EUROPEAN
COMMISSION

Brussels, 23.2.2022
COM(2022) 68 final

2022/0047 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on harmonised rules on fair access to and use of data (Data Act)

(Text with EEA relevance)

{SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act).

Data is a core component of the digital economy, and an essential resource to secure the green and digital transitions. The volume of data generated by humans and machines has been increasing exponentially in recent years. Most data are unused however, or its value is concentrated in the hands of relatively few large companies. Low trust, conflicting economic incentives and technological obstacles impede the full realisation of the potential of data-driven innovation. It is therefore crucial to unlock such potential by providing opportunities for the reuse of data, as well as by removing barriers to the development of the European data economy in compliance with European rules and fully respecting European values, and in line with the mission to reduce the digital divide so that everyone benefits from these opportunities. Ensuring greater balance in the distribution of the value from data in step with the new wave of non-personal industrial data and the proliferation of products connected to the Internet of Things means there is enormous potential for boosting a sustainable data economy in Europe.

Regulating data access and use is a fundamental prerequisite for seizing the opportunities presented by the digital age we live in. The President of the Commission, Ursula von der Leyen, stated in her political guidelines for the 2019-2024 Commission that Europe must '*balance the flow and use of data while preserving high privacy, security, safety and ethical standards*'[1]. The Commission Work Programme 2020[2] set out several strategic objectives, including the European strategy for data[3], adopted in February 2020. That strategy aims at building a genuine single market for data and at making Europe a global leader in the data-agile economy. For this reason, the Data Act is a key pillar and the second major initiative announced in the data strategy. In particular, it contributes to the creation of a cross-sectoral governance framework for data access and use by legislating on matters that affect relations between data economy actors, in order to provide incentives for horizontal data sharing across sectors.

The European Council's Conclusions of 21-22 October 2021 underlined '*the importance of making rapid progress on existing and future initiatives, in particular unlocking the value of data in Europe, notably through a comprehensive regulatory framework that is conducive to innovation and facilitates better data portability, fair access to data and ensures interoperability*'[4]. On 25 March 2021, the European Council reiterated '*the importance of better exploiting the potential of data and digital technologies for the benefit of the society and economy*'[5]. On 1-2 October 2020, it stressed '*the need to make high-quality data more readily available and to promote and enable better sharing and pooling of data, as well as*

---

1 Ursula von der Leyen, A Union that strives for more - My agenda for Europe, Political guidelines for the next European Commission 2019-2024, 16 July 2019

2 European Commission, Annexes to the Commission Work Programme 2020 - A Union that strives for more, COM(2020) 37, 29 January 2020

3 COM/2020/66 final

4 European Council, European Council meeting (21-22 October 2021) - Conclusion EUCO 17/21, 2021, p. 2.

5 European Council, Statement of the members of the European Council meeting (25 March 2021) – Statement SN 18/21, p. 4.

interoperability'[6]. On cloud services, on 15 October 2020, the EU Member States unanimously adopted a Joint Declaration on building the next generation cloud for businesses and the public sector in the EU. This would require a next generation of EU cloud offering that reaches the highest standards in in portability and interoperability, for example[7].

The European Parliament resolution of 25 March 2021 on a European strategy for data urged the Commission to present a data act to encourage and enable greater and fairer flow of data in all sectors, from business-to-business, business-to-government, government-to-business and government-to-government[8]. In its resolution of 25 March 2021, the European Parliament also highlighted the need to create common European data spaces for the free flow of non-personal data across borders and sectors and between businesses, academia, relevant stakeholders and the public sector. From this perspective, it encouraged the Commission to clarify utilisation rights, especially in business-to-business and business-to-government settings. It stressed that market imbalances arising from the concentration of data restrict competition, increase market entry barriers and diminish wider data access and use.

In its resolution, the European Parliament also pointed out that business-to-business contractual agreements do not necessarily guarantee adequate access to data for small and medium-sized enterprises (SMEs). The reason for this is that there are disparities in negotiation power and expertise. The European Parliament therefore stressed the need for contracts to set out clear obligations and determine liability for accessing, processing, sharing and storing data in order to limit its misuse.

As such, the Commission and EU Member States were asked to examine actors' rights and their obligations to access data they have been involved in generating and to improve their awareness of, in particular, the right to access data, to port it, to urge another party to stop using it, or to rectify or delete it, while also identifying the holders and delineating the nature of such rights.

On the business-to-government front, the European Parliament requested that the Commission set out the situations, conditions and incentives under which the private sector should be obliged to make data available for use by the public sector, such as due to its necessity for the organisation of data-driven public services, and also examine compulsory business-to-government data sharing schemes, for instance in situations that are beyond people's control.

In this context, the Commission puts forward the proposed **Data Act** with the **aim of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data**.

The proposal will help achieve the broader policy goals of ensuring EU businesses across all sectors are in a position to innovate and compete, effectively empowering individuals with respect to their data, and better equipping businesses and public sector bodies with a proportionate and predictable mechanism to tackle major policy and societal challenges, including public emergencies and other exceptional situations. Businesses will be able to easily switch their data and other digital assets between competing providers of cloud and other data processing services. Data sharing within and between sectors of the economy requires an interoperability framework of procedural and legislative measures to enhance trust

---

6 European Council, European Council meeting (1-2 October 2020) - Conclusion EUCO 13/20, 2020, p. 5.

7 European Commission (2020). *Commission welcomes Member States' declaration on EU cloud federation*, Press Release.

8 European Parliament resolution of 25 March 2021 on a European strategy for data (2020/2217(INI))

and improve efficiency. The creation of common European data spaces for strategic sectors of the economy and domains of public interest will contribute to a genuine internal market for data enabling data sharing and use across sectors. This Regulation therefore contributes to these governance frameworks and infrastructure as well as data sharing outside data spaces.

The proposal's specific objectives are outlined below.

– **Facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data.** This includes increasing legal certainty around the sharing of data obtained from or generated by the use of products or related services, as well as operationalising rules to ensure fairness in data sharing contracts. The proposal **clarifies** the application of relevant rights under Directive 96/9/EC on the legal protection of databases (the **Database Directive**)[9] to its provisions.

– **Provide for the use by public sector bodies and Union institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need.** This primarily concerns public emergencies, but also other exceptional situations where compulsory business-to-government data sharing is justified, in order to support evidence-based, effective, efficient, and performance-driven public policies and services.

– **Facilitate switching between cloud and edge services.** Access to competitive and interoperable data processing services is a precondition for a flourishing data economy, in which data can be shared easily within and across sectoral ecosystems. The level of trust in data processing services determines the uptake of such services by users across sectors of the economy.

– **Put in place safeguards against unlawful data transfer without notification by cloud service providers**. This is because concerns have been raised about non-EU/European Economic Area (EEA) governments' unlawful access to data. Such safeguards should further enhance trust in the data processing services that increasingly underpin the European data economy.

– **Provide for the development of interoperability standards for data to be reused between sectors**, in a bid to remove barriers to data sharing across domain-specific common European data spaces, in consistency with sectoral interoperability requirements, and between other data that are not within the scope of a specific common European data space. The proposal also supports the setting of standards for 'smart contracts'. These are computer programs on electronic ledgers that execute and settle transactions based on pre-determined conditions. They have the potential to provide data holders and data recipients with guarantees that conditions for sharing data are respected.

• **Consistency with existing policy provisions in the policy area**

This proposal is consistent with existing rules on the **processing of personal data** (including the General Data Protection Regulation, ('GDPR')[10]), and protecting the private life and the **confidentiality of communications**, as well as any (personal and non-personal) data stored in and accessed from terminal equipment (the ePrivacy Directive[11], to be replaced by the ePrivacy Regulation currently the subject of legislative negotiations). This proposal

9 OJ L 77, 27.3.1996, p. 20–28

10 OJ L 119, 4.5.2016, p. 1–88.

11 OJ L 201, 31.7.2002, p. 37–47

complements existing rights, specifically rights regarding data generated by a user's product connected to a publicly available electronic communications network.

The **Free Flow of Non-Personal Data Regulation**[12] put in place a key building block of the European data economy, by ensuring that non-personal data can be stored, processed and transferred anywhere in the Union. It also presented a self-regulatory approach to the problem of 'vendor lock-in' at the level of providers of data processing services, by introducing codes of conduct to facilitate switching data between cloud services (the industry-developed 'Switching Cloud Providers and Porting Data (SWIPO)' Codes of Conduct). This proposal further builds on this, helping businesses and citizens to make the most of the right to switch cloud providers and port data. It is also fully consistent with the Unfair Contract Terms Directive as regards contract law[13]. With regard to cloud services, as the self-regulatory approach seems not to have affected market dynamics significantly, this proposal presents a regulatory approach to the problem highlighted in the Free Flow of Non-Personal Data Regulation.

International data processing and storage and data transfers are governed by the GDPR, World Trade Organization (WTO) trade commitments, the General Agreement on Trade in Services (GATS) and bilateral trade agreements.

Competition law[14] is applicable in the context of amongst others merger control, data sharing by companies or an abuse of a firm's dominant position.

The **Database Directive**[15] provides for the *sui generis* protection of databases that have been created as a result of a substantial investment, even if the database itself is not an original intellectual creation protected by copyright. Building on the substantial amount of case-law interpreting the provisions of the Database Directive, this proposal addresses ongoing legal uncertainties about whether databases containing data generated or obtained by the use of products or related services, such as sensors, or other types of machine-generated data, would be entitled to such protection.

The **Platform to Business Regulation**[16] imposes transparency obligations, requiring platforms to describe for business users the data generated from the provision of the service.

The **Open Data Directive**[17] sets out minimum rules on the re-use of data held by the public sector and of publicly funded research data made publicly available through repositories.

The **Interoperable Europe initiative** seeks to introduce a cooperative interoperability policy for a modernised public sector. The initiative arose out of the ISA[2], a Union funding programme that ran from 2016 to 2021 and supported the development of digital solutions to enable interoperable cross-border and cross-sector public services[18].

This proposal complements the recently adopted **Data Governance Act,** which aims to facilitate the voluntary sharing of data by individuals and businesses and harmonises conditions for the use of certain public sector data, without altering material rights on the data

12 OJ L 303, 28.11.2018, p. 59–68; SWIPO (2021), see *website*.
13 OJ L 95, 21.4.1993, p. 29–34.
14 OJ L 335, 18.12.2010, p. 36–42.
15 OJ L 77, 27.3.1996, p. 20–28.
16 OJ L 186, 11.7.2019, p. 57–79.
17 OJ L 172, 26.6.2019, p. 56–83.
18 OJ L 318, 4.12.2015, p. 1-16.

or established data access and usage rights[19]. It also complements the proposal for a **Digital Markets Act**, which will require certain providers of core platform services identified as 'gatekeepers' to provide, inter alia, more effective portability of data generated through business and end users' activities[20].

This proposal does not affect existing rules in the areas of intellectual property (except the application of the *sui generis* right of the Database Directive), competition, justice, and home affairs and related (international) cooperation, trade-related obligations, or the legal protection of trade secrets.

Legislative adaptations for promoting the digital transition are required in several areas. Clear rules on access to specific data necessary for circularity and sustainability of certain products throughout their life cycle and in non-exceptional situations will be established under the European Digital Product Passport (as part of the Sustainable Products Initiative)[21]. Private law rules are a key element in the overall framework. This Regulation therefore adapts contract law and other rules to improve conditions for data reuse in the Internal Market, and to prevent parties to contracts abusing imbalances in negotiating power to the detriment of weaker parties.

As a horizontal proposal, the **Data Act** envisages **basic rules for all sectors** as regards the rights to use data, such as in the areas of smart machinery or consumer goods. However, the rights and obligations on data access and use have also been regulated to varying degrees at sectoral level. The Data Act will not change any such existing legislation, but future legislation in these areas should in principle be aligned with the horizontal principles of the Data Act. Convergence with the Data Act's horizontal rules should be assessed when sectoral instruments are reviewed. This proposal leaves room for vertical legislation to set more detailed rules for the achievement of sector-specific regulatory objectives.

Given existing sectoral legislation, with regard to the creation of the Green Deal data space, the review[22] of the **INSPIRE Directive**[23] will enable further open availability and reuse of spatial and environmental data. This initiative aims to make it easier for EU public authorities, businesses and citizens to support the transition to a greener and carbon-neutral economy and reducing administrative burden. It is expected to support reusable data services on a large scale to assist in collecting, sharing, processing and analysing large volumes of data relevant for assuring compliance with environmental legislation and priority European Green Deal actions. It will streamline reporting and burden reduction through better reuse of existing data, automatic reporting generation through data mining and business intelligence.

The EU **Electricity Regulation**[24] requires transmission system operators to provide data to regulators and for resource adequacy planning, while the EU **Electricity Directive**[25] provides for the transparent and non-discriminatory access to data and mandates the Commission to develop related interoperability requirements and procedures to facilitate this. The **Payment Services Directive 2**[26] opens some types of payment transactional and account information under certain conditions, thereby enabling business-to-business data sharing in the area of

19 COM/2020/767 final.
20 OJ L 186, 11.7.2019, p. 57–79.
21 COM/2020/98 final.
22 GreenData4All initiative (REFIT) | Legislative train schedule | European Parliament (europa.eu)
23 OJ L 108, 25.4.2007, p. 1–14
24 OJ L 158, 14.6.2019, p. 54–124.
25 OJ L 158, 14.6.2019, p. 125–199.
26 OJ L 337, 23.12.2015, p. 35–127 OJ L 337, 23.12.2015, p. 35–127.

Fintech. In the mobility and transport sector, there is a wide variety of data access and sharing rules. Repair and maintenance information from motor vehicles and agricultural machines is subject to specific data access/sharing obligations under **type approval legislation**[27]. However, new rules are needed to ensure that existing vehicle type-approval legislation is fit for the digital age and promotes the development of clean, connected and automated vehicles. Building on the Data Act as a framework for the access and use of data, these rules will address sector-specific challenges, including access to vehicle functions and resources.

In the framework of the **Intelligent Transport Systems Directive**[28], several delegated regulations have been developed and will continue to be developed, notably to specify data accessibility for road and multimodal passenger transport, in particular through National Access Points. In air traffic management, non-operational data is important for improving inter-modality and connectivity. Operational data related to air traffic management would come under the specific regime defined in the framework of the **Single European Sky**[29]. In vessel traffic monitoring, vessel related data (tracking and tracing) is important for improving inter-modality and connectivity: this data falls under the specific regime defined in the VTMIS Directive[30]. It also falls within the remit of the Digital Maritime System and Services.[31] The proposal for a Regulation on the deployment of **alternative fuels infrastructure**[32] specifies the relevant data types to be made available, in synergy with the general framework established in the Intelligent Transport Systems Directive.

- **Consistency with other Union policies**

This proposal is in line with the Commission's priorities to **make Europe fit for the digital age** and to build a future-ready economy that works for people[33], where the digitalisation of the internal market is characterised by a high degree of trust, security, safety and choice for consumers. The digitalisation of the internal market is highly competitive thanks to a framework that favours transparency, competition and innovation, and which is technology neutral. It supports the **Recovery and Resilience Facility**[34], learning lessons from the COVID-19 pandemic and the benefits of more easily accessible data where necessary.

This proposal supports the critical role of data in achieving the European **Green Deal objectives** in various ways. First, by deepening the understanding of governments, businesses and individuals of the impacts on society and the economy of products, services and materials across entire supply chains. Second, by mobilising the existing wealth of relevant private sector data in order to tackle climate-, biodiversity-, pollution-[35] and natural resource-related in line with objectives of the European Green Deal[36], the relevant Council conclusions[37] and positions[38] of the European Parliament. Third, by closing knowledge gaps and managing related crises through enhanced mitigation, preparedness, response and recovery actions.

---

27 OJ L 151, 14.6.2018, p. 1–218; OJ L 60, 2.3.2013, p. 1–51.
28 OJ L 207, 06.08.2010, p. 1-13.
29 OJ L 96, 31.3.2004, p. 1–9; OJ L 96, 31.3.2004, p. 10–19; OJ L 96, 31.3.2004, p. 20–25.
30 OJ L 308, 29.10.2014, p. 82–87.
31 OJ L 96, 12.4.2016, p. 46–49.
32 COM/2021/559 final
33 COM/2020/67 final.
34 OJ L 57, 18.2.2021, p. 17.
35 COM(2021) 400 final
36 COM/2019/640 final
37 Digitalisation for the Benefit of the Environment, 11 December 2020 , Council conclusions on the new circular economy action plan, 11 December 2020 , Council conclusions on the biodiversity strategy for 2030, 16 October 2020 , Conclusions on the improvement of air quality, 5 March 2020
38 Climate and environmental emergency - Thursday, 28 November 2019 (europa.eu)

In line with the **Industrial Strategy**[39], the proposal deals with highly strategic technologies such as cloud computing and artificial intelligence systems: areas whose full potential the EU has yet to harness, on the cusp of the next industrial data wave. It implements the **Strategy for Data**[40] goal of businesses to being better able to innovate and compete on the basis of EU values, and the principle of **free flow of data within the internal market**. It also tallies with the **Intellectual Property Action Plan**[41] in which the Commission undertook to review the Database Directive.

This proposal should also comply with the principles under the European Pillar of Social Rights (EPSR) Action Plan[42] and the accessibility requirements of the Directive (EU) 2019/882 on the accessibility requirements for products and services[43].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis for this proposal is Article 114 of the Treaty on the Functioning of the European Union, whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules.

This proposal intends to further the completion of the internal market for data in which data from the public sector, businesses and individuals is put to the best possible use, while respecting rights in relation to such data and the investments made in order to collect it. The provisions on switching between data processing services aim to establish fair and competitive market conditions for the internal market in cloud, edge and related services.

The protection of confidential business data and trade secrets is an important aspect of the well-functioning of the internal market, as is the case for other contexts in which services are exchanged and goods are traded. This proposal ensures respect for trade secrets in the context of data use between businesses or by consumers. The initiative will allow the Union to benefit from the scale of the internal market, since products or related services are often developed using data from different Member States, and later commercialised across the Union.

Some Member States have taken legislative action to address the problems described above, in business-to-business and business-to-government scenarios, whereas others have not. This can lead to legislative fragmentation in the internal market and different rules and practices across the Union and related costs by companies that would have to comply with different regimes. It is therefore important to ensure that the proposed measures are applied consistently across Member States.

• Subsidiarity (for non-exclusive competence)

Given the cross-border nature of the use of data and the many areas of impact of the Data Act, the issues this proposal deals with cannot be effectively addressed at Member State level. Fragmentation arising out of differences between national rules should be avoided, as it would lead to higher transactional costs, lack of transparency, legal uncertainty and undesirable forum shopping. Avoiding this is particularly important in all situations concerning the data aspects of business-to-business relations, including fair contractual terms and the obligations

39 COM/2021/350 final.
40 COM/2020/66 final.
41 COM/2020/760 final.
42 COM/2021/102 final.
43 OJ L 151, 7.6.2019

of manufacturers of Internet of Things products or related services, aspects that require homogeneity of the framework throughout the Union.

An assessment of the cross-border aspects of data flows in the area of business-to-government data sharing also demonstrates the need to act at Union level. Many private actors who hold relevant data are multinational companies. These companies should not be confronted with a fragmented legal regime.

Cloud computing services are rarely offered in one Member State only. In line with the GDPR and the Free Flow of Non-Personal Data Regulation that enable consumers and businesses to process personal and non-personal data anywhere they want in the Union, the cross-border processing of data within the Union is essential for conducting business in the internal market. It is therefore crucial that provisions on switching data processing services are applied at Union level, to avoid harmful fragmentation in an otherwise unified market for data processing services.

Only common action at the Union level can enable the achievement of the objectives laid down in this proposal, including the creation of an innovative and competitive level-playing field for data-driven businesses and the empowerment of citizens. This common action is a confident step forward in the realisation of the vision to create a genuine internal market for data.

- **Proportionality**

This proposal balances the rights and interests of affected stakeholders with the general objective to facilitate wider use of data for a broad range of actors. It creates an enabling framework that does not go beyond what is necessary to achieve the objectives. It addresses existing barriers to fuller realisation of the potential value of data among businesses, consumers and the public sector. It also sets out a framework for future sectoral rules to avoid fragmentation and legal uncertainty. It clarifies existing rights and, where necessary, provides access rights to data, thereby helping to develop an internal market for data sharing. The initiative leaves a significant amount of flexibility for application at sector-specific level.

This proposal will give rise to financial and administrative costs. These are to be borne mainly by national authorities, manufacturers and service providers, so that they comply with the obligations set out in this Regulation. However, the exploration of different options and their expected costs and benefits has resulted in a balanced design of the instrument. Similarly, the costs to data users and holders will be counterbalanced by the value to be derived from broader access and use of data, as well as the market uptake of novel services.

- **Choice of the instrument**

The choice of a regulation was made because it is the best mechanism to serve the broader policy goals of ensuring all businesses in the Union are put in a position to innovate and compete, consumers are better able to take control of their data, and Union institutions, agencies and bodies are better equipped to tackle major policy challenges, including public emergencies. A regulation is necessary in light of the goal of comprehensive harmonisation pursued by the proposal, in order to ensure legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide legal and natural persons in all Member States with the same level of legally enforceable rights and obligations, to ensure consistent enforcement in all Member States, as well as effective cooperation between the competent authorities of different Member States.

The proposal will strengthen the internal market for data by increasing legal certainty and guaranteeing a uniform, horizontal and coherent legal framework.

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

• Ex-post evaluations/fitness checks of existing legislation

This proposal partially builds on the latest evaluation of the Database Directive and the Commission's study supporting the review of the Directive[44]. The Database Directive introduced, among other things, a specific *sui generis* right to protect databases if the producer of a database substantially invested in obtaining, verifying and presenting the data. Since its first adoption, the Directive has been evaluated twice. Both evaluations have been supplemented with Commission communications on policy for the data economy[45].

The Court of Justice of the European Union has sharpened the understanding of substantial investments in a database, clarifying that the *sui generis* right aims at protecting the investments in the collection, not the creation of data[46] as a by-product of another economic activity. However, uncertainty remains as to the accidental or unintended application of the *sui generis* right to databases containing machine-generated data, i.e. data obtained from or generated by the use of products or related services. There is a need to balance the policy objectives of IP protection of such databases in the context of the data economy, where the exclusivity of data as a non-rival good is in general considered an impediment to innovation. To ensure consistency with the regulatory interventions proposed in this proposal, the intervention on the *sui generis* right specifically addresses the identified problematic application of the *sui generis* right in the Internet of Things context. The Commission is also currently preparing the evaluation of Regulation (EU) 2018/1807, expected for November 2022. Initial reports by external contractors have shown the limited effect of the SWIPO Codes of Conduct on cloud switching.

• Stakeholder consultations

Extensive work was initiated during the mandate of the previous Commission on identifying the problems that are preventing the Union from realising the full potential of the data-driven innovation in the economy. The proposal builds on past consultation actions, such as the 2017 public consultation supporting the Commission Communication "*Building a European data economy*"[47], the 2017 public consultation on the evaluation of the Database Directive, the 2018 public consultation on the revision of the Directive on the reuse of public sector information, the 2018 SME panel consultation on business-to-business data sharing principles and guidance, and the Commission online open consultation on the Data Strategy[48] from February to May 2020.

---

44 COM/2017/09 final; SWD(2018) 146 final, section 5.4.2; Study to Support an Impact Assessment for the Review of the Database Directive.

45 COM/2017/09 final; COM/2020/66 final; COM/2020/760 final.

46 Fixtures Marketing Ltd v. Oy Veikkaus Ab (C-46/02, 9/11/2004), Fixtures Marketing Ltd v. Svenska Spel Ab (C-338/02, 9/11/2004) British Horseracing Board Ltd v. William Hill (C-203/02, 9/11/2004) Fixtures Marketing Ltd v. OPAP (C-444/02, 9/11/2004).

47 COM/2017/09 final.

48 European Commission (2020). *Outcome of the online consultation on the European strategy for data*.

An Inception Impact Assessment was published on the Better Regulation portal on 28 May 2021 and was left open for feedback for 4 weeks. The Commission received 91 contributions on the Better Regulation Portal[49], mainly from businesses.

A public online consultation on the Data Act was subsequently published on 3 June 2021. It closed on 3 September 2021. The consultation addressed the items covered in the initiative with relevant sections and questions. It targeted all types of stakeholders, gathering input on data sharing, access and use in business-to-business and business-to-government contexts, on consumer empowerment and data portability, the potential role of technical measures such as smart contracts, user's ability to switch between cloud services, intellectual property rights (meaning the protection of databases), and safeguards for non-personal data in the international context. After carrying out an in-depth analysis of the replies, the Commission published a summary report on its website[50].

In total, 449 contributions were received from 32 countries. Business entities constituted the largest number of contributions, comprising 122 business associations and 105 companies/business organisations. In addition, 100 respondents were public authorities and 58 were individual members of the public. Generally, the responses confirmed that there is a whole host of obstacles to effective and efficient data sharing in all types of data relations.

In the business-to-business context, despite data sharing between businesses being a common practice, respondents who had experienced difficulties identified obstacles such as those of a technical nature (formats, lack of standards – 69%); outright refusal to grant access not linked to competition concerns (55%) or the abuse of a contractual imbalance (44%). On contractual issues, almost half of respondents were in favour of introducing an unfairness test (46%), while more than double of those were not in favour (21%). SMEs showed strong support (50%) for an unfairness test, and a significant number of large companies were also in favour (41%) of it. Similarly, 46% of stakeholders across sectors showed support for general access rules based on fair, reasonable and non-discriminatory terms (46%). 60% of respondents, SMEs and micro companies in particular (78%), agreed that model contractual terms could contribute to increased data sharing. 70% of stakeholders expressed the opinion that there is a fairness problem with data generated in the Internet of Things context, and that manufacturers of connected products or related services should not be able to decide unilaterally on what happens to the data generated by such products. 79% of respondents considered that smart contracts could be an effective tool to technically implement data access and use in the context of co-generated Internet of Things data.

Legal uncertainty and barriers, commercial disincentives, and a lack of appropriate infrastructure were amongst the main factors impeding business-to-government data sharing identified by respondents. Almost all public authorities consider that action (Union or Member State) on business-to-government data sharing is needed, compared to 80% of academic/ research institutions and 38% of companies/ business organisations/ associations. A clear majority of stakeholders (in particular citizens and public administrations) also expressed the opinion that business-to-government data sharing should be compulsory, with clear safeguards for specific use-cases with a clear public interest in emergencies and for crisis management purposes, for official statistics, for environmental protection and for a healthier society in general.

---

49 European Commission *webpage*: *Have your Say - Data Act & amended rules on the legal protection of databases.*

50 European Commission (2021). *Public consultation on the Data Act: summary report*.

Respondents also confirmed the usefulness of a right to switchability for business users of cloud computing services. As regards safeguards for non-personal data in international contexts, 76% of respondents perceive potential access to data by foreign authorities on the basis of foreign legislation as a risk to their organisation, with 19% indicating that it is a major risk.

- **Collection and use of expertise**

The proposal was supported by several studies, workshops and other expert input:

– **Study to support this Impact Assessment on enhancing the use of data in Europe**, including interviews with targeted stakeholders. This included two cross-sectoral workshops on business-to-business and business-to-government data sharing, and a final validation workshop organised in spring 2021.

– **Study on model contractual terms, fairness control in data sharing and in cloud contracts and on data access rights** assessed, in particular, fairness aspects in business-to-business data sharing relations and included targeted stakeholder interviews and a validation workshop.

– **Study on the economic detriment from unfair and unbalanced cloud computing contracts**. This included an online survey of a sample of SMEs and start-ups using cloud computing for conducting their business.

– **Study on the switching of cloud service providers**, including a cross-sectorial workshop in the second quarter of 2017.

– **Study in support of the review of the Database Directive**, including interviews with targeted stakeholders. It has assisted the Commission in the preparation of this Impact Assessment to accompany the review of the Database Directive, in the context of the Data Act and in the achievement of their intertwined objectives.

– **Methodological support to impact assessment of using privately held data by official statistics**. This exercise provides input to the assessment of the impact of business-to-government data reuse in official statistics by developing a methodological approach and by describing the benefits and costs of data reuse and of selected use cases for different statistical domains and different types of private sector data. In addition, it contributes to ongoing research and deliberations in order to arrive at a better understanding of business-to-government data sharing.

– **Webinars on personal data platforms and industrial data platforms**. Three webinars were organised on 6, 7 and 8 May 2020. They brought together the relevant data platform projects in the Big Data Value Public-Private Partnership portfolio.

– **High-Level Expert Group Report on Business-to-Government data sharing.** The report provides an analysis of the problems surrounding business-to-government data sharing in the Union and offers a set of recommendations in order to ensure scalable, responsible and sustainable business-to-government data sharing in the public's interest. In addition to the recommendation to the Commission to explore the option of a legal framework in this area, it presents several ways of encouraging private companies to share their data. These include monetary and non-monetary incentives, for example tax incentives, investment of public funds to support the development of trusted technical tools and recognition schemes for data sharing.

– **Workshop on labels for / certification of providers of technical solutions for data exchange**. Around one hundred participants from businesses (including SMEs),

European institutions and academia attended this webinar on 12 May 2020. Its aim was to examine whether a labelling or certification scheme could boost the business uptake of data intermediaries by enhancing trust in the data ecosystem.

– **Ten workshops organised between July and November 2019 involved more than 300 stakeholders and covered different sectors**. The workshops discussed how the organisation of **data sharing in certain areas,** such as the environment, agriculture, energy or healthcare, could benefit society as a whole, helping public actors to design better policies and improve public services, as well as private actors to produce services contributing to facing societal challenges.

– **SME Panel consultation.** This panel consultation, organised from October 2018 to January 2019, sought the views of SMEs on the Commission's business-to-business data sharing principles and guidance issued in the Communication "*Towards a common European data space*" and accompanying the Staff Working Document of 25 April 2018[51].

– **The latest Eurobarometer on the impact of digitisation.** This general survey on the daily lives of Europeans includes questions on people's control over and sharing of personal information. Published on 5 March 2020, it provides information on the willingness of European citizens to share their personal information, including under which conditions.

– **The Opinion of the European Data Protection Supervisor** (EDPS) on the European strategy for data[52]. On 16 June 2020, the EDPS adopted Opinion 3/2020 on the European strategy for data. The EDPS welcomed the strategy, considering its implementation an opportunity to set an example for an alternative data economy model.

• **Impact assessment**

This proposal is accompanied by an impact assessment[53], submitted to the Regulatory Scrutiny Board (RSB) on 29 September 2021 and 13 December 2021. On 21 January 2022, the Board issued a positive opinion subject to reservations.

• **Regulatory fitness and simplification**

By clarifying that the *sui generis* right under the Database Directive (Directive 96/9/EC) does not apply to databases containing data generated or obtained by the use of products or related services, the proposal ensures that the *sui generis* right will not interfere with rights for businesses and consumers to access and use data and to share data provided for in this Regulation. The clarification will align the application of the *sui generis* right with the aim of the legislative proposal and have a positive impact on the uniform application of rules in the internal market and for the data economy.

By facilitating data access and use, the Data Act should reduce burdens, both in the public sector and among businesses, mainly as a result of lowering transaction costs and in terms of efficiency gains. In the scope of the 'one in, one out' approach[54], which aims to minimise burdens for citizens and businesses related to the implications and costs of applying legislation, the Data Act's estimated net administrative burden, based on the Impact

51 COM(2018)232 final; SWD(2018)125 final of 25.4.2018.
52 EDPS Opinion 3/2020 on the European Strategy for Data.
53 **[Links to final document and to the summary sheet to be added.]**
54 SWD(2021) 305 final.

Assessment, accounts for benefits that are likely not only to offset but to far outweigh the associated administrative costs.

- **Fundamental rights**

The proposal is in compliance with the Union legislation on the protection of personal data and the privacy of communications and terminal equipment and envisages additional safeguards where access to personal data can be concerned, as well as in cases subject to intellectual property rights.

In Chapter II, a high level of consumer protection is reinforced with the new right to access user generated data in situations previously not covered by Union law. The right to use and dispose of lawfully acquired possessions is reinforced with a right to access data generated from the use of an Internet of Things object. This way, the owner may benefit from a better user experience and a wider range of, for example, repair and maintenance services. In the context of consumer protection, the rights of children as vulnerable consumers deserve specific attention and the rules of the Data Act will contribute to clarity about data access and use situations.

The Internet of Things data access right for third parties upon the user's request limits the freedom to conduct a business and the freedom of contract of the manufacturer or designer of a product or related service. The limitation is justified in order to enhance consumer protection, in particular to promote consumer's economic interests. The manufacturer or designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service, which contributes to lock-in effects and hinders market entry for players offering aftermarket services. The Internet of Things data access right addresses this situation by further empowering consumers using products or related services to meaningfully control how the data generated by their use of the product or related service is used and enabling innovation by more market players. Consumers can therefore benefit from a wider choice in aftermarket services, such as repair and maintenance, and no longer depend on only the manufacturer's services. The proposal facilitates the portability of the user's data to third parties and thereby allows for a competitive offer of aftermarket services, as well as broader data-based innovation and the development of products or services unrelated to those initially purchased or subscribed to by the user.

The limitation of the manufacturer's or designer's freedom to contract and conduct a business is proportionate and mitigated by the unaffected ability of the manufacturer or designer to also use the data, insofar it is in line with the applicable legislation and the agreement with the user. Furthermore, the manufacturer or designer will also benefit from the right to require compensation for enabling third party access. The access right is without prejudice to the existing access and portability rights for data subjects under the GDPR. Additional safeguards ensure a proportionate use of the data by the third party.

In Chapter IV, a fair and effective system of protection against unfair contractual terms in data sharing will contribute to micro, small or medium-sized enterprises' ability to conduct a business. This provision restricts the contractual freedom of companies in the scope to a limited extent, as it only applies to unfair contractual terms related to data access and use unilaterally imposed by one contractual party on a micro, small or medium-sized enterprise. This is justified as SMEs are typically in a weaker bargaining position and often left with no other choice than to accept 'take it or leave it' contractual terms. The contractual freedom largely remains unaffected as only excessive and abusive terms are invalidated, and the concluded contract, if possible, remains valid without the unfair terms. Furthermore, the

parties can still individually negotiate a specific contractual term[55].

In Chapter V, the provisions related to business-to-government data sharing based on an exceptional need will enhance the capacity of public authorities to take action for the common good, such as to respond, prevent or assist in the recovery from a public emergency. The private sector also stands to benefit from the streamlining of data request procedures.

In Chapter VI, the provisions on switching of data processing providers enhances the position of the business customers and safeguards their choice to change provider. The limitation of the right to conduct a business for data processing providers is justified because the new rules address lock-in effects in the cloud and edge market and improve the choice for business users and individuals of data processing services.

In Chapter X, the intervention on the *sui generis* database right of the Database Directive does not limit the IP protection therein. It rather contributes to legal certainty in cases where the protection of the *sui generis* right was previously unclear.

4. BUDGETARY IMPLICATIONS

This proposal will not have any budgetary implications.

5. OTHER ELEMENTS

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

On a sectoral and macroeconomic level, the ongoing Data Market Monitoring study will help track the economic impact of the current proposal on the growth of the data market in the Union.

The impact on SMEs, namely their perception of problems related to data access and use, will be assessed with an SME panel consultation five years after adoption of the Data Act.

Given the central role of the Common European Data Spaces in the implementation of the European strategy for data, many of the effects of this initiative will be monitored on the level of the sectoral data spaces, and the insights collected by the Data Spaces Support Centre to be funded under the Digital Europe Programme. The regular interaction between the Commission services, the Support Centre and the European Data Innovation Board (to be established following the entry into force of the Data Governance Act) should serve as a reliable source of information allowing in order to assess progress.

Finally, an evaluation will be launched four years after the adoption of the Data Act to evaluate the initiative and to prepare further action as required.

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

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

Chapter II increases legal certainty for consumers and businesses to access data generated by the products or related services they own, rent or lease. Manufacturers and designers have to design the products in a way that makes the data easily accessible by default, and they will have to be transparent on what data will be accessible and how to access them. Provisions in

[55] For more explanations on the unfairness test and the principle of contractual freedom see Impact Assessment, Annex 11.

this Chapter shall not affect the possibility for manufacturers to access and use data from products or related services they offer, where agreed with the user. There is an obligation of the data holder to make such data available to third parties upon the request of the user. Users will be entitled to authorise the data holder to give access to the data to third party service providers, such as providers of aftermarket services. Micro and small enterprises will be exempt from these obligations.

Chapter III sets out general rules applicable to obligations to make data available. Where a data holder is obliged to make data available to a data recipient as in Chapter II or in other Union law or Member State legislation, the general framework addresses the conditions under which data is made available and the compensation for making data available. Any conditions will have to be fair and non-discriminatory, and any compensation will have to be reasonable, without precluding other Union law or national legislation implementing Union law from excluding compensation or providing for lower compensation for making data available. Any compensation set for SMEs cannot exceed the costs incurred for making the data available, unless otherwise specified in sectoral legislations. Dispute settlement bodies certified by the Member States may assist parties that disagree on the compensation or conditions to come to an agreement.

Chapter IV addresses unfairness of contractual terms in data sharing contracts between businesses, in situations where a contractual term is unilaterally imposed by one party on a micro, small or medium-sized enterprise. This Chapter guarantees that contractual agreements on data access and use do not take advantage of imbalances in negotiating power between the contractual parties. The instrument of an unfairness test includes a general provision defining unfairness of a data sharing-related contractual term complemented by a list of clauses that are either always unfair or presumed to be unfair. In situations of unequal bargaining power, that test protects the weaker contractual party in order to avoid unfair contracts. Such unfairness impedes the use of data by both contractual parties. With that, the provisions ensure a fairer allocation of value in the data economy[56]. Model contractual terms recommended by the Commission may assist commercial parties in concluding contracts based on fair terms.

Chapter V creates a harmonised framework for the use by public sector bodies and Union institutions, agencies and bodies of data held by enterprises in situations where there is an exceptional need for the data requested. The framework is based on an obligation to make data available and would only apply in the case of public emergencies or in situations where public sector bodies have an exceptional need to use certain data, but such data cannot be obtained on the market, in a timely manner through enacting new legislation, or by means of existing reporting obligations. In case of an exceptional need to respond to public emergency, such as public health emergencies, or major natural or human-induced disasters, data would be made available for free. In other cases of exceptional need, including to prevent or assist the recovery from a public emergency, the data holder making the data available should be entitled to compensation that include costs related to making the relevant data available plus a reasonable margin. To ensure that the right to request data is not abused and that the public sector remains accountable for its use, the requests for data would need to be proportionate, clearly indicate the purpose to be achieved, and respect the interests of the enterprise making the data available. Competent authorities would ensure the transparency and public availability of all requests. They would also handle any resulting complaints.

[56] For more explanations on the unfairness test, including on the functioning in practice, see Annex 11 of the Impact Assessment.

Chapter VI introduces minimum regulatory requirements of contractual, commercial and technical nature, imposed on providers of cloud, edge and other data processing services, to enable switching between such services. In particular, the proposal ensures that customers maintain functional equivalence (a minimum level of functionality) of the service after they have switched to another service provider. The proposal contains an exception for technical unfeasibility, but puts the burden of proof in this regard on the service provider. The proposal does not mandate specific technical standards or interfaces. However, it requires services to be compatible with European standards or open interoperability technical specifications where these exist.

Chapter VII addresses unlawful third party access to non-personal data held in the Union by data processing services offered on the Union market. The proposal does not affect the legal basis of data access requests made to data held by EU citizens or businesses and is without prejudice to the Union's data protection and privacy framework. It offers specific safeguards, by way of providers having to take all reasonable technical, legal and organisational measures to prevent such access that conflicts with competing obligations to protect such data under Union law, unless strict conditions are met. The Regulation complies with the Union's international commitments in the WTO and in bilateral trade agreements.

Chapter VIII provides for essential requirements to be complied with regarding interoperability for operators of data spaces and data processing service providers as well as for essential requirements for smart contracts. The Chapter also enables open interoperability specifications and European standards for the interoperability of data processing services to promote a seamless multi-vendor cloud environment.

Chapter IX lays down the implementation and enforcement framework with competent authorities in each Member State, including a complaints mechanism. The Commission shall recommend voluntary model contractual terms on access to and use of data. Penalties shall apply for infringements of this Regulation.

Chapter X contains a provision so that the *sui generis* right established in Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or related service to hinder the effective exercise of the right of users to access and use data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation.

Chapter XI allows the Commission to adopt delegated acts to introduce a monitoring mechanism on switching charges imposed on providers of data processing services, to further specify the essential requirements regarding interoperability, and to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services . It also provides for the committee procedure to adopt implementing acts to facilitate the adoption of common specifications for interoperability and smart contracts where harmonised standards do not exist or are insufficient to ensure the conformity with essential requirements. The proposal also clarifies the relation to other Union legal acts governing data sharing rights and obligations.

2022/0047 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on harmonised rules on fair access to and use of data (Data 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[57],

Having regard to the opinion of the Committee of the Regions[58],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In recent years, data-driven technologies have had transformative effects on all sectors of the economy. The proliferation in products connected to the Internet of Things in particular has increased the volume and potential value of data for consumers, businesses and society. High quality and interoperable data from different domains increase competitiveness and innovation and ensure sustainable economic growth. The same dataset may potentially be used and reused for a variety of purposes and to an unlimited degree, without any loss in its quality or quantity.

(2) Barriers to data sharing prevent an optimal allocation of data to the benefit of society. These barriers include a lack of incentives for data holders to enter voluntarily into data sharing agreements, uncertainty about rights and obligations in relation to data, costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, bottlenecks impeding data access, a lack of common data sharing practices and abuse of contractual imbalances with regards to data access and use.

(3) In sectors characterised by the presence of micro, small and medium-sized enterprises, there is often a lack of digital capacities and skills to collect, analyse and use data, and access is frequently restricted where one actor holds it in the system or due to a lack of interoperability between data, between data services or across borders.

(4) In order to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data, it is necessary to lay down a harmonised

[57] OJ C , , p. .
[58] OJ C , , p. .

framework specifying who, other than the manufacturer or other data holder is entitled to access the data generated by products or related services, under which conditions and on what basis. Accordingly, Member States should not adopt or maintain additional national requirements on those matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of this Regulation.

(5) This Regulation ensures that users of a product or related service in the Union can access, in a timely manner, the data generated by the use of that product or related service and that those users can use the data, including by sharing them with third parties of their choice. It imposes the obligation on the data holder to make data available to users and third parties nominated by the users in certain circumstances. It also ensures that data holders make data available to data recipients in the Union under fair, reasonable and non-discriminatory terms and in a transparent manner. Private law rules are key in the overall framework of data sharing. Therefore, this Regulation adapts rules of contract law and prevents the exploitation of contractual imbalances that hinder fair data access and use for micro, small or medium-sized enterprises within the meaning of Recommendation 2003/361/EC. This Regulation also ensures that data holders make available to public sector bodies of the Member States and to Union institutions, agencies or bodies, where there is an exceptional need, the data that are necessary for the performance of tasks carried out in the public interest. In addition, this Regulation seeks to facilitate switching between data processing services and to enhance the interoperability of data and data sharing mechanisms and services in the Union. This Regulation should not be interpreted as recognising or creating any legal basis for the data holder to hold, have access to or process data, or as conferring any new right on the data holder to use data generated by the use of a product or related service. Instead, it takes as its starting point the control that the data holder effectively enjoys, de facto or de jure, over data generated by products or related services.

(6) Data generation is the result of the actions of at least two actors, the designer or manufacturer of a product and the user of that product. It gives rise to questions of fairness in the digital economy, because the data recorded by such products or related services are an important input for aftermarket, ancillary and other services. In order to realise the important economic benefits of data as a non-rival good for the economy and society, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use.

(7) The fundamental right to the protection of personal data is safeguarded in particular under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725. Directive 2002/58/EC additionally protects private life and the confidentiality of communications, including providing conditions to any personal and non-personal data storing in and access from terminal equipment. These instruments provide the basis for sustainable and responsible data processing, including where datasets include a mix of personal and non-personal data. This Regulation complements and is without prejudice to Union law on data protection and privacy, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC. No provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications.

(8) The principles of data minimisation and data protection by design and by default are essential when processing involves significant risks to the fundamental rights of individuals. Taking into account the state of the art, all parties to data sharing,

including where within scope of this Regulation, should implement technical and organisational measures to protect these rights. Such measures include not only pseudonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allow valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves.

(9) This Regulation complements and is without prejudice to Union law aiming to promote the interests of consumers and to ensure a high level of consumer protection, to protect their health, safety and economic interests, in particular Directive 2005/29/EC of the European Parliament and of the Council[59], Directive 2011/83/EU of the European Parliament and of the Council[60] and Directive 93/13/EEC of the European Parliament and of the Council[61].

(10) This Regulation is without prejudice to Union legal acts providing for the sharing of, the access to and the use of data for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or for customs and taxation purposes, irrespective of the legal basis under the Treaty on the Functioning of the European Union on which basis they were adopted. Such acts include Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, the [e-evidence proposals [COM(2018) 225 and 226] once adopted], the [Proposal for] a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, as well as international cooperation in this context in particular on the basis of the Council of Europe 2001 Convention on Cybercrime ("Budapest Convention"). This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence and national security in accordance with Union law, and activities from customs on risk management and in general, verification of compliance with the Customs Code by economic operators.

(11) Union law setting physical design and data requirements for products to be placed on the Union market should not be affected by this Regulation.

(12) This Regulation complements and is without prejudice to Union law aiming at setting accessibility requirements on certain products and services, in particular Directive 2019/882[62].

---

[59] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

[60] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[61] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

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

(13) This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence and national security in accordance with Union law, and activities from customs on risk management and in general, verification of compliance with the Customs Code by economic operators.

(14) Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. Electronic communications services include land-based telephone networks, television cable networks, satellite-based networks and near-field communication networks. Such products may include vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery. The data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation. Such data are potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, in particular though facilitating the maintenance and repair of the products in question.

(15) In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.

(16) It is necessary to lay down rules applying to connected products that incorporate or are interconnected with a service in such a way that the absence of the service would prevent the product from performing its functions. Such related services can be part of the sale, rent or lease agreement, or such services are normally provided for products of the same type and the user could reasonably expect them to be provided given the nature of the product and taking into account any public statement made by or on behalf of the seller, renter, lessor or other persons in previous links of the chain of transactions, including the manufacturer. These related services may themselves generate data of value to the user independently of the data collection capabilities of the product with which they are interconnected. This Regulation should also apply to a related service that is not supplied by the seller, renter or lessor itself, but is supplied, under the sales, rental or lease contract, by a third party. In the event of doubt as to whether the supply of service forms part of the sale, rent or lease contract, this Regulation should apply.

(17) Data generated by the use of a product or related service include data recorded intentionally by the user. Such data include also data generated as a by-product of the user's action, such as diagnostics data, and without any action by the user, such as when the product is in 'standby mode', and data recorded during periods when the product is switched off. Such data should include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights.

(18) The user of a product should be understood as the legal or natural person, such as a business or consumer, which has purchased, rented or leased the product. Depending

on the legal title under which he uses it, such a user bears the risks and enjoys the benefits of using the connected product and should enjoy also the access to the data it generates. The user should therefore be entitled to derive benefit from data generated by that product and any related service.

(19) In practice, not all data generated by products or related services are easily accessible to their users, and there are often limited possibilities for the portability of data generated by products connected to the Internet of Things. Users are unable to obtain data necessary to make use of providers of repair and other services, and businesses are unable to launch innovative, more efficient and convenient services. In many sectors, manufacturers are often able to determine, through their control of the technical design of the product or related services, what data are generated and how they can be accessed, even though they have no legal right to the data. It is therefore necessary to ensure that products are designed and manufactured and related services are provided in such a manner that data generated by their use are always easily accessible to the user.

(20) In case several persons or entities own a product or are party to a lease or rent agreement and benefit from access to a related service, reasonable efforts should be made in the design of the product or related service or the relevant interface so that all persons can have access to data they generate. Users of products that generate data typically require a user account to be set up. This allows for identification of the user by the manufacturer as well as a means to communicate to exercise and process data access requests. Manufacturers or designers of a product that is typically used by several persons should put in place the necessary mechanism that allow separate user accounts for individual persons, where relevant, or the possibility for several persons to use the same user account. Access should be granted to the user upon simple request mechanisms granting automatic execution, not requiring examination or clearance by the manufacturer or data holder. This means that data should only be made available when the user actually wants this. Where automated execution of the data access request is not possible, for instance, via a user account or accompanying mobile application provided with the product or service, the manufacturer should inform the user how the data may be accessed.

(21) Products may be designed to make certain data directly available from an on-device data storage or from a remote server to which the data are communicated. Access to the on-device data storage may be enabled via cable-based or wireless local area networks connected to a publicly available electronic communications service or a mobile network. The server may be the manufacturer's own local server capacity or that of a third party or a cloud service provider who functions as data holder. They may be designed to permit the user or a third party to process the data on the product or on a computing instance of the manufacturer.

(22) Virtual assistants play an increasing role in digitising consumer environments and serve as an easy-to-use interface to play content, obtain information, or activate physical objects connected to the Internet of Things. Virtual assistants can act as a single gateway in, for example, a smart home environment and record significant amounts of relevant data on how users interact with products connected to the Internet of Things, including those manufactured by other parties and can replace the use of manufacturer-provided interfaces such as touchscreens or smart phone apps. The user may wish to make available such data with third party manufacturers and enable novel smart home services. Such virtual assistants should be covered by the data access right provided for in this Regulation also regarding data recorded before the virtual

assistant's activation by the wake word and data generated when a user interacts with a product via a virtual assistant provided by an entity other than the manufacturer of the product. However, only the data stemming from the interaction between the user and product through the virtual assistant falls within the scope of this Regulation. Data produced by the virtual assistant unrelated to the use of a product is not the object of this Regulation.

(23) Before concluding a contract for the purchase, rent, or lease of a product or the provision of a related service, clear and sufficient information should be provided to the user on how the data generated may be accessed. This obligation provides transparency over the data generated and enhances the easy access for the user. This obligation to provide information does not affect the obligation for the controller to provide information to the data subject pursuant to Article 12, 13 and 14 of Regulation 2016/679.

(24) This Regulation imposes the obligation on data holders to make data available in certain circumstances. Insofar as personal data are processed, the data holder should be a controller under Regulation (EU) 2016/679. Where users are data subjects, data holders should be obliged to provide them access to their data and to make the data available to third parties of the user's choice in accordance with this Regulation. However, this Regulation does not create a legal basis under Regulation (EU) 2016/679 for the data holder to provide access to personal data or make it available to a third party when requested by a user that is not a data subject and should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies in particular where the manufacturer is the data holder. In that case, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user. This agreement may be part of the sale, rent or lease agreement relating to the product. Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which the data holder intends to use the data. This Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder. This Regulation should also not prevent sector-specific regulatory requirements under Union law, or national law compatible with Union law, which would exclude or limit the use of certain such data by the data holder on well-defined public policy grounds.

(25) In sectors characterised by the concentration of a small number of manufacturers supplying end users, there are only limited options available to users with regard to sharing data with those manufacturers. In such circumstances, contractual agreements may be insufficient to achieve the objective of user empowerment. The data tends to remain under the control of the manufacturers, making it difficult for users to obtain value from the data generated by the equipment they purchase or lease. Consequently, there is limited potential for innovative smaller businesses to offer data-based solutions in a competitive manner and for a diverse data economy in Europe. This Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement. Sectoral legislation may be brought forward to address sector-specific needs and objectives. Furthermore, the data holder should not use any data generated by the use of the product or related service in order to derive insights about the economic situation of the user or its assets or production methods or the use in any other way that could undermine the commercial position of the user on the markets it is active on. This

would, for instance, involve using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on potential acquisition of the user's products or agricultural produce to the user's detriment, or for instance, using such information to feed in larger databases on certain markets in the aggregate (,e.g. databases on crop yields for the upcoming harvesting season) as such use could affect the user negatively in an indirect manner. The user should be given the necessary technical interface to manage permissions, preferably with granular permission options (such as "allow once" or "allow while using this app or service"), including the option to withdraw permission.

(26) In contracts between a data holder and a consumer as a user of a product or related service generating data, Directive 93/13/EEC applies to the terms of the contract to ensure that a consumer is not subject to unfair contractual terms. For unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC[63], this Regulation provides that such unfair terms should not be binding on that enterprise.

(27) The data holder may require appropriate user identification to verify the user's entitlement to access the data. In the case of personal data processed by a processor on behalf of the controller, the data holder should ensure that the access request is received and handled by the processor.

(28) The user should be free to use the data for any lawful purpose. This includes providing the data the user has received exercising the right under this Regulation to a third party offering an aftermarket service that may be in competition with a service provided by the data holder, or to instruct the data holder to do so. The data holder should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date as the data the data holder itself may be able or entitled to access from the use of the product or related service. Any trade secrets or intellectual property rights should be respected in handling the data. It is important to preserve incentives to invest in products with functionalities based on the use of data from sensors built into that product. The aim of this Regulation should accordingly be understood as to foster the development of new, innovative products or related services, stimulate innovation on aftermarkets, but also stimulate the development of entirely novel services making use of the data, including based on data from a variety of products or related services. At the same time, it aims to avoid undermining the investment incentives for the type of product from which the data are obtained, for instance, by the use of data to develop a competing product.

(29) A third party to whom data is made available may be an enterprise, a research organisation or a not-for-profit organisation. In making the data available to the third party, the data holder should not abuse its position to seek a competitive advantage in markets where the data holder and third party may be in direct competition. The data holder should not therefore use any data generated by the use of the product or related service in order to derive insights about the economic situation of the third party or its assets or production methods or the use in any other way that could undermine the commercial position of the third party on the markets it is active on.

(30) The use of a product or related service may, in particular when the user is a natural person, generate data that relates to an identified or identifiable natural person (the data subject). Processing of such data is subject to the rules established under

[63] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises

Regulation (EU) 2016/679, including where personal and non-personal data in a data set are inextricably linked[64]. The data subject may be the user or another natural person. Personal data may only be requested by a controller or a data subject. A user who is the data subject is under certain circumstances entitled under Regulation (EU) 2016/679 to access personal data concerning them, and such rights are unaffected by this Regulation. Under this Regulation, the user who is a natural person is further entitled to access all data generated by the product, personal and non-personal. Where the user is not the data subject but an enterprise, including a sole trader, and not in cases of shared household use of the product, the user will be a controller within the meaning of Regulation (EU) 2016/679. Accordingly, such a user as controller intending to request personal data generated by the use of a product or related service is required to have a legal basis for processing the data under Article 6(1) of Regulation (EU) 2016/679, such as the consent of the data subject or legitimate interest. This user should ensure that the data subject is appropriately informed of the specified, explicit and legitimate purposes for processing those data, and how the data subject may effectively exercise their rights. Where the data holder and the user are joint controllers within the meaning of Article 26 of Regulation (EU) 2016/679, they are required to determine, in a transparent manner by means of an arrangement between them, their respective responsibilities for compliance with that Regulation. It should be understood that such a user, once data has been made available, may in turn become a data holder, if they meet the criteria under this Regulation and thus become subject to the obligations to make data available under this Regulation.

(31) Data generated by the use of a product or related service should only be made available to a third party at the request of the user. This Regulation accordingly complements the right provided under Article 20 of Regulation (EU) 2016/679. That Article provides for a right of data subjects to receive personal data concerning them in a structured, commonly used and machine-readable format, and to port those data to other controllers, where those data are processed on the basis of Article 6(1), point (a), or Article 9(2), point (a), or of a contract pursuant to Article 6(1), point (b). Data subjects also have the right to have the personal data transmitted directly from one controller to another, but only where technically feasible. Article 20 specifies that it pertains to data provided by the data subject but does not specify whether this necessitates active behaviour on the side of the data subject or whether it also applies to situations where a product or related service by its design observes the behaviour of a data subject or other information in relation to a data subject in a passive manner. The right under this Regulation complements the right to receive and port personal data under Article 20 of Regulation (EU) 2016/679 in several ways. It grants users the right to access and make available to a third party to any data generated by the use of a product or related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike the technical obligations provided for in Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of data coming within its scope, whether personal or non-personal. It also allows the data holder to set reasonable compensation to be met by third parties, but not by the user, for any cost incurred in providing direct access to the data generated by the user's product. If a data holder and third party are unable to agree terms for such direct access, the data subject should be in no way prevented from exercising the rights contained in Regulation (EU) 2016/679,

64 OJ L 303, 28.11.2018, p. 59–68.

including the right to data portability, by seeking remedies in accordance with that Regulation. It is to be understood in this context that, in accordance with Regulation (EU) 2016/679, a contractual agreement does not allow for the processing of special categories of personal data by the data holder or the third party.

(32) Access to any data stored in and accessed from terminal equipment is subject to Directive 2002/58/EC and requires the consent of the subscriber or user within the meaning of that Directive unless it is strictly necessary for the provision of an information society service explicitly requested by the user or subscriber (or for the sole purpose of the transmission of a communication). Directive 2002/58/EC ('ePrivacy Directive') (and the proposed ePrivacy Regulation) protect the integrity of the user's terminal equipment as regards the use of processing and storage capabilities and the collection of information. Internet of Things equipment is considered terminal equipment if it is directly or indirectly connected to a public communications network.

(33) In order to prevent the exploitation of users, third parties to whom data has been made available upon request of the user should only process the data for the purposes agreed with the user and share it with another third party only if this is necessary to provide the service requested by the user.

(34) In line with the data minimisation principle, the third party should only access additional information that is necessary for the provision of the service requested by the user. Having received access to data, the third party should process it exclusively for the purposes agreed with the user, without interference from the data holder. It should be as easy for the user to refuse or discontinue access by the third party to the data as it is for the user to authorise access. The third party should not coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user. in this context, third parties should not rely on so-called dark patterns in designing their digital interfaces. Dark patterns are design techniques that push or deceive consumers into decisions that have negative consequences for them. These manipulative techniques can be used to persuade users, particularly vulnerable consumers, to engage in unwanted behaviours, and to deceive users by nudging them into decisions on data disclosure transactions or to unreasonably bias the decision-making of the users of the service, in a way that subverts and impairs their autonomy, decision-making and choice. Common and legitimate commercial practices that are in compliance with Union law should not in themselves be regarded as constituting dark patterns. Third parties should comply with their obligations under relevant Union law, in particular the requirements set out in Directive 2005/29/EC, Directive 2011/83/EU, Directive 2000/31/EC and Directive 98/6/EC.

(35) The third party should also refrain from using the data to profile individuals unless these processing activities are strictly necessary to provide the service requested by the user. The requirement to delete data when no longer required for the purpose agreed with the user complements the right to erasure of the data subject pursuant to Article 17 of Regulation 2016/679. Where the third party is a provider of a data intermediation service within the meaning of [Data Governance Act], the safeguards for the data subject provided for by that Regulation apply. The third party may use the data to develop a new and innovative product or related service but not to develop a competing product.

(36) Start-ups, small and medium-sized enterprises and companies from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This

Regulation aims to facilitate access to data for these entities, while ensuring that the corresponding obligations are scoped as proportionately as possible to avoid overreach. At the same time, a small number of very large companies have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. These companies include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and whom existing or new market operators are unable to challenge or contest. The [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)] aims to redress these inefficiencies and imbalances by allowing the Commission to designate a provider as a "gatekeeper", and imposes a number of obligations on such designated gatekeepers, including a prohibition to combine certain data without consent, and an obligation to ensure effective rights to data portability under Article 20 of Regulation (EU) 2016/679. Consistent with the [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)], and given the unrivalled ability of these companies to acquire data, it would not be necessary to achieve the objective of this Regulation, and would thus be disproportionate in relation to data holders made subject to such obligations, to include such gatekeeper undertakings as beneficiaries of the data access right. This means that an undertaking providing core platform services that has been designated as a gatekeeper cannot request or be granted access to users' data generated by the use of a product or related service or by a virtual assistant based on the provisions of Chapter II of this Regulation. An undertaking providing core platform services designated as a gatekeeper pursuant to Digital Markets Act should be understood to include all legal entities of a group of companies where one legal entity provides a core platform service. Furthermore, third parties to whom data are made available at the request of the user may not make the data available to a designated gatekeeper. For instance, the third party may not sub-contract the service provision to a gatekeeper. However, this does not prevent third parties from using data processing services offered by a designated gatekeeper. This exclusion of designated gatekeepers from the scope of the access right under this Regulation does not prevent these companies from obtaining data through other lawful means.

(37) Given the current state of technology, it is overly burdensome to impose further design obligations in relation to products manufactured or designed and related services provided by micro and small enterprises. That is not the case, however, where a micro or small enterprise is sub-contracted to manufacture or design a product. In such situations, the enterprise, which has sub-contracted to the micro or small enterprise, is able to compensate the sub-contractor appropriately. A micro or small enterprise may nevertheless be subject to the requirements laid down by this Regulation as data holder, where it is not the manufacturer of the product or a provider of related services.

(38) This Regulation contains general access rules, whenever a data holder is obliged by law to make data available to a data recipient. Such access should be based on fair, reasonable, non-discriminatory and transparent conditions to ensure consistency of data sharing practices in the internal market, including across sectors, and to encourage and promote fair data sharing practices even in areas where no such right to data access is provided. These general access rules do not apply to obligations to make data available under Regulation (EU) 2016/679. Voluntary data sharing remains unaffected by these rules.

(39) Based on the principle of contractual freedom, the parties should remain free to negotiate the precise conditions for making data available in their contracts, within the framework of the general access rules for making data available.

(40) In order to ensure that the conditions for mandatory data access are fair for both parties, the general rules on data access rights should refer to the rule on avoiding unfair contract terms.

(41) In order to compensate for the lack of information on the conditions of different contracts, which makes it difficult for the data recipient to assess if the terms for making the data available are non-discriminatory, it should be on the data holder to demonstrate that a contractual term is not discriminatory. It is not unlawful discrimination, where a data holder uses different contractual terms for making data available or different compensation, if those differences are justified by objective reasons. These obligations are without prejudice to Regulation (EU) 2016/679.

(42) In order to incentivise the continued investment in generating valuable data, including investments in relevant technical tools, this Regulation contains the principle that the data holder may request reasonable compensation when legally obliged to make data available to the data recipient. These provisions should not be understood as paying for the data itself, but in the case of micro, small or medium-sized enterprises, for the costs incurred and investment required for making the data available.

(43) In justified cases, including the need to safeguard consumer participation and competition or to promote innovation in certain markets, Union law or national legislation implementing Union law may impose regulated compensation for making available specific data types.

(44) To protect micro, small or medium-sized enterprises from excessive economic burdens which would make it commercially too difficult for them to develop and run innovative business models, the compensation for making data available to be paid by them should not exceed the direct cost of making the data available and be non-discriminatory.

(45) Direct costs for making data available are the costs necessary for data reproduction, dissemination via electronic means and storage but not of data collection or production. Direct costs for making data available should be limited to the share attributable to the individual requests, taking into account that the necessary technical interfaces or related software and connectivity will have to be set up permanently by the data holder. Long-term arrangements between data holders and data recipients, for instance via a subscription model, could reduce the costs linked to making the data available in regular or repetitive transactions in a business relationship.

(46) It is not necessary to intervene in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company. In such cases, the companies are considered capable of negotiating any compensation if it is reasonable, taking into account factors such as the volume, format, nature, or supply of and demand for the data as well as the costs for collecting and making the data available to the data recipient.

(47) Transparency is an important principle to ensure that the compensation requested by the data holder is reasonable, or, in case the data recipient is a micro, small or medium-sized enterprise, that the compensation does not exceed the costs directly related to making the data available to the data recipient and is attributable to the individual request. In order to put the data recipient in the position to assess and verify

that the compensation complies with the requirements under this Regulation, the data holder should provide to the data recipient the information for the calculation of the compensation with a sufficient degree of detail.

(48) Ensuring access to alternative ways of resolving domestic and cross-border disputes that arise in connection with making data available should benefit data holders and data recipients and therefore strengthen trust in data sharing. In cases where parties cannot agree on fair, reasonable and non-discriminatory terms of making data available, dispute settlement bodies should offer a simple, fast and low-cost solution to the parties.

(49) To avoid that two or more dispute settlement bodies are seized for the same dispute, particularly in a cross-border setting, a dispute settlement body should be able to reject a request to resolve a dispute that has already been brought before another dispute settlement body or before a court or a tribunal of a Member State.

(50) Parties to dispute settlement proceedings should not be prevented from exercising their fundamental rights to an effective remedy and to a fair trial. Therefore, the decision to submit a dispute to a dispute settlement body should not deprive those parties of their right to seek redress before a court or a tribunal of a Member State.

(51) Where one party is in a stronger bargaining position, there is a risk that that party could leverage such position to the detriment of the other contracting party when negotiating access to data and make access to data commercially less viable and sometimes economically prohibitive. Such contractual imbalances particularly harm micro, small and medium-sized enterprises without a meaningful ability to negotiate the conditions for access to data, who may have no other choice than to accept 'take-it-or-leave-it' contractual terms. Therefore, unfair contract terms regulating the access to and use of data or the liability and remedies for the breach or the termination of data related obligations should not be binding on micro, small or medium-sized enterprises when they have been unilaterally imposed on them.

(52) Rules on contractual terms should take into account the principle of contractual freedom as an essential concept in business-to-business relationships. Therefore, not all contractual terms should be subject to an unfairness test, but only to those terms that are unilaterally imposed on micro, small and medium-sized enterprises. This concerns 'take-it-or-leave-it' situations where one party supplies a certain contractual term and the micro, small or medium-sized enterprise cannot influence the content of that term despite an attempt to negotiate it. A contractual term that is simply provided by one party and accepted by the micro, small or medium-sized enterprise or a term that is negotiated and subsequently agreed in an amended way between contracting parties should not be considered as unilaterally imposed.

(53) Furthermore, the rules on unfair contractual terms should only apply to those elements of a contract that are related to making data available, that is contractual terms concerning the access to and use of data as well as liability or remedies for breach and termination of data related obligations. Other parts of the same contract, unrelated to making data available, should not be subject to the unfairness test laid down in this Regulation.

(54) Criteria to identify unfair contractual terms should be applied only to excessive contractual terms, where a stronger bargaining position is abused. The vast majority of contractual terms that are commercially more favourable to one party than to the other,

including those that are normal in business-to-business contracts, are a normal expression of the principle of contractual freedom and shall continue to apply.

(55) If a contractual term is not included in the list of terms that are always considered unfair or that are presumed to be unfair, the general unfairness provision applies. In this regard, the terms listed as unfair terms should serve as a yardstick to interpret the general unfairness provision. Finally, model contractual terms for business-to-business data sharing contracts to be developed and recommended by the Commission may also be helpful to commercial parties when negotiating contracts.

(56) In situations of exceptional need, it may be necessary for public sector bodies or Union institutions, agencies or bodies to use data held by an enterprise to respond to public emergencies or in other exceptional cases. Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law. To limit the burden on businesses, micro and small enterprises should be exempted from the obligation to provide public sector bodies and Union institutions, agencies or bodies data in situations of exceptional need.

(57) In case of public emergencies, such as public health emergencies, emergencies resulting from environmental degradation and major natural disasters including those aggravated by climate change, as well as human-induced major disasters, such as major cybersecurity incidents, the public interest resulting from the use of the data will outweigh the interests of the data holders to dispose freely of the data they hold. In such a case, data holders should be placed under an obligation to make the data available to public sector bodies or to Union institutions, agencies or bodies upon their request. The existence of a public emergency is determined according to the respective procedures in the Member States or of relevant international organisations.

(58) An exceptional need may also arise when a public sector body can demonstrate that the data are necessary either to prevent a public emergency, or to assist recovery from a public emergency, in circumstances that are reasonably proximate to the public emergency in question. Where the exceptional need is not justified by the need to respond to, prevent or assist recovery from a public emergency, the public sector body or the Union institution, agency or body should demonstrate that the lack of timely access to and the use of the data requested prevents it from effectively fulfilling a specific task in the public interest that has been explicitly provided in law. Such exceptional need may also occur in other situations, for example in relation to the timely compilation of official statistics when data is not otherwise available or when the burden on statistical respondents will be considerably reduced. At the same time, the public sector body or the Union institution, agency or body should, outside the case of responding to, preventing or assisting recovery from a public emergency, demonstrate that no alternative means for obtaining the data requested exists and that the data cannot be obtained in a timely manner through the laying down of the necessary data provision obligations in new legislation.

(59) This Regulation should not apply to, nor pre-empt, voluntary arrangements for the exchange of data between private and public entities. Obligations placed on data holders to provide data that are motivated by needs of a non-exceptional nature, notably where the range of data and of data holders is known and where data use can take place on a regular basis, as in the case of reporting obligations and internal market obligations, should not be affected by this Regulation. Requirements to access data to verify compliance with applicable rules, including in cases where public sector bodies

assign the task of the verification of compliance to entities other than public sector bodies, should also not be affected by this Regulation.

(60) For the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal and administrative offences, the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes, public sector bodies and Union institutions, agencies and bodies should rely on their powers under sectoral legislation. This Regulation accordingly does not affect instruments for the sharing, access and use of data in those areas.

(61) A proportionate, limited and predictable framework at Union level is necessary for the making available of data by data holders, in cases of exceptional needs, to public sector bodies and to Union institution, agencies or bodies both to ensure legal certainty and to minimise the administrative burdens placed on businesses. To this end, data requests by public sector bodies and by Union institution, agencies and bodies to data holders should be transparent and proportionate in terms of their scope of content and their granularity. The purpose of the request and the intended use of the data requested should be specific and clearly explained, while allowing appropriate flexibility for the requesting entity to perform its tasks in the public interest. The request should also respect the legitimate interests of the businesses to whom the request is made. The burden on data holders should be minimised by obliging requesting entities to respect the once-only principle, which prevents the same data from being requested more than once by more than one public sector body or Union institution, agency or body where those data are needed to respond to a public emergency. To ensure transparency, data requests made by public sector bodies and by Union institutions, agencies or bodies should be made public without undue delay by the entity requesting the data and online public availability of all requests justified by a public emergency should be ensured.

(62) The objective of the obligation to provide the data is to ensure that public sector bodies and Union institutions, agencies or bodies have the necessary knowledge to respond to, prevent or recover from public emergencies or to maintain the capacity to fulfil specific tasks explicitly provided by law. The data obtained by those entities may be commercially sensitive. Therefore, Directive (EU) 2019/1024 of the European Parliament and of the Council[65] should not apply to data made available under this Regulation and should not be considered as open data available for reuse by third parties. This however should not affect the applicability of Directive (EU) 2019/1024 to the reuse of official statistics for the production of which data obtained pursuant to this Regulation was used, provided the reuse does not include the underlying data. In addition, it should not affect the possibility of sharing the data for conducting research or for the compilation of official statistics, provided the conditions laid down in this Regulation are met. Public sector bodies should also be allowed to exchange data obtained pursuant to this Regulation with other public sector bodies to address the exceptional needs for which the data has been requested.

(63) Data holders should have the possibility to either ask for a modification of the request made by a public sector body or Union institution, agency and body or its cancellation in a period of 5 or 15 working days depending on the nature of the exceptional need invoked in the request. In case of requests motivated by a public emergency, justified reason not to make the data available should exist if it can be shown that the request is

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

similar or identical to a previously submitted request for the same purpose by another public sector body or by another Union institution, agency or body. A data holder rejecting the request or seeking its modification should communicate the underlying justification for refusing the request to the public sector body or to the Union institution, agency or body requesting the data. In case the *sui generis* database rights under Directive 96/6/EC of the European Parliament and of the Council[66] apply in relation to the requested datasets, data holders should exercise their rights in a way that does not prevent the public sector body and Union institutions, agencies or bodies from obtaining the data, or from sharing it, in accordance with this Regulation.

(64) Where it is strictly necessary to include personal data in the data made available to a public sector body or to a Union institution, agency or body the applicable rules on personal data protection should be complied with and the making available of the data and their subsequent use should and be accompanied by safeguards for the rights and interests of individuals concerned by those data. The body requesting the data should demonstrate the strict necessity and the specific and limited purposes for processing. The data holder should take reasonable efforts to anonymise the data or, where such anonymisation proves impossible, the data holder should apply technological means such as pseudonymisation and aggregation, prior to making the data available.

(65) Data made available to public sector bodies and to Union institutions, agencies and bodies on the basis of exceptional need should only be used for the purpose for which they were requested, unless the data holder that made the data available has expressly agreed for the data to be used for other purposes. The data should be destroyed once it is no longer necessary for the purpose stated in the request, unless agreed otherwise, and the data holder should be informed thereof.

(66) When reusing data provided by data holders, public sector bodies and Union institutions, agencies or bodies should respect both existing applicable legislation and contractual obligations to which the data holder is subject. Where the disclosure of trade secrets of the data holder to public sector bodies or to Union institutions, agencies or bodies is strictly necessary to fulfil the purpose for which the data has been requested, confidentiality of such disclosure should be ensured to the data holder.

(67) When the safeguarding of a significant public good is at stake, such as is the case of responding to public emergencies, the public sector body or the Union institution, agency or body should not be expected to compensate enterprises for the data obtained. Public emergencies are rare events and not all such emergencies require the use of data held by enterprises. The business activities of the data holders are therefore not likely to be negatively affected as a consequence of the public sector bodies or Union institutions, agencies or bodies having recourse to this Regulation. However, as cases of an exceptional need other than responding to a public emergency might be more frequent, including cases of prevention of or recovery from a public emergency, data holders should in such cases be entitled to a reasonable compensation which should not exceed the technical and organisational costs incurred in complying with the request and the reasonable margin required for making the data available to the public sector body or to the Union institution, agency or body. The compensation should not be understood as constituting payment for the data itself and as being compulsory.

---

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

(68) The public sector body or Union institution, agency or body may share the data it has obtained pursuant to the request with other entities or persons when this is needed to carry out scientific research activities or analytical activities it cannot perform itself. Such data may also be shared under the same circumstances with the national statistical institutes and Eurostat for the compilation of official statistics. Such research activities should however be compatible with the purpose for which the data was requested and the data holder should be informed about the further sharing of the data it had provided. Individuals conducting research or research organisations with whom these data may be shared should act either on a not-for-profit basis or in the context of a public-interest mission recognised by the State. Organisations upon which commercial undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, which could result in preferential access to the results of the research, should not be considered research organisations for the purposes of this Regulation.

(69) The ability for customers of data processing services, including cloud and edge services, to switch from one data processing service to another, while maintaining a minimum functionality of service, is a key condition for a more competitive market with lower entry barriers for new service providers.

(70) Regulation (EU) 2018/1807 of the European Parliament and of the Council encourages service providers to effectively develop and implement self-regulatory codes of conduct covering best practices for, *inter alia*, facilitating the switching of data processing service providers and the porting of data. Given the limited efficacy of the self-regulatory frameworks developed in response, and the general unavailability of open standards and interfaces, it is necessary to adopt a set of minimum regulatory obligations on providers of data processing services to eliminate contractual, economic and technical barriers to effective switching between data processing services.

(71) Data processing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other virtual or physical infrastructure, operating systems, software, including software development tools, storage, applications and services. The capability of the customer of the data processing service to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the service provider could be described as on-demand administration. The term ‘broad remote access’ is used to describe that the computing capabilities are provided over the network and accessed through mechanisms promoting the use of heterogeneous thin or thick client platforms (from web browsers to mobile devices and workstations). The term ‘scalable’ refers to computing resources that are flexibly allocated by the data processing service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term ‘elastic pool’ is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase or decrease resources available depending on workload. The term ‘shareable’ is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term ‘distributed’ is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing. The term ‘highly distributed’ is used to describe data processing services that involve data processing

closer to where data are being generated or collected, for instance in a connected data processing device. Edge computing, which is a form of such highly distributed data processing, is expected to generate new business models and cloud service delivery models, which should be open and interoperable from the outset.

(72) This Regulation aims to facilitate switching between data processing services, which encompasses all conditions and actions that are necessary for a customer to terminate a contractual agreement of a data processing service, to conclude one or multiple new contracts with different providers of data processing services, to port all its digital assets, including data, to the concerned other providers and to continue to use them in the new environment while benefitting from functional equivalence. Digital assets refer to elements in digital format for which the customer has the right of use, including data, applications, virtual machines and other manifestations of virtualisation technologies, such as containers. Functional equivalence means the maintenance of a minimum level of functionality of a service after switching, and should be deemed technically feasible whenever both the originating and the destination data processing services cover (in part or in whole) the same service type. Meta-data, generated by the customer's use of a service, should also be portable pursuant to this Regulation's provisions on switching.

(73) Where providers of data processing services are in turn customers of data processing services provided by a third party provider, they will benefit from more effective switching themselves, while simultaneously invariably bound by this Regulation's obligations for what pertains to their own service offerings.

(74) Data processing service providers should be required to offer all assistance and support that is required to make the switching process successful and effective without requiring those data processing service providers to develop new categories of services within or on the basis of the IT-infrastructure of different data processing service providers to guarantee functional equivalence in an environment other than their own systems. Nevertheless, service providers are required to offer all assistance and support that is required to make the switching process effective. Existing rights relating to the termination of contracts, including those introduced by Regulation (EU) 2016/679 and Directive (EU) 2019/770 of the European Parliament and of the Council[67] should not be affected.

(75) To facilitate switching between data processing services, providers of data processing services should consider the use of implementation and/or compliance tools, notably those published by the Commission in the form of a Rulebook relating to cloud services. In particular, standard contractual clauses are beneficial to increase confidence in data processing services, to create a more balanced relationship between users and service providers and to improve legal certainty on the conditions that apply for switching to other data processing services. In this light, users and service providers should consider the use of standard contractual clauses developed by relevant bodies or expert groups established under Union law.

(76) Open interoperability specifications and standards developed in accordance with paragraph 3 and 4 of Annex II of Regulation (EU) 1025/2021 in the field of interoperability and portability enable a seamless multi-vendor cloud environment, which is a key requirement for open innovation in the European data economy. As market-driven processes have not demonstrated the capacity to establish technical

[67] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019, p. 1).

specifications or standards that facilitate effective cloud interoperability at the PaaS (platform-as-a-service) and SaaS (software-as-a-service) levels, the Commission should be able, on the basis of this Regulation and in accordance with Regulation (EU) No 1025/2012, to request European standardisation bodies to develop such standards, particularly for service types where such standards do not yet exist. In addition to this, the Commission will encourage parties in the market to develop relevant open interoperability specifications. The Commission, by way of delegated acts, can mandate the use of European standards for interoperability or open interoperability specifications for specific service types through a reference in a central Union standards repository for the interoperability of data processing services. European standards and open interoperability specifications will only be referenced if in compliance with the criteria specified in this Regulation, which have the same meaning as the requirements in paragraphs 3 and 4 of Annex II of Regulation (EU) No 1025/2021 and the interoperability facets defined under the ISO/IEC 19941:2017.

(77) Third countries may adopt laws, regulations and other legal acts that aim at directly transferring or providing governmental access to non-personal data located outside their borders, including in the Union. Judgments of courts or tribunals or decisions of other judicial or administrative authorities, including law enforcement authorities in third countries requiring such transfer or access to non-personal data should be enforceable when based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. In other cases, situations may arise where a request to transfer or provide access to non-personal data arising from a third country law conflicts with an obligation to protect such data under Union law or national law, in particular as regards the protection of fundamental rights of the individual, such as the right to security and the right to effective remedy, or the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data, including the protection of trade secrets, and the protection of intellectual property rights, and including its contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, transfer or access should only be allowed if it has been verified that the third country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent court in the third country, which is empowered to take duly into account the relevant legal interests of the provider of such data. Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality.

(78) To foster further trust in the data, it is important that safeguards in relation to Union citizens, the public sector and businesses are implemented to the extent possible to ensure control over their data. In addition, Union law, values and standards should be upheld in terms of (but not limited to) security, data protection and privacy, and consumer protection. In order to prevent unlawful access to non-personal data, providers of data processing services subject to this instrument, such as cloud and edge services, should take all reasonable measures to prevent access to the systems where non-personal data is stored, including, where relevant, through the encryption of data,

the frequent submission to audits, the verified adherence to relevant security reassurance certification schemes, and the modification of corporate policies.

(79) Standardisation and semantic interoperability should play a key role to provide technical solutions to ensure interoperability. In order to facilitate the conformity with the requirements for interoperability, it is necessary to provide for a presumption of conformity for interoperability solutions that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council. The Commission should adopt common specifications in areas where no harmonised standards exist or where they are insufficient in order to further enhance interoperability for the common European data spaces, application programming interfaces, cloud switching as well as smart contracts. Additionally, common specifications in the different sectors could remain to be adopted, in accordance with Union or national sectoral law, based on the specific needs of those sectors. Reusable data structures and models (in form of core vocabularies), ontologies, metadata application profile, reference data in the form of core vocabulary, taxonomies, code lists, authority tables, thesauri should also be part of the technical specifications for semantic interoperability. Furthermore, the Commission should be enabled to mandate the development of harmonised standards for the interoperability of data processing services.

(80) To promote the interoperability of smart contracts in data sharing applications, it is necessary to lay down essential requirements for smart contracts for professionals who create smart contracts for others or integrate such smart contracts in applications that support the implementation of agreements for sharing data. In order to facilitate the conformity of such smart contracts with those essential requirements, it is necessary to provide for a presumption of conformity for smart contracts that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council.

(81) In order to ensure the efficient implementation of this Regulation, Member States should designate one or more competent authorities. If a Member State designates more than one competent authority, it should also designate a coordinating competent authority. Competent authorities should cooperate with each other. The authorities responsible for the supervision of compliance with data protection and competent authorities designated under sectoral legislation should have the responsibility for application of this Regulation in their areas of competence.

(82) In order to enforce their rights under this Regulation, natural and legal persons should be entitled to seek redress for the infringements of their rights under this Regulation by lodging complaints with competent authorities. Those authorities should be obliged to cooperate to ensure the complaint is appropriately handled and resolved. In order to make use of the consumer protection cooperation network mechanism and to enable representative actions, this Regulation amends the Annexes to the Regulation (EU) 2017/2394 of the European Parliament and of the Council[68] and Directive (EU) 2020/1828 of the European Parliament and of the Council[69].

---

68 Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, p. 1).

69 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

(83) Member States competent authorities should ensure that infringements of the obligations laid down in this Regulation are sanctioned by penalties. When doing so, they should take into account the nature, gravity, recurrence and duration of the infringement in view of the public interest at stake, the scope and kind of activities carried out, as well as the economic capacity of the infringer. They should take into account whether the infringer systematically or recurrently fails to comply with its obligations stemming from this Regulation. In order to help enterprises to draft and negotiate contracts, the Commission should develop and recommend non-mandatory model contractual terms for business-to-business data sharing contracts, where necessary taking into account the conditions in specific sectors and the existing practices with voluntary data sharing mechanisms. These model contractual terms should be primarily a practical tool to help in particular smaller enterprises to conclude a contract. When used widely and integrally, these model contractual terms should also have the beneficial effect of influencing the design of contracts about access to and use of data and therefore lead more broadly towards fairer contractual relations when accessing and sharing data.

(84) In order to eliminate the risk that holders of data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service claim the *sui generis* right under Article 7 of Directive 96/9/EC where such databases do not qualify for the *sui generis* right, and in so doing hinder the effective exercise of the right of users to access and use data and the right to share data with third parties under this Regulation, this Regulation should clarify that the *sui generis* right does not apply to such databases as the requirements for protection would not be fulfilled.

(85) In order to take account of technical aspects of data processing services, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of supplementing this Regulation to introduce a monitoring mechanism on switching charges imposed by data processing service providers on the market, to further specify the essential requirements for operators of data spaces and data processing service providers on interoperability and to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[70]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(86) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of supplementing this Regulation to adopt common specifications to ensure the interoperability of common European data spaces and data sharing, the switching between data processing services, the interoperability of smart contracts as well as for technical means, such as application programming interfaces, for enabling transmission of data between parties including continuous or real-time and for core vocabularies of semantic interoperability, and to adopt common specifications for

[70] OJ L 123, 12.5.2016, p. 1.

smart contracts. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[71].

(87) This Regulation should not affect specific provisions of acts of the Union adopted in the field of data sharing between businesses, between businesses and consumers and between businesses and public sector bodies that were adopted prior to the date of the adoption of this Regulation. To ensure consistency and the smooth functioning of the internal market, the Commission should, where relevant, evaluate the situation with regard to the relationship between this Regulation and the acts adopted prior to the date of adoption of this Regulation regulating data sharing, in order to assess the need for alignment of those specific provisions with this Regulation. This Regulation should be without prejudice to rules addressing needs specific to individual sectors or areas of public interest. Such rules may include additional requirements on technical aspects of the data access, such as interfaces for data access, or how data access could be provided, for example directly from the product or via data intermediation services. Such rules may also include limits on the rights of data holders to access or use user data, or other aspects beyond data access and use, such as governance aspects. This Regulation also should be without prejudice to more specific rules in the context of the development of common European data spaces.

(88) This Regulation should not affect the application of the rules of competition, and in particular Articles 101 and 102 of the Treaty. The measures provided for in this Regulation should not be used to restrict competition in a manner contrary to the Treaty.

(89) In order to allow the economic actors to adapt to the new rules laid out in this Regulation, they should apply from a year after entry into force of the Regulation.

(90) 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 a joint opinion on [XX XX 2022].

HAVE ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter and scope

1. This Regulation lays down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients, and on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest:

2. This Regulation applies to:

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

(a) manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services;

(b) data holders that make data available to data recipients in the Union;

(c) data recipients in the Union to whom data are made available;

(d) public sector bodies and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request;

(e) providers of data processing services offering such services to customers in the Union.

3. Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect the applicability of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC, including the powers and competences of supervisory authorities. Insofar as the rights laid down in Chapter II of this Regulation are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679.

4. This Regulation shall not affect Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including Regulation (EU) 2021/784 of the European Parliament and of the Council[72] and the [e-evidence proposals [COM(2018) 225 and 226] once adopted, and international cooperation in that area. This Regulation shall not affect the collection, sharing, access to and use of data under Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing and Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying the transfer of funds. This Regulation shall not affect the competences of the Member States regarding activities concerning public security, defence, national security, customs and tax administration and the health and safety of citizens in accordance with Union law.

Article 2
Definitions

For the purposes of this Regulation, the following definitions apply:

(1) ‘data’ means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording;

(2) ‘product’ means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or

[72] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79).

environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data;

(3) ‘related service’ means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions;

(4) ‘virtual assistants’ means software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access their own and third party services or control their own and third party devices;

(5) ‘user’ means a natural or legal person that owns, rents or leases a product or receives a services;

(6) ‘data holder’ means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data;

(7) ‘data recipient’ means a legal or natural person, acting for purposes which are related to that person’s trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law;

(8) ‘enterprise’ means a natural or legal person which in relation to contracts and practices covered by this Regulation is acting for purposes which are related to that person’s trade, business, craft or profession;

(9) ‘public sector body’ means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies;

(10) ‘public emergency’ means an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s);

(11) ‘processing’ means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(12) ‘data processing service’ means a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature;

(13) ‘service type’ means a set of data processing services that share the same primary objective and basic data processing service model;

(14) ‘functional equivalence’ means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract;

(15) ‘open interoperability specifications’ mean ICT technical specifications, as defined in Regulation (EU) No 1025/2012, which are performance oriented towards achieving interoperability between data processing services;

(16) ‘smart contract’ means a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger;

(17) ‘electronic ledger’ means an electronic ledger within the meaning of Article 3, point (53), of Regulation (EU) No 910/2014;

(18) ‘common specifications’ means a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation;

(19) ‘interoperability’ means the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data in order to perform their functions;

(20) ‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012.

CHAPTER II
BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING

Article 3

Obligation to make data generated by the use of products or related services accessible

1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.

2. Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format:

   (a) the nature and volume of the data likely to be generated by the use of the product or related service;

   (b) whether the data is likely to be generated continuously and in real-time;

   (c) how the user may access those data;

   (d) whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used;

(e) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established;

(f) the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently;

(g) how the user may request that the data are shared with a third-party;

(h) the user's right to lodge a complaint alleging a violation of the provisions of this Chapter with the competent authority referred to in Article 31.

Article 4

The right of users to access and use data generated by the use of products or related services

1. Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.

2. The data holder shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. The data holder shall not keep any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure.

3. Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.

4. The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate.

5. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.

6. The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active.

Article 5

Right to share data with third parties

1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.

2. Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper, pursuant to Article […] of [Regulation XXX on contestable and fair markets in the digital sector (Digital Markets Act)[73]], shall not be an eligible third party under this Article and therefore shall not:

   (a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1);

   (b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;

   (c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).

3. The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1. The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.

4. The third party shall not deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.

5. The data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time.

6. Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.

7. Any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation.

8. Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. In such a case, the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party.

9. The right referred to in paragraph 1 shall not adversely affect data protection rights of others.

---

[73] OJ […].

Article 6

Obligations of third parties receiving data at the request of the user

1. A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose.

2. The third party shall not:

   (a) coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user;

   (b) use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of Regulation (EU) 2016/679, unless it is necessary to provide the service requested by the user;

   (c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;

   (d) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article […] of [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)];

   (e) use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose;

   (f) prevent the user, including through contractual commitments, from making the data it receives available to other parties.

Article 7

Scope of business to consumer and business to business data sharing obligations

1. The obligations of this Chapter shall not apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as micro or small enterprises, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro or small enterprise.

2. Where this Regulation refers to products or related services, such reference shall also be understood to include virtual assistants, insofar as they are used to access or control a product or related service.

CHAPTER III
OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE

Article 8
Conditions under which data holders make data available to data recipients

1. Where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV.

2. A data holder shall agree with a data recipient the terms for making the data available. A contractual term concerning the access to and use of the data or the liability and remedies for the breach or the termination of data related obligations shall not be binding if it fulfils the conditions of Article 13 or if it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II.

3. A data holder shall not discriminate between comparable categories of data recipients, including partner enterprises or linked enterprises, as defined in Article 3 of the Annex to Recommendation 2003/361/EC, of the data holder, when making data available. Where a data recipient considers the conditions under which data has been made available to it to be discriminatory, it shall be for the data holder to demonstrate that there has been no discrimination.

4. A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II.

5. Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation implementing Union law.

6. Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.

Article 9
Compensation for making data available

1. Any compensation agreed between a data holder and a data recipient for making data available shall be reasonable.

2. Where the data recipient is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly.

3. This Article shall not preclude other Union law or national legislation implementing Union law from excluding compensation for making data available or providing for lower compensation.

4. The data holder shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can verify that the requirements of paragraph 1 and, where applicable, paragraph 2 are met.

Article 10
Dispute settlement

1. Data holders and data recipients shall have access to dispute settlement bodies, certified in accordance with paragraph 2 of this Article, to settle disputes in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available in accordance with Articles 8 and 9.

2. The Member State where the dispute settlement body is established shall, at the request of that body, certify the body, where the body has demonstrated that it meets all of the following conditions:

   (a) it is impartial and independent, and it will issue its decisions in accordance with clear and fair rules of procedure;

   (b) it has the necessary expertise in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available, allowing the body to effectively determine those terms;

   (c) it is easily accessible through electronic communication technology;

   (d) it is capable of issuing its decisions in a swift, efficient and cost-effective manner and in at least one official language of the Union.

   If no dispute settlement body is certified in a Member State by [date of application of the Regulation], that Member State shall establish and certify a dispute settlement body that fulfils the conditions set out in points (a) to (d) of this paragraph.

3. Member States shall notify to the Commission the dispute settlement bodies certified in accordance with paragraph 2. The Commission shall publish a list of those bodies on a dedicated website and keep it updated.

4. Dispute settlement bodies shall make the fees, or the mechanisms used to determine the fees, known to the parties concerned before those parties request a decision.

5. Dispute settlement bodies shall refuse to deal with a request to resolve a dispute that has already been brought before another dispute settlement body or before a court or a tribunal of a Member State.

6. Dispute settlement bodies shall grant the parties the possibility, within a reasonable period of time, to express their point of view on matters those parties have brought before those bodies. In that context, dispute settlement bodies shall provide those parties with the submissions of the other party and any statements made by experts. Those bodies shall grant the parties the possibility to comment on those submissions and statements.

7. Dispute settlement bodies shall issue their decision on matters referred to them no later than 90 days after the request for a decision has been made. Those decisions shall be in writing or on a durable medium and shall be supported by a statement of reasons supporting the decision.

8. The decision of the dispute settlement body shall only be binding on the parties if the parties have explicitly consented to its binding nature prior to the start of the dispute settlement proceedings.

9. This Article does not affect the right of the parties to seek an effective remedy before a court or tribunal of a Member State.

Article 11

Technical protection measures and provisions on unauthorised use or disclosure of data

1. The data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not be used as a means to hinder the user's right to effectively provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1).

2. A data recipient that has, for the purposes of obtaining data, provided inaccurate or false information to the data holder, deployed deceptive or coercive means or abused evident gaps in the technical infrastructure of the data holder designed to protect the data, has used the data made available for unauthorised purposes or has disclosed those data to another party without the data holder's authorisation, shall without undue delay, unless the data holder or the user instruct otherwise:

   (a) destroy the data made available by the data holder and any copies thereof;

   (b) end the production, offering, placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods.

3. Paragraph 2, point (b), shall not apply in either of the following cases:

   (a) use of the data has not caused significant harm to the data holder;

   (b) it would be disproportionate in light of the interests of the data holder.

Article 12

Scope of obligations for data holders legally obliged to make data available

1. This Chapter shall apply where a data holder is obliged under Article 5, or under Union law or national legislation implementing Union law, to make data available to a data recipient.

2. Any contractual term in a data sharing agreement which, to the detriment of one party, or, where applicable, to the detriment of the user, excludes the application of this Chapter, derogates from it, or varies its effect, shall not be binding on that party.

3. This Chapter shall only apply in relation to obligations to make data available under Union law or national legislation implementing Union law, which enter into force after [date of application of the Regulation].

CHAPTER IV
UNFAIR TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES

Article 13

Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise

1. A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC shall not be binding on the latter enterprise if it is unfair.

2. A contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.

3. A contractual term is unfair for the purposes of this Article if its object or effect is to:

   (a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;

   (b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in case of breach of those obligations;

   (c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract.

4. A contractual term is presumed unfair for the purposes of this Article if its object or effect is to:

   (a) inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;

   (b) allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;

   (c) prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner;

   (d) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof;

   (e) enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and

comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so.

5. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed.

6. Where the unfair contractual term is severable from the remaining terms of the contract, those remaining terms shall remain binding.

7. This Article does not apply to contractual terms defining the main subject matter of the contract or to contractual terms determining the price to be paid.

8. The parties to a contract covered by paragraph 1 may not exclude the application of this Article, derogate from it, or vary its effects.

CHAPTER V
MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES AND UNION INSTITUTIONS, AGENCIES OR BODIES BASED ON EXCEPTIONAL NEED

Article 14
Obligation to make data available based on exceptional need

1. Upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.

2. This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.

Article 15
Exceptional need to use data

An exceptional need to use data within the meaning of this Chapter shall be deemed to exist in any of the following circumstances:

(a) where the data requested is necessary to respond to a public emergency;

(b) where the data request is limited in time and scope and necessary to prevent a public emergency or to assist the recovery from a public emergency;

(c) where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law; and

(1) the public sector body or Union institution, agency or body has been unable to obtain such data by alternative means, including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data; or

(2) obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises.

Article 16

Relationship with other obligations to make data available to public sector bodies and Union institutions, agencies and bodies

1. This Chapter shall not affect obligations laid down in Union or national law for the purposes of reporting, complying with information requests or demonstrating or verifying compliance with legal obligations.

2. The rights from this Chapter shall not be exercised by public sector bodies and Union institutions, agencies and bodies in order to carry out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration. This Chapter does not affect the applicable Union and national law on the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, or for customs or taxation administration.

Article 17

Requests for data to be made available

1. Where requesting data pursuant to Article 14(1), a public sector body or a Union institution, agency or body shall:

   (a) specify what data are required;

   (b) demonstrate the exceptional need for which the data are requested;

   (c) explain the purpose of the request, the intended use of the data requested, and the duration of that use;

   (d) state the legal basis for requesting the data;

   (e) specify the deadline by which the data are to be made available or within which the data holder may request the public sector body, Union institution, agency or body to modify or withdraw the request.

2. A request for data made pursuant to paragraph 1 of this Article shall:

   (a) be expressed in clear, concise and plain language understandable to the data holder;

   (b) be proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested;

   (c) respect the legitimate aims of the data holder, taking into account the protection of trade secrets and the cost and effort required to make the data available;

   (d) concern, insofar as possible, non-personal data;

   (e) inform the data holder of the penalties that shall be imposed pursuant to Article 33 by a competent authority referred to in Article 31 in the event of non-compliance with the request;

(f) be made publicly available online without undue delay.

3. A public sector body or a Union institution, agency or body shall not make data obtained pursuant to this Chapter available for reuse within the meaning of Directive (EU) 2019/1024. Directive (EU) 2019/1024 shall not apply to the data held by public sector bodies obtained pursuant to this Chapter.

4. Paragraph 3 does not preclude a public sector body or a Union institution, agency or body to exchange data obtained pursuant to this Chapter with another public sector body, Union institution, agency or body, in view of completing the tasks in Article 15 or to make the data available to a third party in cases where it has outsourced, by means of a publicly available agreement, technical inspections or other functions to this third party. The obligations on public sector bodies, Union institutions, agencies or bodies pursuant to Article 19 apply.

Where a public sector body or a Union institution, agency or body transmits or makes data available under this paragraph, it shall notify the data holder from whom the data was received.

Article 18
Compliance with requests for data

1. A data holder receiving a request for access to data under this Chapter shall make the data available to the requesting public sector body or a Union institution, agency or body without undue delay.

2. Without prejudice to specific needs regarding the availability of data defined in sectoral legislation, the data holder may decline or seek the modification of the request within 5 working days following the receipt of a request for the data necessary to respond to a public emergency and within 15 working days in other cases of exceptional need, on either of the following grounds:

   (a) the data is unavailable;

   (b) the request does not meet the conditions laid down in Article 17(1) and (2).

3. In case of a request for data necessary to respond to a public emergency, the data holder may also decline or seek modification of the request if the data holder already provided the requested data in response to previously submitted request for the same purpose by another public sector body or Union institution agency or body and the data holder has not been notified of the destruction of the data pursuant to Article 19(1), point (c).

4. If the data holder decides to decline the request or to seek its modification in accordance with paragraph 3, it shall indicate the identity of the public sector body or Union institution agency or body that previously submitted a request for the same purpose.

5. Where compliance with the request to make data available to a public sector body or a Union institution, agency or body requires the disclosure of personal data, the data holder shall take reasonable efforts to pseudonymise the data, insofar as the request can be fulfilled with pseudonymised data.

6. Where the public sector body or the Union institution, agency or body wishes to challenge a data holder's refusal to provide the data requested, or to seek

modification of the request, or where the data holder wishes to challenge the request, the matter shall be brought to the competent authority referred to in Article 31.

Article 19

Obligations of public sector bodies and Union institutions, agencies and bodies

1. A public sector body or a Union institution, agency or body having received data pursuant to a request made under Article 14 shall:

   (a) not use the data in a manner incompatible with the purpose for which they were requested;

   (b) implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects;

   (c) destroy the data as soon as they are no longer necessary for the stated purpose and inform the data holder that the data have been destroyed.

2. Disclosure of trade secrets or alleged trade secrets to a public sector body or to a Union institution, agency or body shall only be required to the extent that it is strictly necessary to achieve the purpose of the request. In such a case, the public sector body or the Union institution, agency or body shall take appropriate measures to preserve the confidentiality of those trade secrets.

Article 20

Compensation in cases of exceptional need

1. Data made available to respond to a public emergency pursuant to Article 15, point (a), shall be provided free of charge.

2. Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15, points (b) or (c), such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the Union institution, agency or body requesting the data, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.

Article 21

Contribution of research organisations or statistical bodies in the context of exceptional needs

1. A public sector body or a Union institution, agency or body shall be entitled to share data received under this Chapter with individuals or organisations in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested, or to national statistical institutes and Eurostat for the compilation of official statistics.

2. Individuals or organisations receiving the data pursuant to paragraph 1 shall act on a not-for-profit basis or in the context of a public-interest mission recognised in Union or Member State law. They shall not include organisations upon which commercial undertakings have a decisive influence or which could result in preferential access to the results of the research.

3. Individuals or organisations receiving the data pursuant to paragraph 1 shall comply with the provisions of Article 17(3) and Article 19.

4. Where a public sector body or a Union institution, agency or body transmits or makes data available under paragraph 1, it shall notify the data holder from whom the data was received.

Article 22
Mutual assistance and cross-border cooperation

1. Public sector bodies and Union institutions, agencies and bodies shall cooperate and assist one another, to implement this Chapter in a consistent manner.

2. Any data exchanged in the context of assistance requested and provided pursuant to paragraph 1 shall not be used in a manner incompatible with the purpose for which they were requested.

3. Where a public sector body intends to request data from a data holder established in another Member State, it shall first notify the competent authority of that Member State as referred to in Article 31, of that intention. This requirement shall also apply to requests by Union institutions, agencies and bodies.

4. After having been notified in accordance with paragraph 3, the relevant competent authority shall advise the requesting public sector body of the need, if any, to cooperate with public sector bodies of the Member State in which the data holder is established, with the aim of reducing the administrative burden on the data holder in complying with the request. The requesting public sector body shall take the advice of the relevant competent authority into account.

CHAPTER VI

SWITCHING BETWEEN DATA PROCESSING SERVICES

Article 23
Removing obstacles to effective switching between providers of data processing services

1. Providers of a data processing service shall take the measures provided for in Articles 24, 25 and 26 to ensure that customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider. In particular, providers of data processing service shall remove commercial, technical, contractual and organisational obstacles, which inhibit customers from:

   (a) terminating, after a maximum notice period of 30 calendar days, the contractual agreement of the service;

   (b) concluding new contractual agreements with a different provider of data processing services covering the same service type;

   (c) porting its data, applications and other digital assets to another provider of data processing services;

   (d) maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type, in accordance with Article 26.

2. Paragraph 1 shall only apply to obstacles that are related to the services, contractual agreements or commercial practices provided by the original provider.

Article 24

Contractual terms concerning switching between providers of data processing services

1. The rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services shall be clearly set out in a written contract. Without prejudice to Directive (EU) 2019/770, that contract shall include at least the following:

   (a) clauses allowing the customer, upon request, to switch to a data processing service offered by another provider of data processing service or to port all data, applications and digital assets generated directly or indirectly by the customer to an on-premise system, in particular the establishment of a mandatory maximum transition period of 30 calendar days, during which the data processing service provider shall:

      (1) assist and, where technically feasible, complete the switching process;

      (2) ensure full continuity in the provision of the respective functions or services.

   (b) an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service;

   (c) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the service provider, in accordance with paragraph 1, point (a) and paragraph 2.

2. Where the mandatory transition period as defined in paragraph 1, points (a) and (c) of this Article is technically unfeasible, the provider of data processing services shall notify the customer within 7 working days after the switching request has been made, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period, which may not exceed 6 months. In accordance with paragraph 1 of this Article, full service continuity shall be ensured throughout the alternative transition period against reduced charges, referred to in Article 25(2).

Article 25

Gradual withdrawal of switching charges

1. From [date X+3yrs] onwards, providers of data processing services shall not impose any charges on the customer for the switching process.

2. From [date X, the date of entry into force of the Data Act] until [date X+3yrs], providers of data processing services may impose reduced charges on the customer for the switching process.

3. The charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned.

4. The Commission is empowered to adopt delegated acts in accordance with Article 38 to supplement this Regulation in order to introduce a monitoring mechanism for the Commission to monitor switching charges imposed by data processing service providers on the market to ensure that the withdrawal of switching charges as described in paragraph 1 of this Article will be attained in accordance with the deadline provided in the same paragraph.

Article 26
Technical aspects of switching

1. Providers of data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall ensure that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service.
2. For data processing services other than those covered by paragraph 1, providers of data processing services shall make open interfaces publicly available and free of charge.
3. For data processing services other than those covered by paragraph 1, providers of data processing services shall ensure compatibility with open interoperability specifications or European standards for interoperability that are identified in accordance with Article 29(5) of this Regulation.
4. Where the open interoperability specifications or European standards referred to in paragraph 3 do not exist for the service type concerned, the provider of data processing services shall, at the request of the customer, export all data generated or co-generated, including the relevant data formats and data structures, in a structured, commonly used and machine-readable format.

CHAPTER VII
INTERNATIONAL CONTEXTS NON-PERSONAL DATA SAFEGUARDS

Article 27
International access and transfer

1. Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.
2. Any decision or judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a provider of data processing services to transfer from or give access to non-personal data within the scope of this Regulation held in the Union may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between

the requesting third country and the Union or any such agreement between the requesting third country and a Member State.

3. In the absence of such an international agreement, where a provider of data processing services is the addressee of a decision of a court or a tribunal or a decision of an administrative authority of a third country to transfer from or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only:

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

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

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

The addressee of the decision may ask the opinion of the relevant competent bodies or authorities, pursuant to this Regulation, in order to determine whether these conditions are met, notably when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States.

The European Data Innovation Board established under Regulation [xxx – DGA] shall advise and assist the Commission in developing guidelines on the assessment of whether these conditions are met.

4. If the conditions in paragraph 2 or 3 are met, the provider of data processing services shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation thereof.

5. The provider of data processing services shall inform the data holder about the existence of a request of an administrative authority in a third-country to access its data before complying with its request, except in cases where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

CHAPTER VIII
INTEROPERABILITY

Article 28
Essential requirements regarding interoperability

1. Operators of data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services:

   (a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

(b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner;

(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;

(d) the means to enable the interoperability of smart contracts within their services and activities shall be provided.

These requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements coming from other Union or national sectoral legislation.

2. The Commission is empowered to adopt delegated acts, in accordance with Article 38 to supplement this Regulation by further specifying the essential requirements referred to in paragraph 1.

3. Operators of data spaces that meet the harmonised standards or parts thereof published by reference in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements referred to in paragraph 1 of this Article, to the extent those standards cover those requirements.

4. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements under paragraph 1 of this Article

5. The Commission shall, by way of implementing acts, adopt common specifications, where harmonised standards referred to in paragraph 4 of this Article do not exist or in case it considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article, where necessary, with respect to any or all of the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

6. The Commission may adopt guidelines laying down interoperability specifications for the functioning of common European data spaces, such as architectural models and technical standards implementing legal rules and arrangements between parties that foster data sharing, such as regarding rights to access and technical translation of consent or permission.

Article 29
Interoperability for data processing services

1. Open interoperability specifications and European standards for the interoperability of data processing services shall:

(a) be performance oriented towards achieving interoperability between different data processing services that cover the same service type;

(b) enhance portability of digital assets between different data processing services that cover the same service type;

(c) guarantee, where technically feasible, functional equivalence between different data processing services that cover the same service type.

2. Open interoperability specifications and European standards for the interoperability of data processing services shall address:

(a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;

(b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;

(c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

3. Open interoperability specifications shall comply with paragraph 3 and 4 of Annex II of Regulation (EU) No 1025/2012.

4. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft European standards applicable to specific service types of data processing services.

5. For the purposes of Article 26(3) of this Regulation, the Commission shall be empowered to adopt delegated acts, in accordance with Article 38, to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services in central Union standards repository for the interoperability of data processing services, where these satisfy the criteria specified in paragraph 1 and 2 of this Article.

Article 30

Essential requirements regarding smart contracts for data sharing

1. The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements:

(a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

(b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;

(c) data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and

(d) access control: a smart contract shall be protected through rigorous access control mechanisms at the governance and smart contract layers.

2. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the

context of an agreement to make data available shall perform a conformity assessment with a view to fulfilling the essential requirements under paragraph 1 and, on the fulfilment of the requirements, issue an EU declaration of conformity.

3. By drawing up the EU declaration of conformity, the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall be responsible for compliance with the requirements under paragraph 1.

4. A smart contract that meets the harmonised standards or the relevant parts thereof drawn up and published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements under paragraph 1 of this Article to the extent those standards cover those requirements.

5. The Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential the requirements under paragraph 1 of this Article.

6. Where harmonised standards referred to in paragraph 4 of this Article do not exist or where the Commission considers that the relevant harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article in a cross-border context, the Commission may, by way of implementing acts, adopt common specifications in respect of the essential requirements set out in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

CHAPTER IX
IMPLEMENTATION AND ENFORCEMENT

Article 31
Competent authorities

1. Each Member State shall designate one or more competent authorities as responsible for the application and enforcement of this Regulation. Member States may establish one or more new authorities or rely on existing authorities.

2. Without prejudice to paragraph 1 of this Article:

   (a) the independent supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned. Chapters VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to the processing of personal data;

   (b) for specific sectoral data exchange issues related to the implementation of this Regulation, the competence of sectoral authorities shall be respected;

   (c) the national competent authority responsible for the application and enforcement of Chapter VI of this Regulation shall have experience in the field of data and electronic communications services.

3. Member States shall ensure that the respective tasks and powers of the competent authorities designated pursuant to paragraph 1 of this Article are clearly defined and include:

(a) promoting awareness among users and entities falling within scope of this Regulation of the rights and obligations under this Regulation;

(b) handling complaints arising from alleged violations of this Regulation, and investigating, to the extent appropriate, the subject matter of the complaint and informing the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another competent authority is necessary;

(c) conducting investigations into matters that concern the application of this Regulation, including on the basis of information received from another competent authority or other public authority;

(d) imposing, through administrative procedures, dissuasive financial penalties which may include periodic penalties and penalties with retroactive effect, or initiating legal proceedings for the imposition of fines;

(e) monitoring technological developments of relevance for the making available and use of data;

(f) cooperating with competent authorities of other Member States to ensure the consistent application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay;

(g) ensuring the online public availability of requests for access to data made by public sector bodies in the case of public emergencies under Chapter V;

(h) cooperating with all relevant competent authorities to ensure that the obligations of Chapter VI are enforced consistently with other Union legislation and self-regulation applicable to providers of data processing service;

(i) ensuring that charges for the switching between providers of data processing services are withdrawn in accordance with Article 25.

4. Where a Member State designates more than one competent authority, the competent authorities shall, in the exercise of the tasks and powers assigned to them under paragraph 3 of this Article, cooperate with each other, including, as appropriate, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679, to ensure the consistent application of this Regulation. In such cases, relevant Member States shall designate a coordinating competent authority.

5. Member States shall communicate the name of the designated competent authorities and their respective tasks and powers and, where applicable, the name of the coordinating competent authority to the Commission. The Commission shall maintain a public register of those authorities.

6. When carrying out their tasks and exercising their powers in accordance with this Regulation, the competent authorities shall remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party.

7. Member States shall ensure that the designated competent authorities are provided with the necessary resources to adequately carry out their tasks in accordance with this Regulation.

Article 32
Right to lodge a complaint with a competent authority

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed.

2. The competent authority with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken.

3. Competent authorities shall cooperate to handle and resolve complaints, including by exchanging all relevant information by electronic means, without undue delay. This cooperation shall not affect the specific cooperation mechanism provided for by Chapters VI and VII of Regulation (EU) 2016/679.

Article 33
Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

2. Member States shall by [date of application of the Regulation] notify the Commission of those rules and measures and shall notify it without delay of any subsequent amendment affecting them.

3. For infringements of the obligations laid down in Chapter II, III and V of this Regulation, the supervisory authorities referred to in Article 51 of the Regulation (EU) 2016/679 may within their scope of competence impose administrative fines in line with Article 83 of Regulation (EU) 2016/679 and up to the amount referred to in Article 83(5) of that Regulation.

4. For infringements of the obligations laid down in Chapter V of this Regulation, the supervisory authority referred to in Article 52 of Regulation (EU) 2018/1725 may impose within its scope of competence administrative fines in accordance with Article 66 of Regulation (EU) 2018/1725 up to the amount referred to in Article 66(3) of that Regulation.

Article 34
Model contractual terms

The Commission shall develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations.

CHAPTER X
SUI GENERIS RIGHT UNDER DIRECTIVE 1996/9/EC

Article 35
Databases containing certain data

In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the *sui generis* right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service.

CHAPTER XI
FINAL PROVISIONS

Article 36
Amendment to Regulation (EU) No 2017/2394

In the Annex to Regulation (EU) No 2017/2394 the following point is added:

'29. [Regulation (EU) XXX of the European Parliament and of the Council [Data Act]].'

Article 37
Amendment to Directive (EU) 2020/1828

In the Annex to Directive (EU) 2020/1828 the following point is added:

'67. [Regulation (EU) XXX of the European Parliament and of the Council [Data Act]]'

Article 38
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 Articles 25(4), 28(2) and 29(5) shall be conferred on the Commission for an indeterminate period of time from […].
3. The delegation of power referred to in Articles 25(4), 28(2) and 29(5) 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 on Better Law-Making of 13 April 2016.
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 Articles 25(4), 28(2) and 29(5) 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 39
Committee procedure

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

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

Article 40
Other Union legal acts governing rights and obligations on data access and use

1. The specific obligations for the making available of data between businesses, between businesses and consumers, and on exceptional basis between businesses and public bodies, in Union legal acts that entered into force on or before [xx XXX xxx], and delegated or implementing acts based thereupon, shall remain unaffected.

2. This Regulation is without prejudice to Union legislation specifying, in light of the needs of a sector, a common European data space, or an area of public interest, further requirements, in particular in relation to:

   (a) technical aspects of data access;

   (b) limits on the rights of data holders to access or use certain data provided by users;

   (c) aspects going beyond data access and use.

Article 41
Evaluation and review

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

(a) other categories or types of data to be made accessible;

(b) the exclusion of certain categories of enterprises as beneficiaries under Article 5;

(c) other situations to be deemed as exceptional needs for the purpose of Article 15;

(d) changes in contractual practices of data processing service providers and whether this results in sufficient compliance with Article 24;

(e) diminution of charges imposed by data processing service providers for the switching process, in line with the gradual withdrawal of switching charges pursuant to Article 25.

Article 42
Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from [12 months after the date of entry into force of this Regulation].

Done at Brussels,

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