EUROPEAN
COMMISSION

Brussels, XXX
[...](2020) XXX draft

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European data governance
An enabling framework for common European data spaces (Data Governance Act)

(Text with EEA relevance)

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:

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

In addition, the instrument supports the common European data spaces as regards the use of standards, the actors involved and the governance at EU level.

The European Strategy for Data proposes to establish sector- or domain-specific data spaces, as the concrete arrangements in which data sharing and/or data pooling can happen beyond one single Member State. A common European data space will be composed of a secure IT environment for processing of data by an open number of organisations, and a set of rules of legislative, administrative and contractual nature that determine the rights of access to and processing of the data. Data will be made available on a voluntary basis, unless required otherwise by law, and can be re-used against remuneration or for free, depending on the data holder's decision.

The present instrument proposes an overarching framework encompassing horizontal measures relevant for all common European data spaces. The framework is without prejudice to sector-specific rules, governance mechanisms and standards where relevant. The objective of the initiative is not to create the common European data spaces by law, but to enhance their development by strengthening trust in data sharing and in data intermediaries.

• 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

---

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

a standard for the world. The legislative framework for the common data spaces would work within the rules of the existing legislation on the protection of personal data. The proposal builds on the mechanisms present in the existing legislation (in particular the portability right under Article 20 GDPR) that give individuals more control over how their data is used.

The current proposal complements the Directive on open data and the re-use of public sector information[6]. This proposal addresses data held by public sector bodies that is not publicly accessible and therefore falls outside the scope of the existing Directive. Therefore, the initiative is also complementary to the Implementing Act on High-Value Datasets under the Open Data Directive, which is expected to be adopted in 2021. The proposal has logical and coherent links with the other initiatives announced in the European Strategy for Data. It aims at improving data governance across the common European data spaces by facilitating data sharing and addressing data intermediaries that have a role in the different data spaces. It does not aim to change the material rights on who can access and use what data under which circumstances. This type of measures is foreseen for the Data Act (2021)[7].

The instrument can build on the development of principles for data management and re-use developed for research data. The FAIR data principles stipulate that such data should in principle be findable, accessible, interoperable and re-usable. Inspiration can be drawn for data re-use in other domains or economic activities.

- **Consistency with other Union policies**

Sector-specific legislation on data access is in place and/or in preparation to address identified market failures in fields such as automotive[8], payment service providers[9], smart metering information[10], electricity network data[11] and intelligent transport systems[12]. The current proposal supports the use of data made available under existing rules without altering them or creating new sectoral obligations.

Similarly, the proposal does not amend existing competition law provisions, and it is designed in full compliance with Articles 101 and 102 TFEU, which prohibit anti-competitive agreements and the abuse of dominant market power, respectively.

While offering an alternative model to the data handling practices of the Big Tech platforms, the current proposal is also clearly distinct from the envisaged Digital Services Act (DSA). The DSA, foreseen for Q4 2020, will address issues relating to the market power of online platforms, resulting from, among other factors, their control of large amounts of data. The DSA may propose remedies addressing these platforms, including in relation to data access and use. The DSA package also intends to clarify the responsibilities and obligations of digital services, and in particular online platforms, based on, amongst other elements, an evaluation of the e-Commerce Directive.

---

6 OJ L 172, 26.6.2019, p. 56–83.
7 See COM/2020/66 final.
8 OJ L 188 18.7.2009, p. 1 as amended by OJ L 151, 14.6.2018, p. 1.
9 OJ L 337, 23.12.2015, p. 35-127.
10 OJ L 158, 14.6.2019, p. 125-199, OJ L 211, 14.8.2009, p. 94-136.
11 OJ L 220, 25.8.2017, p. 1-120; OJ L 113, 1.5.2015, p. 13-26.
12 OJ L 207, 6.8.2010, p. 1-13.

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. This article provides for the EU 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 reinforce the Single Market for Data. With a growing digitalisation of the economy and society, there is a risk of Member States increasingly legislating data-related issues in an uncoordinated way, which would intensify fragmentation in the internal 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 internal market.

Digital policies are a shared competence between the EU and its Member States. Articles 4(2) and (3) of the TFEU specify that, in the area of the internal 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 across several Member States so that they can roll out EU-wide products and services, as data samples available in individual Member States often do not have the richness and diversity to allow 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 the preferences of customers in another Member State, and this requires local data. 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 concerted action by the Member States can ensure that a European model of data sharing, with trusted data intermediaries for B2B data sharing and for personal data spaces, can take off.

A Single Market for Data would 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 investments made into their collection are respected. Companies would be able to market their products and services in all Member States. 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 harmonizes a series of practices in relation with data sharing, while respecting the Member States' prerogatives in terms of organising their administration and legislation on access to information. The initiative will also leave a significant amount of flexibility for application at sector-specific level, including through the European data spaces.

The proposed Regulation will induce financial and administrative costs to be borne mainly by national authorities. However, the exploration of different options and their expected costs and benefits led to a balanced design of the instrument. It will leave enough flexibility for national

authorities to decide on the level of financial investment and possibilities to recover such costs through administrative charges or to take additional measures, while offering overall coordination at EU level (e.g. through a European structure for coordinating the governance aspects of data sharing).

- **Choice of the instrument**

The choice of a Regulation as the form of the legal instrument is justified by the predominance of elements that necessitate a uniform application and should not leave margins to implementation to the Member States in order to create a fully horizontal governance framework. These elements include the general authorisation of data sharing service providers and altruism mechanisms, 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 setup of coordination structures at European level. The direct applicability of the Regulation would avoid an implementation period and process for the Member States, so that the establishment of the common European data spaces could start as soon as possible, in line with the EU Recovery Plan.

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 mechanisms supporting the re-use of public sector data, the use of which is subject to the respect of rights of others and not already subject to sector-specific EU legislation.

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

- **Stakeholder consultations**

A public online consultation was published on the day of adoption of the European strategy for data[13] (19 February 2020) and closed on 31 May 2020. The consultation explicitly indicated it was launched in view of preparing the current initiative, and addressed the items covered in the initiative with relevant sections and questions. It targeted all types of stakeholders. In addition to issues related to the governance of common European data spaces, it gathered input on the EU-wide list of high-value datasets that the Commission will draw up under the Open Data Directive, and explored issues related to cloud computing. Furthermore, it contained some generic questions on the European data strategy.

In total, 806 contributions were received, of which 219 were on behalf of a company, 119 from a business association, 201 from EU citizens, 98 on behalf of 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). Amongst 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

[13] COM/2020/66 final

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**

A series of 10 workshops on common European data spaces took place in 2019 and an additional one in May 2020, in view of exploring with the relevant experts the framework conditions for creating common European data spaces in the identified sectors. Gathering in total more than 300 stakeholders, mainly from the private and the public sectors, the workshops covered different sectors (agriculture, health, finance/banking, energy, transport, sustainability/environment, public services, smart manufacturing) as well as more cross-cutting aspects (data ethics, data market places). The concerned DGs were involved in these workshops.

- **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.

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 coordination at EU level and soft regulatory measures was found to be insufficient, since it would not significantly change the situation as compared to the baseline scenario. Thus, the main analysis concentrated on policy options 2 and 3, which meant a lower and higher intensity regulatory intervention, respectively. The preferred option turned out to be a package 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 lower and the higher intensity option would introduce basic EU-wide rules for the re-use of such information (in particular non-exclusivity). The lower intensity regulatory intervention would foresee in addition the requirement that individual public sector bodies allowing this type of re-use would be technically equipped to ensure that privacy and confidentiality are fully preserved. In addition it would contain an obligation for Member States to provide at least for a one-stop shop mechanism for the request of such uses, without determining the exact institutional and administrative form. The higher intensity option would have prescribed the establishment of one single data authorisation body. Given the costs of and the 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 comprise of a softer, voluntary labelling mechanism, where fitness check and 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, the lower intensity regulatory intervention was identified as preferred policy option. However, the higher intensity regulatory intervention in the form of a compulsory scheme – which differs from a certification 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.

In the case of data altruism, the lower intensity regulatory intervention comprised of a voluntary certification framework for organisations seeking to offer such services, while the higher intensity regulatory intervention envisaged a compulsory authorisation framework. As this latter would allow for a higher level of trust which could contribute to more "donations" and result in a higher level of development and research, while generating a similar amount of costs, it was chosen as preferred option for this intervention area.

Finally, for the European horizontal governance mechanism, the lower intensity regulatory intervention comprised of a formal Commission expert group, while the higher intensity regulatory intervention consisted of an independent structure with legal personality (structurally similar to the European Data Protection Board). Given the high costs and the issues of feasibility around the inception of the higher intensity option, the lower intensity policy option was chosen.

The Impact Assessment support study[14] 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 Big 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 as a precondition for the development of common European data spaces, where individuals and companies are in control of the data they generate, and are comfortable with the way in which the data are used in innovative ways.

- **Fundamental rights**

Since personal data falls into 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 individuals have over the data they generate.

Regarding the enhanced re-use of public sector data, both the fundamental rights of 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 that offer services to data subjects will have to comply with the applicable data protection rules.

In the context of data altruism of individuals, individuals need to be protected, so that they do not share data with organisations that (i) do not respect their altruistic intentions or (ii)

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

encourage individuals to make available more data than they would normally be prepared to (by setting 'unethical' incentives). Further promoting use of personal data held by the public sector bears inherent risks that are addressed in the institutional design.

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, the Commission would set up a monitoring and evaluation process.

The monitoring of the specific objectives and the preferred option will be achieved through representative surveys among stakeholders carried out by the Support Centre for Data Sharing and via records of the European Data Innovation Board on the different intervention areas reported by the dedicated national authorities, and an evaluation study to support the review of the instrument.

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

Title II creates a mechanism for re-use of public sector data the re-use of which is conditional on the respect of rights of others (notably rights under GDPR, but also intellectual property rights and legitimate interests in keeping commercially confidential information private), and is without prejudice to existing sector-specific EU legislations that pertain to access to and re-use of this data. The re-use of such data falls outside the scope of the Open Data Directive (Directive (EU) 2019/1024). Provisions under this Title do not create right to re-use such data, but make the application of these provisions conditional on national law or lawful practices permitting the re-use of such data. They provide for a set of basic conditions under which such data shall be permitted (e.g. the requirement of non-exclusivity). Individual public sector bodies allowing this type of re-use would need to be technically equipped to ensure that privacy and confidentiality are fully preserved. Member States shall 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.

Title III aims to enhance trust in common European data spaces and lower transaction costs linked to B2B and C2B data sharing by building trust in intermediaries that organise data sharing in a data space among business users (brokers, marketplaces, facilitators) and for individuals as data subjects (personal data spaces), respectively. This approach is designed to allow facilitators to organise data spaces in an open and collaborative manner without the orchestrator to acquire a significant degree of market power. They shall remain neutral in the sense that they limit their activities to the intermediation service and do not further monetise the data.

The act provides for a general authorisation framework for such intermediaries based on criteria that seek to preserve neutrality. In the case of providers of data sharing services offering services for individuals, the additional criterion of assuming fiduciary duties towards the individuals using them will also have to be met. This framework will empower individuals by

giving them a better overview of and control over their data. The monitoring of compliance with the requirements will be done by a competent authority designated by the Member States.

Title IV facilitates data altruism (data voluntarily made available by individuals or companies for the common good). It establishes a compulsory general authorisation framework for data altruism schemes to protect the individuals and companies that provide the data. In addition, a common European data altruism consent form shall be developed to lower the costs of collecting consent and facilitate portability of the data (where the data to be made available is not held by the individual).

Title V sets out the requirements for the functioning of the competent authorities that are designated to award and monitor and to implement the general authorisation for data sharing service providers and entities engaged in data altruism.

Title VI calls for the creation of a formal Expert Group ('European Data Innovation Board') which, in addition to ensuring a consistent practice in processing requests for data (under Title II), in ensuring a consistent practice regarding the general authorisation framework for data sharing services providers (under Title III), and for data altruism (Title IV) shall support and advise the Commission on the governance of cross-sectoral standardisation and the preparation of strategic cross-sector standardisation requests, and help build an institutional capacity going beyond standardisation. The Board shall be composed of Member States' experts, as well as representatives of the different sectors and/or common European data spaces. The Board shall be assisted by a secretariat provided by the Commission.

Title VII allows the Commission to adopt delegated acts for the details of the European data altruism consent form.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European data governance
An enabling framework for common European data spaces (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[15],

Having regard to the opinion of the Committee of the Regions[16],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Treaty of the European Union provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted. Setting out common rules and practices in the Member States relating to the establishment and development of a framework for data governance, supporting the functioning of common European data spaces should contribute to the achievement of those objectives.

(2) Action at Union level is necessary in order to address the barriers to a well-functioning data-driven economy and to create the means for 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 of data intermediaries to business users and to data subjects, as well as the collection and processing of data made available for altruistic purposes by individuals and undertakings.

(3) 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.

(4) The expanding Internet of Things is expected to generate a growing amount of data, for example as a result of their deployment in automated industrial production processes or in consumer devices. Such data may be of personal but also of non-personal nature. Specific examples of such data include aggregated and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the

---

15 OJ C , p .
16 OJ C , p .

use of pesticides and water, data on maintenance needs for industrial machines, but also data from smart home appliances, vehicles or wearable devices, most of which can be linked to an individual and therefore the personal data related to that individual. This enormous amount of data could serve as a most valuable input for other new data-driven services and for applications in the public interest, as it has been the case for the operation of smart cities, smart and resource-efficient farming or measures to prevent the spread of infectious diseases. In respect to the latter, the valuable contribution that data can have for public interest applications has been shown in the management of the COVID-19 pandemic.

(5) The increasing volume of non-personal industrial data and public data in Europe, combined with technological change in how the data is stored and processed, will constitute a potential source of growth and innovation that should be employed for productive and pro-competitive purposes. Improving the governance structures for handling data and increasing the pools of quality data available for use and reuse is essential and the first step towards the completion of the single market for data. Additionally, businesses and the public sector in the European Union can be empowered through the use of data to make better decisions. As data – unlike most economic resources – can be duplicated at close to zero cost and its use by one person or organisation theoretically does not prevent the simultaneous use by another person or organisation, it is even more compelling to seize the opportunity presented by data for social and economic good. That potential should be put to work to address the needs of individuals and thus create value for the economy and society. To release this potential, there is a need to ensure better access to data and its responsible usage.

(6) In a society where individuals will generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules. Citizens and undertakings (in particular, small and medium-sized enterprises (SMEs) alike should be empowered to make better decisions based on insights derived from data they produce. At the same time, European values and fundamental rights and the conviction that the human being is and should remain at the centre, should prevail. The GDPR already provides that individuals as data subjects with a number of rights regarding their data, and obliges those processing the data to do so lawfully, transparently and responsibly. In situations when the data processing is based on consent, the individuals should retain full control over the access and usage of their personal data, and have the possibility to monitor what they share, which space it is stored in and who can access or use it, while retaining the right to alter the consent on the basis of which the processing takes place.

(7) The process of completing the single market for data should happen with consideration to the structure of European industry, and with specific regard towards start-ups and SMEs. There are currently market imbalances in relation to access to and use of data, for example when it comes to access to data by SMEs. Imbalances may arise due to the competitive advantages emanating from the vast amounts of diverse data held by large online platforms as well as in other situations, such as with regard to access to co-generated Internet-of-Things data from industrial and consumer devices.

(8) In order for the European Union to fulfil its ambition to become a leading role model for a society empowered by data, it will have to build on its strong legal framework to tackle the issues related to data governance. Inspiration can be found in existing sets of principles, such as the FAIR principles facilitating the re-use of research data by promoting that they be findable, accessible, interoperable and re-useable (at the legal level). Cross-sectoral measures for data access and use should create the necessary over-

arching framework for the data-agile economy, thereby avoiding harmful fragmentation of the internal market through inconsistent practices between sectors and diverging actions between the Member States. Such measures should nonetheless take into account the specificities of individual sectors and of the Member States.

(9) In its Data Strategy[17], 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 EU in compliance with applicable law. In order to turn this vision into reality, it proposes to establish domain-specific data spaces, as the concrete arrangements in which data sharing and data pooling can happen. Such European data spaces can cover areas such as health, mobility, manufacturing, financial, energy, or agriculture or thematic areas, such as the European green deal or European data spaces for public administration or skills. The data spaces would be composed of an information and communication technology environment for secure processing of data by organisations, the number of which is open, and a set of rules of legislative, administrative and contractual nature that determine the rights of access to and processing the data, in compliance with Union and Member State law. Data would be made available on a voluntary basis, unless law requires otherwise.

(10) Given the variety of domains in which such spaces could be established and the diversity of challenges in terms of data access and use, the governance and technical implementations of such spaces will vary. For this reason, this Regulation only contains elements of concern to different common European data spaces, without prejudice to the governance mechanisms established at sectoral level. Sector-specific legislation can develop, adapt and propose new and complementary elements, depending on the specificities of the sector. Certain sectors of the economy are already regulated by sector-specific Union legal acts that include rules related to cross-border or EU wide sharing or access to data[18]. When those Union legal acts contain provisions imposing requirements at least similar in effect to those of the current Regulation, those provisions should apply.

(11) Government-held information, data that has been generated at the expense of public budgets, should benefit society as part of a long-standing EU policy. 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, data the re-use of which is conditional on the respect of rights of others (commercially confidential data, data under 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 national rules transposing Directive (EU) 2016/943) in public databases is often not made available, not even for research or innovative activities. Due to its sensitivity as being subject to rights of third parties, making this data available would require meeting technical and legal requirements to ensure compliance with the 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.

(12) There are techniques enabling privacy-friendly analyses on databases that contain personal data. One technique is anonymization of the data which makes the data in

---

[17] COM (2020) 66 final.

[18] 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.

question non-personal data, falling outside scope of the GDPR. As anonymization often impacts heavily on the utility of the data, in recent years, technology has advanced in providing solutions for privacy-preserving big data analytics that maximize the capacity to extract certain insights from large volumes of data whilst protecting individuals' data and privacy and preserving meaningful human control. These technologies can help ensure that data-related risks are mitigated both at design time and run time, and they can help ensure that architectures are safe and secure. They include techniques such as pseudonymisation, generalisation, suppression and randomisation that are carried out with the help of multi-party computation, homomorphic encryption, differential privacy, execution of analytical algorithms developed by third parties under the control of the data controller in its own systems, federated machine learning, use of synthetic data, and data wrapping. Application of these privacy-enhancing technologies together with comprehensive data protection approaches can ensure the safe re-use of personal data and commercially sensitive business data for research, innovation and statistical purposes. On this basis, nuanced approaches can be designed with respect to such re-use of data. A broader use of such technologies is desirable, not least in the public sector. Data use and re-use in this context may thus mean that the data processing is done in an information technology and communication environment controlled by the public sector.

(13) This Regulation does not introduce a general right to re-use data the re-use of which is conditional on the respect of rights of others. The data covered by this Regulation fall outside the scope of Directive (EU) 2019/1024 that excludes data subject to commercial and statistical confidentiality and data for which third parties have intellectual property rights. Personal data fall outside scope of Directive (EU) 2019/1024 insofar as the access regime excludes or restricts access to such data for reasons of privacy and the integrity of the individual, in particular in accordance with data protection rules. This Regulation is without prejudice and complementary to more specific obligations on public sector bodies to allow re-use of data laid down in existing Union or Member State legislations of a sector-specific nature.

(14) This Regulation specifies a number of conditions for re-use of such data that apply across the European Union. Such conditions should be non-discriminatory, proportionate and objectively justified, while not restricting competition. Public sector bodies allowing re-use should have in place the technical means ensuring the protection of rights and interests of third parties.

(15) Public sector bodies should comply with Union and national competition rules when establishing the principles for re-use of data they hold, avoiding as far as possible exclusive agreements between themselves and private partners and agreements that, although they do not expressly grant an exclusive right to re-use the data, could reasonably be expected to result in the limited availability of data for other parties. However, in order to provide a public service, an exclusive right to re-use specific public sector data may sometimes be necessary. 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, e.g. by offering advanced digital services. Such arrangements should, however, be concluded on the basis of public procurement subject to regular review based on a market analysis in order to ascertain whether such exclusivity continues to be necessary and should comply with the relevant State aid rules, as appropriate. Additionally, such exclusive agreements should be published online.

(16) 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 before the entry into force of this Regulation should not be renewed after the expiration of their term. In case of indefinite or longer-term agreements, they should be terminated within 3 years from the date of entry into force of this Regulation.

(17) Conditions attached to the re-use should be limited to what is necessary to preserve the rights and interests of others in the data, the integrity of the information technology and communication systems of the public sector bodies and certain conditions that preserve other interests of the public sector bodies. They could e.g. include the requirement to acknowledge the source of the data. Depending on the case at hand, this may mean that only on-premise access within a secure processing environment may be permitted. Conditions that are intended to preserve interests of public sector bodies other than the integrity of their information technology and communications systems should be proportionate, should not unnecessarily restrict possibilities for re-use and should not be used to restrict competition. Whenever the transmission to a third party is necessary, the personal data have to be anonymised before transmission, unless there is a legal basis in Union or Member State law for transmitting personal data. Data subject to intellectual or industrial property rights as well as trade secrets shall only be transmitted to a third party with the agreement of the right holder. The public sector bodies, where relevant, shall also facilitate the re-use of data on the basis of consent of data subjects or permissions of companies on the re-use of data pertaining to them through adequate technical means.

(18) Companies and data subjects should be able to trust that the re-use of data, which are held by the public sector and which are personal data in nature, contain commercially confidential information or content protected under intellectual and industrial property rights occurs in a manner that respects the rights and interests of third parties. 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 is the requirement that the processing of such public sector data take place with the Union, in case it is necessary for the re-use purpose in question and lawful to transmit the data by the public sector body to a person or a legal entity for re-use. Such a requirement is based on the need for ensuring security, privacy and the protection of intellectual property rights, and it brings trust to individuals and legal entities to which the data in question pertain that they will be only processed by re-users that are subject to Union and national law. Re-users should also ensure that, whenever it is not prohibited by law, they are informed about use of data pertaining to them by foreign governmental authorities that is not based on their voluntary agreement. Furthermore, when non-personal data (such as commercially sensitive non-personal data, non-personal data subject to statistical confidentiality or protected by intellectual property rights) is transferred, re-users should have adequate safeguards in place, including organisational, technical and legal measures to ensure that such data can be obtained by non-EU governmental or judicial authorities only on the basis of a judicial decision from a EU Member States that can be challenged by concerned parties through judicial means. The execution of judicial decisions from third countries should be based on an international agreement (e.g. the Budapest Cybercrime Convention), which enables access to the data, and to which the Union or a Member State is a party.

(19) Public sector bodies may charge fees for the re-use of data they make available under this Regulation but may also decide to make the data available at no cost, e.g. for certain categories of re-uses such as non-commercial re-use, or re-use by small and medium-sized enterprises. Where fees are applied and in line with State aid rules, they should in

principle be based on national rules within the limits set by this Regulation. They should be reasonable, pre-established, published online and non-discriminatory. Where fees are applied, public sector bodies should take measures to incentivise re-use for non-commercial re-use and for re-use by small and medium-sized enterprises, for example, by way of lower fees, so as 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.

(20) Member States should give support for re-use through the appropriate support structures. A single contact point would be the prime interface for re-users that seek to re-use data held by the public sector the use of which is conditional on the respect of the rights of others. The single contact point should have a cross-sector remit, and would complement, if necessary existing arrangements at the sectoral level. In addition, Member States should establish or facilitate the establishment of support structures for public sector bodies allowing re-use of data that is conditional on the respect of the right of others. These support structures should provide expertise in relation with the applicable rules and regulations. The structures should also support 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. 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 support structures, which could have domain-specific specialisations.

(21) Providers of data sharing services (data intermediaries) are expected to play a key role in the establishment and operation of the common European data spaces, as their rapid development and the creation of data pools will depend on the capacity to fill them with a substantial amount of relevant data. Data intermediaries offering services that connect the different actors within the data spaces 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. Currently data sharing is insufficiently developed, partly as a result of a distrust of the intermediaries available on the market. Such distrust results from concerns on whether rules on data protection are complied with, whether conditions on the use of non-personal data can be set by the data holder and not by the intermediary and whether such conditions are respected, also vis-à-vis data access request from authorities of third countries to which an intermediary may be exposed.

(22) This lack of trust could be remedied by ensuring data holders and data users better control over the access to and use of their data, in accordance with European legislation. Both in situations where data sharing occurs in a business-to-business context or in a business-to-consumer context, data intermediaries can offer a novel, 'European' way of data governance, by providing a separation in the data economy between data provision, intermediation and use. Such data intermediaries should take due account of the solutions existing in the sectorial dataspaces and may take the form of data marketplaces, which facilitate bilateral interactions between data holders and users, as well as multilateral arrangements between a number of data holders and users. Data pools are formed by establishing databases resulting from contributions by several data holders for use by data users. Providers of data sharing services may also offer the

establishment of a specific technical infrastructure for interconnection of data holders and data users. In order to preserve control of European companies and individuals over the use of data they intend to share with the help of a data intermediary and to ensure the effectiveness of European rules on protection of intellectual property rights as well as trade secrets, they should take adequate organisational, technical and legal measures to ensure compliance with the provisions in Regulation (EU) 2016/679 on international transfers of personal data and that also ensure that non-personal data can be obtained by non-EU governmental or judicial authorities only on the basis of a decision that can be challenged by concerned parties through judicial means. The execution of judicial decisions from third countries should be based on an international agreement which enables access to the data, and to which the Union or a Member State is a party. Such organisational, technical and legal measures should not restrict the possibility for companies not established in the Union to offer such services.

(23) A key element to bring trust in such data sharing services is their neutrality as intermediaries between holders of data and data users. In order to demonstrate their neutrality in this context, data sharing service providers would have to ensure that they only act as intermediaries in the transactions, and do not use the data the exchange they aim to facilitate for any other purpose. This will also require structural separation between the data sharing service and any other services related to the data sharing service provider, so as to avoid issues of conflict of interest. For those intermediating between individuals as data holders and companies as data users, the provider of data sharing services should bear a fiduciary duty towards the individuals, meaning that the data sharing service provider should act in the best interest of the data subject clients. When 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. Requiring data sharing service providers to be established in the European Union or a country of the European Economic Area aims to ensure that the monitoring of compliance with the requirements is ensured and does not create an unnecessary burden for the competent authorities responsible for this task.

(24) Providers of data sharing services should comply with Regulation (EU) 2016/679. The provisions of this Regulation are without prejudice to the responsibility of supervisory authorities under Regulation (EU) 2016/679 to ensure compliance of data sharing service providers with that Regulation. Providers of data sharing services should also ensure compliance with the rules on competition and in particular Articles 101 and 102 of the Treaty on the Functioning of the European Union. Data sharing may generate various types of efficiencies but may 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.

(25) A specific category of data intermediaries includes providers of data sharing services that offer their services to individual persons as 'data subjects' in the sense of Regulation (EU) 2016/679 (also referred to as 'personal data spaces'). They focus exclusively on personal data and seek to enhance individual agency. This can give rise to a number of added value services that assist data subjects in managing the use of personal data pertaining to them better. Consent dashboards that would provide an aggregate view on all consent statements given digitally based on 'consent receipts' or managing the relationship between organisations that the data subject would like to give data access

to and organisations that hold relevant data (e.g. a utility). In certain situations it may be desirable to collate actual data within a 'personal data space' so that processing can happen within that space without personal data being transmitted to third parties in order to preserve a maximum of privacy. Providers of data sharing services in this context would offer to 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 may include advising individuals on what data users to allow processing of personal data pertaining to them and making due diligence checks on such data users before allowing them to contact an individual.

(26) An emerging variant are 'data cooperatives' or 'data unions' that seek to achieve a number of objectives, in particular strengthen the position of individuals to make informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use in a manner that gives better choices to the individual members of the group or potentially solving conflicts in positions of individual members of a group on how data can be used when such data pertain to several data subjects within that group can have effects on other members of the group.

(27) A general authorisation framework should be established in order to ensure a data governance within the European Union based on trustworthy intermediaries that can match supply and demand, support data exchange through the provision of technical platforms, permit the establishment of data pools for joint exploitation by the participating companies and possibly by others as well as personal data spaces and data cooperatives as intermediaries between data subjects and potential data users in the economy.

(28) For handling the general authorisation framework for data sharing intermediaries, each Member State should designate one or more competent authorities. These competent authorities should be chosen based on their capacity and expertise regarding horizontal or sectoral data sharing, and they should be independent as well as transparent and impartial during the course of performing their tasks. Member States should notify the Commission of the identity of the designated competent authorities. In order to start their activities, providers of data sharing services should notify any of the competent authorities in the Member State of the main establishment of the provider of data sharing services. 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. The general authorisation framework is without prejudice to Member States' supervisory authorities' competence to ensure compliance of organisations with Regulation (EU) 2016/679.

(29) Sector-specific legislation may lay down additional requirements for data sharing services to operate within that sector or a sectoral common European data space. Furthermore, the general authorisation framework laid down in this Regulation is without prejudice to already existing authorisation frameworks and certification

schemes established in specific sectors, in case those sectoral schemes impose requirements that are similar in effect to those of the current Regulation.

(30) There is a strong potential in the use of data made available voluntarily by individual data subjects based on their consent or, where it concerns non-personal data only, by companies for the common good in the form of 'data altruism'. Examples of such common good purposes are improving healthcare, combating climate change, improving mobility, contributing to scientific research, serving statistical purposes and more in general improving public services. Making available for the common good refers to purposes that advance the welfare of the general public or parts thereof. For this reason, making data available on altruistic grounds should, at most, lead only to an incidental personal benefit for the data subject or a company. Some Member States are experimenting with data altruism, e.g. in the area of healthcare. Such initiatives so far have shown that it is difficult to obtain such data at the scale required, for example for machine learning.

(31) In order to give assurances to individuals and companies that make available data for the common good, entities setting up these data altruism mechanisms should be subject to general authorisation that ascertains that the conditions are set in place that permit individuals and companies to trust in the altruistic use of the data they make available. Member States should ensure that, where relevant, specific expertise for individual domains such as healthcare, is taken into account in the context of the monitoring process of compliance with the requirement for the general authorisation.

(32) Activities supporting data altruism may be undertaken by entities that intend to process themselves the data for their final intended purpose. This includes public sector bodies and private organisations, including research performing organisations and not-for-profit organisations. It also includes organisations that could develop specialised expertise in the field of data altruism and support other organisations that will later process the data for the intended purpose. Such activities as well as the entities that intend to carry out these activities should have a non-commercial character. In order to preserve control of European companies and individuals over the use of data they intend to share with the help of a data altruism, entities engaging in data altruism directly or entities acting as an intermediary for data altruism should take adequate organisational, technical and legal measures to ensure compliance with the provisions in Regulation (EU) 2016/679 on international transfers of personal data and also ensure that non-personal data can be obtained by non-EU governmental or judicial authorities only on the basis of a decision that can be challenged by concerned parties through judicial means. The execution of judicial decisions from third countries should be based on an international agreement (e.g. the Budapest Cybercrime Convention) which enables access to the data, and to which the Union or a Member State is a party.

(33) Processing of personal data in the context of data altruism should be exclusively based on consent in the sense of Articles 6(1)(a) and 9(2)(a) of Regulation (EU) 2016/679. In this respect it should considered that it is often not possible to fully identify the purpose of personal data processing for scientific research at the time of data collection and therefore, in accordance with Recital (33) of Regulation (EU) 2016/679, data subjects should under certain conditions be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards. Data subjects should have the opportunity to give their consent only to certain areas of research, or parts of research projects to the extent allowed by the intended purpose. It should also be borne in mind that Article 5(1)(b) of that Regulation specifies that further processing for scientific or historical research purposes or statistical purposes shall, in accordance

with Article 89(1) of that Regulation, not be considered to be incompatible with the initial purposes. In such situations, additional safeguards are necessary to preserve the rights of the data subject. In particular, in accordance with Article 35 data protection impact assessments could be established. In cases of large scale processing of special categories of data in the sense of Article 9(1) of that Regulation such data protection impact assessment would be mandatory. Additionally information should be given pro-actively to inform data subjects about the use made of the data made available in accordance with Article 13 of that Regulation. Oversight mechanisms such as ethics councils or boards should be in place to ensure that the data controller maintains high standards of scientific ethics and continuously evaluates the need to process the data. In addition, data subjects should be given the opportunity to withdraw, limit or specify their consent at any moment in time through easy-to-use technical means, e.g. 'personal data spaces'. Data subjects should be informed regularly about this opportunity, at minimum whenever a concrete scientific processing purpose is identified.

(34) 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 would provide transparency to data subjects that their data is accessed and used in accordance with their intent 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.

(35) Sector-specific legislation may lay down additional requirements for organisations to undertake data altruism activities within that sector or a sectoral common European data space, such as data formats or additional safeguards.

(36) In order to successfully implement the horizontal data governance framework, a European Data Innovation Board should be established, in the form of a Commission expert group. The Board should consist of representatives of the Member States and the European Commission. In addition, representatives of common European dataspaces, specific sectors and domains (such as health, transport and statistics) should be selected to participate, on the basis of an expression of interest or in their capacity as representatives of existing Commission expert groups or similar entities. This should include representatives of common European data spaces in sectors where they have a mandate to speak on behalf of an entire sector.

(37) 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 through technical standardisation, 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 ('data sharing schema') that allows data spaces to be organised without making recourse to an intermediary. The Board should cooperate with existing 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. The Commission should establish an annual working plan and consult publicly on this matter.

(38) In order to develop the data altruism consent form, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission.

(39) 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.

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

(41) 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 right to property and the integration of persons with disabilities. Nothing in this Regulation should be interpreted or implemented in a manner that is inconsistent with the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

HAVE ADOPTED THIS REGULATION:

TITLE I
GENERAL PROVISIONS

Article 1
Subject matter and scope

In order to enhance the availability of data in the Union, 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 general authorisation framework for providers of data sharing services addressing business users or addressing data subjects, in order to increase trust in the provision of data sharing services in the Union and to avoid the fragmentation of the internal market.

(c) A general authorisation framework for the collection and processing of data made available for altruistic purposes by individuals or undertakings.

Article 2
Definitions

For the purpose of this regulation, the following definitions apply:

(1) 'Re-use' means the use by natural or legal persons of data 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.

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

(3) 'Data holder' means a legal person or data subject who, in accordance with applicable Union or national law, has the right grant access or to share certain personal or non-personal data under its control

(4) 'Data user' means a natural or legal person who has lawful access to certain data and is authorised to use that data for commercial or non-commercial purposes

(5) 'Data sharing' means the act of a data holder, providing data access to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, or mandatory rules

(6) 'Data access' means the act of a data user of retrieving or processing data that has been provided by a data holder, in accordance with specific technical, legal, or organisational requirements. Data access does not necessarily imply the transfer or download of such data

(7) 'Data altruism' refers to actions of data subjects that allow the processing of their personal data or of other data holders to allow the use of their data for purposes of general interest, without seeking a direct reward, and where the data is used purely on a non-commercial basis and not in competition with one or more service suppliers

(8) '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

TITLE II

ENHANCED USE OF DATA HELD BY PUBLIC SECTOR BODIES THE RE-USE OF WHICH IS CONDITIONAL ON RESPECTING THE RIGHTS OF OTHERS

Article 3
Scope of application

(1) This Title applies to existing data held by public sector bodies which are sensitive data on grounds of

(a) Commercial confidentiality (including business, professional or company secrets),

(b) Statistical confidentiality;

(c) Protection of intellectual property rights of third parties,

(d) Protection of personal data

(2) This Title 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 the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules

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

(3) The provisions of this title are without prejudice to Union and national law on access to data and to obligations of public sector bodies to allow the re-use of data under Union and national law.

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 provided in Article 3 (1) which grant exclusive rights or which have as object or effect granting such exclusive rights or restricting the availability for the re-use of data to other entities than those parties to such agreements or other practices are prohibited.

(2) By derogation from (1), where an exclusive right to re-use such existing data is necessary for the provision of a service in the public interest by a public sector body, such right shall be awarded on the basis of Directives 2014/23/EU, 2014/24/EU and 2014/25/EU. The duration of such exclusive rights shall not exceed 3 years.

(3) The agreements concluded pursuant paragraph (2) shall be transparent and be made publicly available online.

(4) Agreements or other practices falling in the scope of the prohibition included in paragraph (1) which do not meet the conditions set in paragraph (2), which were concluded before date of entry into force of the Regulation shall be terminated at the end of the contract and in any event not later than 3 years from the date of entry into force of the Regulation.

Article 5
Conditions for re-use

(1) Public sector bodies which allow the re-use of one or more of the categories of data provided in Article 3 (1) shall allow such re-use within the Union on a non-discriminatory basis.

(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 to which re-use is allowed. These conditions shall not be used to restrict competition.

(3) Public sector bodies may establish the obligation to access and re-use the data within a secure processing environment provided and controlled by the public sector or, in the case that remote access can be permitted without jeopardising the rights and interests of third parties in the data re-use, set conditions that preserve such rights and interests and the integrity of the technical systems used.

(4) In case it is necessary for the re-use purpose in question and lawful to transmit the data in question by the public sector body to a person or a legal entity for re-use, the processing of such data shall be limited to the European Union.

(5) In case personal data is transmitted to, or allowed to be accessed and processed by a natural or legal person for re-use, the processing of such data shall be compliant with the requirements laid down in Regulation (EU) 2016/679. If there is no legal basis under

Regulation (EU) 2016/679 for the transmission of personal data, the relevant data shall be provided as anonymised data before transmission, namely as information which does not relate to an identified or identifiable natural person or as data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

(6) In case a purpose of a re-use request cannot be fulfilled on the basis of anonymised data and also not by using a secure processing environment of the public sector and there is no legal basis for transmitting the data to a third party, and where it is practically feasible without disproportionate cost, the public sector body shall seek consent of the data subjects and/or permissions of legal entities that have rights and interests in the use of the data.

(7) The public sector body may only transmit non-personal data to natural or legal persons that have adequate safeguards in place, including of a technical, organisational and legal nature, that prevent them from responding to requests from authorities of third countries with a view of obtaining access to non-personal data relating to companies established in the Union and Union public administration, unless the request is based on a judicial decision from the Member State in which the company to which the data relate is established or the Member State of the public sector body concerned.

(8) Public sector bodies which allow the re-use of data on the basis of the present Article shall have adequate technical and legal capacity to ensure the rights and interests of data subjects and other third parties that have rights and interests over the data under Article 3 (1) are protected. Public sector bodies may have recourse for such purpose to the competent body designated pursuant to Article 8 (1).

Article 6
Fees

(1) Public sector bodies which allow re-use of the categories of data provided 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) Where applying such fees, public sector bodies shall take measures to incentivise the re-use of the categories of data provided in Article 3 (1) for non-commercial purposes and by small and medium-sized enterprises, in line with Article 107 and 108 of the Treaty on the functioning of the European Union.

(4) Fees shall be derived from the costs related to the processing of requests for re-use of the categories of data provided in Article 3 (1) and shall be published in advance.

(5) 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
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 access for the re-use of the categories of data listed in Article 3 and shall transmit them to the competent public sector bodies. 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 access for the re-use of the categories of data provided in Article 3 (1) shall be granted or refused within a reasonable time, and no later than 2 months from the date of the request.

(4) Where request for access for the re-use of data is refused, Member States shall ensure that any affected natural or legal person is entitled to refer the issue to the competent national body designated in accordance with Article 8 (1).

(5) The designated body shall resolve the dispute, within the shortest possible time frame and in any case within four months from the date of the receipt of the request, except in exceptional circumstances, without prejudice to the possibility of any party to refer the case to a court.

Article 8

Support for public sector bodies

(1) Member States shall designate one or more competent bodies to support the public sector bodies which grant access for the re-use of the categories of data provided in Article 3 (1) in the exercise of these tasks.

(2) Such support shall include:

(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 that ensure 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 to obtain, where relevant, consent or permission in line with specific preferences of data holders, including on the jurisdiction or jurisdictions in which the data processing is intended to take place.

(3) For this purpose, such 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 listed in Article 3 (1).

TITLE III

A EUROPEAN AUTHORISATION FRAMEWORK FOR DATA SHARING SERVICE PROVIDERS

Article 9

Creating trust for providers of data sharing services

(1) A European general authorisation framework shall be established in order to increase trust in the provision of data sharing services, as identified in paragraph (2), thereby improving the conditions for the functioning of the internal market by increasing data exchanges within the Union, with a view to create a single market for data.

(2) The general authorisation framework shall apply to the provision of the following services:

(a) services aimed at supporting data holders which are legal persons to make available their data to potential data users, which may include bilateral or multilateral exchanges of such 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) services aimed at the creation of personal data spaces, namely services enabling data subjects to exercise the rights provided in Regulation (EU) 2016/679, which may be paired by making available dedicated data storage services to the data subjects;

(c) services related to the creation of data cooperatives, namely services enabling several data subjects to exercise collectively the rights provided in Regulation (EU) 2016/679, which may be paired by making available data storage services to such data subjects.

(3) Member States shall not introduce new national authorisation frameworks for the services covered by the European general authorisation framework for data sharing services.

(4) The provider of data sharing services shall be compliant with the requirements laid down in Regulation (EU) 2016/679, including the provisions on transfers of personal data to third countries or international organisations.

(5) The general authorisation is without prejudice to powers of supervisory authorities to ensure compliance of providers of data sharing services with applicable law, including on the protection of personal data and competition law.

(6) The provision of data sharing services as well as the exchange of information between undertakings are without prejudice to the application of competition law.

Article 10

Requirements for data sharing service providers

Data sharing service providers under Article 9 (2) shall comply with the following requirements:

(a) The provider of data sharing services may not use the data for other purposes than to put them at the disposal of data users.

(b) The provider of data sharing services shall structurally separate its data intermediation services from any other value-added services it may provide. The same provider of data sharing services may not offer the services provided for in Article 9 and other services related to the use of data which go beyond what is necessary to deliver the data sharing service.

(c) The metadata collected on the basis of the data sharing offered may be used only for the development of the data sharing service.

(d) The provider of data sharing services shall ensure a fair and non-discriminatory access procedure to the data sharing service for both data holders and data users, including as regards prices.

(e) The data sharing service provider shall facilitate the data exchange in the format in which it has received it from the data holder or data subject. It shall only

convert the data into specific formats in order to facilitate use by data users or if requested by the data user or where mandated by Union law.

(f) The provider of data sharing services shall have procedures in place to prevent fraudulent or abusive practices in relation to access to data from parties seeking access through their services.

(g) The provider of data sharing services shall ensure a reasonable continuity of provision of its services. In case of services which ensure storage of data, they shall have sufficient guarantees in place that allow data holders and data users to obtain access to their data in case of insolvency.

(h) In order to facilitate supervision of the compliance with the requirements laid out in this Article and other relevant Union law, the provider of data sharing services shall be established within the Union or a country of the European Economic Area. The data sharing services provider shall be deemed to be under the jurisdiction of the Member State where it is established.

(i) The provider of data sharing services shall have adequate safeguards in place, including of a technical, organisational and legal nature, that prevent it from responding to requests from authorities of third countries with a view of obtaining access to non-personal data relating to companies established in the Union and Union public administration, unless the request is based on a judicial decision from the Member State in which the company to which the data relate is established.

(j) The provider of data sharing services shall take measures to ensure a high level of security for the storage and transmission of non-personal data.

(k) The provider of data sharing services shall ensure compliance with the rules on competition, in particular Articles 101 and 102 of the Treaty on the functioning of the European Union.

(l) The provider of data sharing services offering services to data subjects shall assume a fiduciary duty with regard of those data subjects and act in the best interest of the data subjects when exercising rights on their behalf, in particular the duty to advise data subjects on potential data uses and standard terms and conditions attached to such uses.

(m) When a data sharing service provider facilitates obtaining consent from data subjects or permissions to process data made available by legal persons, the data sharing service provider shall specify the jurisdiction or jurisdictions in which the data processing is intended to take place.

(n) Where the provider of data sharing services is subject to sector-specific provisions that are similar in effect to the provisions of this Regulation, including provisions for mandatory or voluntary certification, the provider of data sharing services shall make proof of compliance with those provisions.

Article 11

Competent authorities

(1) Each Member state shall designate in their territory one or more authorities competent to carry out the tasks related to the general authorisation framework. The designated competent authorities shall comply with the requirements laid out in Article 23.

(2) Each Member State shall inform the Commission of the identity of the designated competent authority or authorities.

Article 12
General authorisation of data sharing service providers

(1) Any provider of data sharing services who wishes to undertake one of the activities described in Article 9 (2) is subject to general authorisation. Such authorisation shall be valid in all Member States of the European Union.

(2) Any provider of data sharing services shall be deemed to have its main establishment in the Member State where it has the place of its central administration.

(3) Upon notification, the provider of data sharing services may start the activity subject to the conditions set in this title.

(4) Providers of data sharing services are required to notify their intent to undertake one of the activities described in Article 9 (2) to a competent authority in the Member State of their main establishment designated under Article 20. A provider of data sharing services shall be deemed to have its main establishment in the Member State or country of the European Economic Area where it has the place of its central administration. Upon notification, the provider may start the activity subject to the provisions of this title.

(5) The notification shall include the following information

(a) Name of the provider;

(b) The provider's legal status, form and registration number, where the provider is registered in trade or other similar public register;

(c) The geographical address of the provider's main establishment in the Union, if any, and, where applicable, any secondary branch in another Member State;

(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 it seeks to provide;

(g) A description on the manner in which it complies with the requirements set out in Article 10.

(6) Member States may not impose any additional or separate notification requirements.

(7) At the request of the provider, the competent authority shall, within one week, issue standardised declarations, confirming that the provider has submitted a notification under paragraph (3) and detailing under what circumstances the data sharing service may be carried out under the general authorisation.

(8) The competent authority shall forward by electronic means and without delay each notification to the national competent authorities in all Member States.

(9) The competent authority shall notify the Commission of any 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 the general authorisation.

Article 13
Monitoring of compliance

(1) The competent authority shall monitor and supervise compliance with the conditions of the authorisation set in this Title.

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

(3) The providers of data sharing services shall provide the information requested promptly and in accordance with the timescales and level of detail required.

(4) Where the competent authority finds that a provider of data sharing services does not comply with one or more of the requirements of Article 10 it shall notify the provider of data sharing services of those findings and give the provider the opportunity to state its views, within a reasonable time limit.

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

(6) In this regard, the competent authorities shall impose:

(a) where appropriate, dissuasive financial penalties which may include periodic penalties with retroactive effect; and

(b) orders to cease or delay provision of the service of collecting data based on data altruism service.

(7) The competent authorities shall communicate the measures and the reasons on which they are based to the entity concerned without delay and shall stipulate a reasonable period for the provider of data sharing services to comply with the measures.

(8) If a provider of data sharing services has its main establishment in a Member State, but provides services in other Member States, the competent authority of the Member State of the main establishment 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 the present Article.

(9) Where the data sharing service provider is active in sectors where the data sharing is subject to sector-specific provisions of Union law that are similar in effect to the provisions of this regulation, including provisions for mandatory or voluntary certification, the competent authority shall consult relevant sectoral authorities.

TITLE IV
MEASURES FACILITATING DATA ALTRUISM

Article 14
Facilitating data altruism

(1) The collection of data based on data altruism is subject to the conditions set in the present Title.

(2) In case personal data is processed in the context of data altruism, such processing shall be compliant with the requirements laid down in Regulation (EU) 2016/679, including the provisions on transfers of personal data to third countries or international organisations.

Article 15
General authorisation of entities seeking to make use of data altruism

(1) The collection of data based on data altruism is subject to general authorisation. Such authorisation shall be valid in all Member States of the European Union.

(2) Any entity which intends to collect data based on data altruism is required to submit a notification to the competent authority designated pursuant to Article 20 in the Member State of their main establishment.

(3) Any entity which intends to collect data based on data altruism shall be deemed to have its main establishment in the Member State where it has the place of its central administration.

(4) Upon notification, the entity may start the activity subject to the conditions set in this title.

(5) Entities are required to notify their intent to undertake data altruism activities to a competent authority in the Member State or country of the European Economic Area of their main establishment designated under Article 20. An entity engaging in data altruism activities services shall be deemed to have its main establishment in the Member State or country of the European Economic Area where it has the place of its central administration. Upon notification, the entity may start the activity subject to the provisions of this title.

(6) The notification shall include the following information:

(a) Name of the entity;

(b) The entity's legal status, form and registration number, where the entity is registered in trade or other similar public register;

(c) The geographical address of the entity's main establishment in the Union, if any, and, where applicable, any secondary branch in another Member State;

(d) A website where information on the entity and the activities can be found, where applicable;

(e) The entity's contact persons and contact details;

(f) A description of the service intended to be provided, including information whether the entity intends to collect personal data and if so this could pertain to data falling within one or several of the categories listed in Article 9 of Regulation (EU) 2016/679;

(g) The purposes of general interest of the intended processing;

(h) The means intended to be used for collection of the data;

(i) The intended geographic location(s) of the processing;

(j) Estimated date of starting the activity;

(k) The Member States where the entity intends to collect the data.

(7) The competent authority designated according to Article 20 shall maintain and publish a register of entities that notified the intention to commence the collection of data based on data altruism.

(8) Member States may not impose any additional or separate notification requirements.

(9) At the request of the entity, the competent authority shall, within one week, issue standardised declarations, confirming that the entity has submitted a notification under paragraph (3) and detailing under what circumstances the collection of data based on data altruism may be carried out under the general authorisation.

(10) The competent authority shall forward by electronic means and without delay each notification to the national competent authorities in all Member States concerned by the collection of the data.

Article 16

General authorisation for collecting data based on data altruism

The general authorisation for the collection of data based on data altruism is subject to the conditions set in Articles 17 – 19.

Article 17

Requirements for lawful data altruism activities

The entities collecting data based on data altruism shall comply with the following requirements:

(a) The entity is operating on a not for profit basis.

(b) In case the entity undertakes other activities on a not for profit basis, it shall ensure the functional separation of such activities from the activities related to the collection of data based on data altruism. The entity may not use the data collected based on data altruism for other activities on a not for profit basis.

(c) The entity is:

(1) A legal entity established within the European Union or a country of the European Economic Area;

(2) An international governmental organisation established in a country with which international transfers of personal data are lawful under Regulation (EU) 2016/679.

(d) Adequate safeguards are in place, including of a technical, organisational and legal nature, that prevent them from responding to requests from authorities of third countries with a view of obtaining access to non-personal data relating to companies established in the Union and Union public administration, unless the request is based on a judicial decision from the Member State in which the company to which the data relate is established.

Article 18

Requirements in relation to the collection of data

(1) The entity shall clearly separate the data collection based on data altruism from any other data collection and shall inform the data holder in advance of the purposes of such collection.

(2) The processing of personal data based on data altruism shall be allowed only for specified, explicit and legitimate purposes in the sense of Article 5(1)(b) of Regulation (EU) 2016/679 and only on the basis of consent in the sense of Article 6(1)(a) of that Regulation and Article 9(2)(a) in case of special categories of data.

(3) In the area of scientific research the processing of personal data based on data altruism shall be allowed if consent is given as regards the processing of data for the purposes of defined areas of scientific research or parts of research projects, in accordance with Article 89 of Regulation (EU) 2016/679.

(4) In case data collection is based on the approach described in paragraph (3), the entity shall ensure that in addition to the safeguards provided for in Regulation (EU) 2016/679 the following safeguards are in place:

(a) Data subjects need to be provided with appropriate technical means to withdraw consent at any moment, preferably through online tools.

(b) The entity shall evaluate on a regular basis the need to process the data in question. In this context, the evaluation shall examine whether instead of a deletion of the data in question, techniques can be applied that preserve the rights and interests of the data subject.

(5) The entity shall inform the data holder in advance of collecting data based on data altruism about the jurisdiction or jurisdictions in which the data processing is intended to take place.

(6) The processing of non-personal data shall be subject to the conditions set by the organisation or natural person making such data available.

Article 19

Requirements on entities collecting data based on data altruism that act as intermediaries

Entities collecting data based on data altruism that act as intermediaries on behalf of another entity shall ensure that the following requirements are met in regard to the entity that acts as data user:

(a) The entity is operating on a not for profit basis.

(b) In case the data user undertakes other activities set up to generate profits, it shall ensure a functional separation of such services from collection of data on the basis of data altruism.

(c) The data user is one of the following

(1) A legal entity established within the European Union or the European Economic Area

(2) An international governmental organisation established in a country with which international transfers of personal data are lawful under Regulation (EU) 2016/679

(d) Adequate safeguards are in place, including of a technical, organisational and legal nature, that prevent them from responding to requests from authorities of third countries with a view of obtaining access to non-personal data relating to companies established in the Union and Union public administration, unless the request is based on a judicial decision from the Member State in which the company to which the data relate is established or the Member State of the public sector body concerned.

Article 20
Competent authorities for the general authorisation for services of collecting data based on data altruism

(1) Each Member State shall designate one or more competent authorities responsible for the management, control and enforcement of the general authorisation regime for entities collecting data based on data altruism. The designated competent authorities shall meet the requirements in 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, when such tasks are related to processing of personal data, and relevant sectoral bodies of the same Member State.

Article 21
Monitoring of compliance

(1) The competent authority shall monitor and supervise compliance with the conditions of the general authorisation set in this Title.

(2) The competent authority shall have the power to request information from entities collecting data based on data altruism that is necessary to verify compliance with the requirements provided in Article 17-19. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

(3) The entities shall provide the information requested promptly and in accordance with the timescales and level of detail required.

(4) Where the competent authority finds that an entity does not comply with one or more of the requirements of the general authorisation it shall notify the entity of those findings and give the entity the opportunity to state its views, within a reasonable time limit.

(5) The competent authority shall have the power to require the cessation of the breach referred to in paragraph 6 either immediately or within a reasonable time limit and shall take appropriate and proportionate measures aimed at ensuring compliance.

(6) In this regard, the competent authorities shall impose:

(a) where appropriate, dissuasive financial penalties which may include periodic penalties with retroactive effect; and

(b) orders to cease or delay provision of the service of collecting data based on data altruism service.

(7) The competent authorities shall communicate the measures 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.

(8) If an entity collecting data based on data altruism has its main establishment in a Member State, but provides services in other Member States, the competent authority of the Member State of the main establishment 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 the present Article.

Article 22
European data altruism consent form

(1) In order to facilitate data altruism activities, the Commission may develop European data altruism consent forms, by means of delegated acts.

(2) Those delegated acts shall be adopted in accordance with the procedure referred to in Article 26 (2).

(3) The European data altruism consent forms may be customised for specific sectors and for different purposes and shall use a modular form.

(4) 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 and shall ensure compliance with the requirements set in Regulation (EU) 2016/679.

(5) They 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.

TITLE V
PROVISIONS RELATING TO COMPETENT

Article 23
Requirements relating to competent authorities

(1) The designated competent authorities pursuant Article 11 and Article 20 shall be legally distinct from, and functionally independent of any provider of data sharing services or providers of services of collecting data based on data altruism.

(2) Competent authorities shall exercise their tasks in an impartial, transparent, consistent, neutral, reliable and timely manner.

(3) The top-management and the personnel responsible for carrying out the relevant tasks of the competent authority foreseen in this Regulation cannot be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the activities 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) Such top-management and the personnel shall not engage in any activity that may conflict with their independence of judgment or integrity in relation to evaluation activities for which they are designated.

(5) The competent authorities shall have adequate financial and human resources at their disposal necessary to carry out the tasks assigned to them, including the necessary technical knowledge and resources.

(6) The competent authorities shall provide the Commission and competent authorities from other Member States with the information necessary to carry out their tasks under the present Regulation, after a reasoned request. Where the information requested is considered to be confidential by a national competent authority in accordance with Union and national rules on commercial confidentiality, the Commission and any other competent authorities concerned shall ensure such confidentiality.

TITLE VI
EUROPEAN DATA INNOVATION BOARD

Article 24
European Data Innovation Board

(1) A European Data Innovation Board shall be established in the form of an Expert Group.

(2) The Board shall be composed of representatives of each Member State competent for the tasks under Article 25, and of representatives of the European Commission.

(3) In order to ensure the consistency with developments in specific sectors and domains, the Commission may select European representatives of common European data spaces, sectors or domains to become members of the Board.

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

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

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

Article 25
Tasks of the Board

The Board shall have the following tasks:

(a) To advise and assist the Commission in the work to facilitate the emergence of a consistent practice of processing requests for the re-use of data as referred to under Article 3;

(b) To advise and assist the Commission in the work to facilitate the emergence of a consistent practice in relation with the general authorisation framework under Articles 12 and 16 of this Regulation;

(c) To advise the Commission on the prioritisation of cross-sector standards to be used and developed for data use and data sharing, while taking into account sector-specific standardisations activities;

(d) To assist the Commission in the work to facilitate 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 issues concerning the general authorisation framework for data sharing service providers and the provision of cross-border data altruism services;

(f) To advise and assist the Commission in the work to develop the European data altruism consent forms pursuant to Article 22.

TITLE VII
DELEGATED ACT & COMITOLOGY

Article 26
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 22(2) shall be conferred on the Commission for an indeterminate period of time from [...].

(3) The delegation of power referred to in Article 22(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

(4) Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

(5) As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

(6) A delegated act adopted pursuant to Article 22(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 27
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.

TITLE VIII
FINAL PROVISIONS

Article 28
Relationship with other Union legislation

This Regulation shall be without prejudice to Regulation (EU) 2016/679, Directive (EU) 2016/680, Directive (EU) 2016/943, Regulation (EU) 2018/1807, Directive 2001/29/EC, Directive (EU) 2019/790, Directive 2004/48/EC, Directive (EU) 2019/1024, as well as Directive 2010/40/EU and delegated Regulations adopted on its basis, and any other existing sector-specific EU legislation that organises the access to and re-use of data.

Article 29
Right to lodge a complaint

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

(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 referred to in Article 30.

Article 30
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 authority referred to in Articles 11 and 20;

(b) decisions of the competent authorities referred to in Articles 11 and 20 taken in the management, control and enforcement of the general authorisation regimes for providers of data sharing services and for services of collecting data based on data altruism.

(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.

Article 31
Transitional provision

Entities providing data altruism services on entry into force of this Regulation shall take measures to comply with the obligations set in Title IV of this Regulation by [date - 2 years after the start date of the application of the Regulation].

Article 32
Penalties

Member States shall lay down the rules on penalties applicable to infringements of Articles 17-19 and shall take all measures necessary to ensure that they are implemented. The penalties provided for must 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 33
Evaluation and review

No sooner than 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 the main findings of that evaluation 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 34
Entry into force

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*

I