2018/858/EU of the European Parliament and of the Council ([37]), Directive 2010/40/EU of the European Parliament and of the Council ([38]) and Delegated Regulations adopted on its basis, and any other sector-specific Union legislation that organises the access to and re-use of data. This Regulation should be without prejudice to 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. A horizontal regime for the re-use of certain categories of protected data held by public sector bodies, the provision of data sharing 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 services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act should also apply.

(4) Action at Union level is necessary in order to address the barriers to a well-functioning data-driven economy and to create a Union-wide governance framework for data access 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 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.

(5) The idea that data that has been 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.

---

35 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).

36 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).

37 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).

38 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)

(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. Application of these privacy-enhancing technologies, together with comprehensive data protection approaches should ensure the safe re-use of 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 ([39]). 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 Article 6 of Regulation (EU) 2016/679.

(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. Personal data fall outside the scope of Directive (EU) 2019/1024 insofar as the access regime excludes or restricts access to such data for reasons of data protection, privacy and the integrity of the individual, in particular in accordance with data protection rules. The re-use of data, which may contain trade secrets, should take place without prejudice to Directive (EU) 2016/943[40], which sets the framework for the lawful acquisition, use or disclosure of trade secrets. This Regulation 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 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.

(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

[39] 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).

[40] OJ L 157, 15.6.2016, p. 1–18

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, regardless of a possible publication of an award of a public procurement contract.

(10) Prohibited exclusive agreements and other practices or arrangements between data holders and data re-users 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. 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 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, 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 allows such transmission. 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 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.

(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). 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 ([41]) 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 protect 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 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

[41] 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).

regarding the protection of data the third country concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems. The existence of effective legal remedies for data holders, public sector bodies or data sharing 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 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. 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 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.

(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 have been identified as highly sensitive, 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. In order to ensure harmonised practices across the Union, such types of highly sensitive non-personal

public data should be defined by Union law, for example in the context of the European Health Data Space or other sectoral legislation. The conditions attached to the transfer of such data to third countries should be laid down in delegated acts. Conditions should be proportionate, non-discriminatory and necessary to protect legitimate public policy objectives identified, such as the protection of public health, 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 at lower or no cost, for example for certain categories of re-uses such as non-commercial re-use, 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. 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. 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. Such support structure could support the data holders with management of the consent, including consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. 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.

(22) Providers of data sharing services (data intermediaries) are expected to play a key role in the data economy, 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 holders and 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. This Regulation should only cover providers of data sharing services that have as a main objective the establishment of a business, a

legal and potentially also technical relation between data holders, including data subjects, 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 number of data holders and data users, excluding data sharing services that are meant to be used by a closed group of data holders and users. Providers of cloud services should be excluded, as well as service providers that obtain data from 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 and data users, 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 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, 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 in the context of objects and devices connected to the Internet-of-Things that have as their main objective to ensure functionalities of the connected object or device and 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 Council [42] as well as 'account information service providers' in the sense of Article 4 point 19 of Directive (EU) 2015/2366 of the European Parliament and of the Council[43] should not be considered as data sharing service providers for the purposes 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 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 the individuals' control over the data pertaining 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

[42] 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.

[43] 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.

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 services, in particular related to the use of data and the compliance with the conditions imposed by 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 services. This will contribute to ensuring that data holders and data users have better control over the access to and use of their data, in accordance with Union law. 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 providers should offer a novel, 'European' way of data governance, by providing a separation in the data economy between data provision, intermediation and use. Providers of data sharing services may also make available specific technical infrastructure for the interconnection of data holders and data users.

(26) A key element to bring trust and more control for data holder and data users in data sharing services is the neutrality of data sharing service providers as regards the data exchanged between data holders and data users. It is therefore necessary that data sharing 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 service and any other services provided, so as to avoid issues of conflict of interest. This means that the data sharing service should be provided through a legal entity that is separate from the other activities of that data sharing provider. Data sharing providers that intermediate the exchange of data between individuals as data holders and legal persons should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data holders.

(27) In order to ensure the compliance of the providers of data sharing 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 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 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 services is offering services within the Union, it should be ascertained whether it is apparent that the provider of data sharing 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 services, or the use of a language generally used in the third country where the provider of data sharing 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 services is planning to offer services within the Union. The representative should act on behalf of the provider of data sharing 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 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 services to comply with Regulation (EU) 2016/679 and the responsibility of supervisory authorities to ensure compliance with that Regulation. Where the data sharing 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 services should also take measures to ensure compliance with competition law. 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 future prices, production costs, quantities, turnovers, sales or capacities.

(30) A notification procedure for data sharing 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 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 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 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 services in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities.

(33) The competent authorities designated to monitor compliance of data sharing 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.

(34) The notification framework laid down in this Regulation should be without prejudice to specific additional rules for the provision of data sharing 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 of general interest. Such purposes would include healthcare, combating climate change, improving mobility, facilitating 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 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.

(36) Legal entities that seek to support purposes 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 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.

(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. 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.

(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, agriculture, transport and statistics). 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 Vocabularies[44] and the CEF Building Blocks[45]), 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 Council[46].

(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

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

[45] https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef

[46] 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).

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 though 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 services.

(45) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([47])and delivered an opinion on […].

(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,

HAVE ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and scope

(1) This Regulation lays down:

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

(b) a notification and supervisory framework for the provision of data sharing 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 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 requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical,

[47] 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).

administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act shall also apply.

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;

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

(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;

(5) ‘data holder’ means a legal person or data subject who, 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 to use that data for commercial or non-commercial purposes;

(7) ‘data sharing’ means the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary;

(8) ‘access’ means processing 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 means the place of its central administration in the Union;

(10) ‘data altruism’ means 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, such as scientific research purposes 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:

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

(b) they have legal personality;

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

(13) 'public undertaking' means any undertaking over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it; for the purpose of this definition, a dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly:

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

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

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

(14) 'secure processing environment' means the physical or virtual environment and organisational means to provide the opportunity to re-use data in a manner that allows for the 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 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 services or entity with regard to the obligations of that provider of data sharing 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 ;

(b) statistical confidentiality;

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

(d) protection of personal data.

(2) This Chapter does not apply to:

(a) data held by public undertakings;

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

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

(d) data 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. 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 a product in the general interest.

(3) Such exclusive right 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, 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 paragraph 2, 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.

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 impose an obligation to re-use only pre-processed data where such pre-processing aims to anonymize or pseudonymise personal data or delete commercially confidential information, including trade secrets.

(4) Public sector bodies may impose obligations

(a) to access and re-use the data within a secure processing environment provided and controlled by the public sector ;

(b) 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) 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 be able to verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties.

(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 support re-users in seeking consent of the data subjects and/or permission from the legal entities whose rights and interests may be affected by such re-use, where it is feasible without disproportionate cost 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.

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

(10) Public sector bodies shall only transmit 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 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).

(11) Where specific Union acts adopted in accordance with a legislative procedure establish that certain non-personal data categories held by public sector bodies shall be deemed to be highly sensitive for the purposes of this Article, the Commission shall be empowered to adopt delegated acts in accordance with Article 28 supplementing this Regulation by laying down special conditions applicable for transfers to third-countries. The 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. 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 to a third country, the public sector body shall inform the data holder about the transfer of data to that third country.

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 and by small and medium-sized enterprises in line with State aid rules.

(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). The methodology for calculating fees shall be published in advance.

(6) 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) 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.

(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 in the application of tested techniques ensuring data processing in a manner that preserves privacy 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) assisting the public sector bodies, where relevant, in obtaining consent or permission by re-users for re-use for altruistic and other purposes in line with 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 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 and technical 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.

(2) The single information point shall receive 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. The single information point shall make available by electronic means a register of available data resources containing relevant information describing the nature of available data.

(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 request.

(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 the right to an effective judicial remedy against such decision before the courts of the Member State where the relevant body is located.

CHAPTER III
REQUIREMENTS APPLICABLE TO DATA SHARING SERVICES

Article 9
Providers of data sharing services

(1) The provision of the following data sharing services shall be subject to a notification procedure:

(a) intermediation services between data holders which are legal persons 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 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 data available and potential data users, including making available the technical or other means to enable such services, 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 service providers

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

(2) For the purposes of this Regulation, a provider of data sharing 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 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.

(4) Upon notification, the provider of data sharing 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 services in all Member States.

(6) The notification shall include the following information:

(a) the name of the provider of data sharing 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;

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

(f) a description of the service the provider intends to provide;

(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 shall, within one week, 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 shall notify the Commission of each new notification. The Commission shall keep a register of providers of data sharing services.

(10) The competent authority may charge fees. 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 services.

(11) Where a provider of data sharing services ceases its activities, it shall notify the relevant competent authority determined pursuant to paragraphs 1, 2 and 3 within 15 days. The competent authority shall forward without delay each such notification to the national competent authorities in the Member States and to the Commission by electronic means.

Article 11
Conditions for providing data sharing services

The provision of data sharing 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 data sharing services shall be placed in a separate legal entity;

(2) the metadata collected from the provision of the data sharing service may be used only for the 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 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;

(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 and data users to obtain access to their data in case of insolvency;

(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;

(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;

(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 advising data subjects on potential data uses 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 legal persons, it shall specify the jurisdiction or jurisdictions in which the data use is intended to take place.

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 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 shall comply with Article 23.

(3) The designated competent authorities, the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities shall exchange the information which is necessary for the exercise of their tasks in relation to data sharing providers.

Article 13
Monitoring of compliance

(1) The competent authority shall monitor and supervise compliance with this Chapter.

(2) The competent authority shall have the power to request from providers of data sharing services all the information that is necessary to verify compliance with the requirements laid down in Articles 10 and 11. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

(3) Where the competent authority finds that a provider of data sharing services does not comply with one or more of the requirements laid down in Article 10 or 11, it shall notify that provider of those findings and give it the opportunity to state its views, within 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. In this regard, the competent authorities shall be able, where appropriate:

(a) to impose dissuasive financial penalties which may include periodic penalties with retroactive effect;

(b) to require cessation or postponement of the provision of the data sharing service.

(5) The competent authorities 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 for the entity to comply with the measures.

(6) If a provider of data sharing 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 and requests to take the measures referred to in this Article.

Article 14
Exceptions

This Chapter shall not apply to 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 15
Register of recognised data altruism organisations

(1) Each competent authority designated pursuant to Article 20 shall keep a register of recognised data altruism organisations.

(2) The Commission shall maintain a Union register of recognised data altruism organisations.

(3) 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 constituted to meet objectives of general interest;

(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 legally independent structure, separate from other activities it has undertaken.

Article 17
Registration

(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;

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

(h) the purposes 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 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 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.

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;

(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 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 data it holds, including a summary description of the general interest purposes pursued by such data use 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 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 legal entities as regards their data

(1) Any entity entered in the register of recognised data altruism organisations shall inform data holders:

(a) about the purposes of general interest for which it permits the processing of their data by a data user in an easy-to-understand manner;

(b) about any processing outside the Union.

(2) The entity shall also ensure that the data is not be used for other purposes than those of general interest for which it permits the processing.

(3) Where an entity entered in the register of recognised data altruism organisations provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons, it shall specify the jurisdiction or jurisdictions in which the data use is intended to take place.

Article 20

Competent authorities for 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 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 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.

(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 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:

(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.

(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.

Article 22
European data altruism consent form

(1) In order to facilitate the collection of data based on data altruism, the Commission may adopt implementing acts developing a European data altruism consent form. The form shall allow the collection of consent across Member States in a uniform format. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29 (2).

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

(3) Where personal data are provided, the European data altruism consent form shall ensure that data subjects are able to give consent to and withdraw consent from a

specific data processing operation in compliance with the requirements of Regulation (EU) 2016/679.

(4) The form shall be available in a manner that can be printed on paper and 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 services or entity included in the register of recognised data altruism organisations.

(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, with the information necessary to carry out their tasks under this Regulation. Where a national competent authority considers the information requested to be confidential in accordance with Union and national rules on commercial and professional confidentiality, the Commission and any other competent authorities concerned shall ensure such confidentiality.

Article 24
Right to lodge a complaint

(1) Natural and legal persons shall have the right to lodge a complaint with the relevant national competent authority against a provider of data sharing services or an entity entered in the register of recognised data altruism organisations.

(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 remedy 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) 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 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.

CHAPTER VI
EUROPEAN DATA INNOVATION BOARD

Article 26
European Data Innovation Board

(1) The Commission shall establish a European Data Innovation Board ("the Board") in the form of an Expert Group, consisting of the representatives of competent authorities of all the Member States, the European Data Protection Board, the Commission, relevant data spaces and other representatives of competent authorities in specific sectors.

(2) Stakeholders and relevant third parties may be invited to attend meetings of the Board and to participate in its work.

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

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

Article 27
Tasks of the Board

The Board shall have the following tasks:

(a) 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 providers;

(c) to advise 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 assist the Commission in enhancing the interoperability of data as well as data sharing 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 service providers and the registration and monitoring of recognised data altruism organisations.

CHAPTER VII
COMMITTEE AND DELEGATION

Article 28
Exercise of the Delegation

(1) The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

(2) The power to adopt delegated acts referred to in Article 5 (11) 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 of Regulation (EU) No 182/2011 shall apply.

(3) 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

(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 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 in order to prevent 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 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 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) 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 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 ask the opinion of the relevant competent bodies or authorities, pursuant to this Regulation, in order to determine if these conditions are met.

(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 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 provider and the entity providing data altruism shall inform 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 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.

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 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 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 [12 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	*For the Council*
The President	*The President*