insurance europe

News Flash

Nº: **FLASH-22-011** Date: **04-02-2022**

To: Insurtech PG, Data Protection PG, Conduct of Business Committee, Connected & Automated Driving PG, Cyber Insurance PG

Leaked: EC proposal for a Data Act

The secretariat has obtained the following leaked document (see **Annex**) containing the draft European Commission's (EC) proposal for the Data Act.

The Data Act would introduce the principle that every user, individual or organisation, must have **access to the data** it contributed to generate. IoT products and related services should make the data available to the user in an accessible manner by default. According to the draft, the data holder must, upon request by a user, or by a third party authorised by the user, make available the data generated by the use of a product or related service to a third party, without undue delay and, where applicable, continuously and in real-time.

Where a data holder is obliged to make data available to a third party, the contractual terms should be **fair, reasonable and non-discriminatory**, otherwise they would be considered null. The proposal would reverse the burden of proof by saying that "where the other enterprise considers conditions to be discriminatory, it shall be for the data holder to prove that there has been no such discrimination." In case of disagreement, the two parties can refer to **dispute settlement bodies** certified by member states.

Public bodies **may request companies** to provide data in exceptional circumstances, notably to respond to a public emergency, including for example natural disasters, public health emergencies and terrorist attacks. In case of emergency, the data should be provided free of charge, however, the data holder can seek compensation equal to the actual costs in certain cases.

Providers of cloud and other data processing services would be legally required to ensure '**switchability'** by guaranteeing a minimum level of functionality of **cloud services** across different providers.

Finally, on international data transfers, cloud service providers must take all reasonable technical, legal and organisational measures to prevent governmental access or transfers of non-personal data that would conflict with European or national law.

Next steps

- The EC is expected to formally adopt the Data Act proposal on 23 February.
- The secretariat will further analyse the leaked version.

For more info

Danilo Gattullo, policy advisor, conduct of business, Gattullo@insuranceeurope.eu, +32 2 896 48 24
Cristina Guerrero Fabra, policy advisor, general insurance, guerrerofabra@insuranceeurope.eu, +32 2 896 48 34

© Insurance Europe. Confidential, internal document.
Not for distribution, all rights reserved.

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Regulation on ensuring fairness in the allocation of value across the data economy (Data Act).

Data is at the core 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 but most data are unused, or their value is concentrated in the hands of relatively few large companies. Low trust in data-sharing, conflicting economic incentives and technological obstacles do not allow for the full realisation of the potential of data-driven innovation. It is therefore crucial to unlock such potential by opening opportunities for the reuse of data and removing barriers to the development of the European data economy in full respect of European rules and values. Ensuring a more balanced distribution of the value of data in tempo with the next wave of non-personal industrial data and the proliferation of Internet-of-Things (IoT) devices means that the potential for boosting a sustainable data economy in Europe is enormous.

Regulating data access and use is fundamental to grasp the opportunities from the digital age. The President of the Commission, Ursula von der Leyen, declared 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 ensuing Commission Work Programme 2020[2] outlined several strategic objectives, including the European Strategy for Data[3], which was adopted in February 2020. The data strategy aims at building a genuine single market for data and at making Europe a global leader in the data-agile economy. In this respect, the Data Act is a key pillar and the second major initiative announced in the data strategy. It contributes most notably to the creation of a cross-sectoral governance framework for data access and use by legislating on issues that affect relation between actors in the data economy 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, it recalled '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 interoperability'[6]. With regard to cloud services, on 15 October 2020, the EU Member States unanimously adopted a

---

[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.

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

Obtenu par CONTEXTE

Joint Declaration on building the next generation cloud for businesses and the public sector in the EU, which calls for a next generation EU cloud offering that reaches the highest standards, for example in portability and interoperability[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 a greater and fair business-to-business, business-to-government, government-to-business and government-to-government flow of data in all sectors[8]. Similarly, in that resolution, the European Parliament highlighted the need to create common European data spaces that ensure the free flow of non-personal data across borders and sectors and between businesses, academia, the relevant stakeholders and the public sector. It also encouraged the Commission to clarify utilisation rights, notably in business-to-business and business-to-government settings, and stressed that market imbalances deriving from the concentration of data restrict competition and increase market entry barriers and diminish wider data access and use. It noted that business-to-business contractual agreements do not necessarily guarantee adequate access to data for SMEs owing to disparities in negotiation power and expertise, and hence stressed the need for contracts to set clear obligations and liability for accessing, processing, sharing and storing of data in order to limit the misuse of such data. As such, the Commission and the Member States were requested to examine actors' rights and obligations to access data they have been involved in generating and to improve their awareness, 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 business-to-government, the Commission was called on to define 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 of force majeure.

Against this political background, the Commission puts forward the proposed **Data Act** with the **aim to ensure fairness in the allocation of data value among actors in the data economy and to foster access to and use of data**. The proposal will serve broader policy goals of ensuring EU businesses across all sectors are in a position to innovate and compete, individuals are effectively empowered with respect to their data, and public bodies better equipped to tackle major policy challenges, including public emergencies.

The specific objectives of the proposal are to:

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

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 situations where compulsory business-to-government data sharing is justified, in order to support

[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))

[9] OJ L 77, 27.3.1996, p. 20–28

Obtenu par COMITEXTE

evidence-based, effective, efficient, and performance-oriented 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 sectorial ecosystems. The level of trust in data processing services determines the uptake of such services by users across sectors of the economy.

Provide for safeguards against unlawful data transfer without notification by the cloud service provider. Concerns around unlawful access by non-EU/EEA governments have been raised. 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 to address barriers to data sharing within and between domain-specific common European data spaces and also between other data not subject to a specific common European data space. The proposal also supports setting standards for "smart contracts", meaning computer programs on electronic ledgers that execute and settle transactions based on pre-determined conditions, with the potential to provide guarantees to data holders and data recipients that conditions for sharing data are respected.

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

This proposal is consistent with existing rules governing the **processing of personal data** (including the General Data Protection Regulation, 'GDPR'[10]) and protecting the private life and the **confidentiality of communications**, including any (personal and non-personal) data stored in and accessed from terminal equipment ('ePrivacy Directive'[11], to be replaced by the ePrivacy Regulation which is currently in legislative negotiations). This proposal builds on existing rights with specific regard to data generated by a user's product connected to a publicly available electronic communications network.

The **Free Flow of Non-Personal Data Regulation**[12] implemented a key building block of the European data economy, by ensuring that non-personal data can be stored, processed and transferred anywhere in the EU. 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 'SWIPO' codes of conduct, developed by industry). The current proposal builds further on this basis, facilitating businesses and citizens to put that right to the best possible use, 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, the current proposal presents a regulatory approach to the problem highlighted in the Free Flow of Non-Personal Data Regulation.

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

---

10 OJ L 119, 4.5.2016, p. 1–88.
11 OJ L 201, 31.7.2002, p. 37–47
12 OJ L 303, 28.11.2018, p. 59–68; SWIPO (2021), see *website*.
13 OJ L 95, 21.4.1993, p. 29–34.

Obtenu par CONTEXTE

Competition law[14] is applicable in the context of amongst others merger control, data pooling by companies or an abuse of a firm's dominant position. The Horizontal Block Exemption Regulation provides for an exemption of Article 101 TFEU for agreements on sharing of know-how and other results of joint research and development between businesses if the conditions of the Regulation are met.

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

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

The **Open Data Directive**[17] sets out minimum rules governing the re-use of data held in the public sector and of publicly funded research data which has been made publicly available via repositories.

The **Interoperability Europe initiative** seeks to introduce a cooperative interoperability policy for a modernized public sector. The initiative evolved from the ISA^2, a now completed funding programme of the EU (2016-2021) that supported the development of digital solutions to enable interoperable cross-border and cross-sector public services[18].

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

The proposal leaves unaffected existing applicable rules in the areas of intellectual property (with the exception of the application of the sui generis right of the Database Directive), competition, justice, and home affairs and related (international) cooperation, trade-related obligations, and the legal protection of trade secrets.

As a horizontal proposal, the **Data Act** envisages common **basic rules for all sectors**, most of which are unregulated as regards rights to use data, such as in the areas of smart machinery and consumer goods. However, the rights and obligations on data access and use have also been regulated to various extents on the sectoral level. While the Data Act will not change any such existing legislation, future legislation should in principle be aligned with the horizontal principles of the Data Act. Convergence with the Data Act's horizontal rules should be

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.
19 COM/2020/767 final.
20 OJ L 186, 11.7.2019, p. 57–79.

Obtenu par CONTEXTE

assessed when sectoral instruments are reviewed. This proposal leaves room for vertical legislation to set more detailed rules addressing sector-specific regulatory objectives.

In view of existing sectoral legislation, with regard to the creation of the Green Deal data space, the review[21] of the **INSPIRE Directive**[22] will enable further open availability and re-use of geodata 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**[23] requires transmission system operators to provide data to regulators and for resource adequacy planning, while the EU **Electricity Directive**[24] 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**[25] opens up some types of payment transactional and account information under certain conditions, thus acting as an enabler for B2B data sharing in the area of Fintech. In the mobility and transport sector a wide variety of pre-existing data access and sharing rules exist. The repair and maintenance information from motor vehicles and agricultural machines is subject to specific data access/sharing obligations under **type approval legislation**[26]. In the framework of the **Intelligent Transport Systems Directive**[27], a number of 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 to improve inter-modality and connectivity. Operational real-time data related to air traffic management would come under the specific regime defined in the framework of the **Single European Sky**[28]. In vessel traffic monitoring, vessel related data (tracking and tracing) is important to improve inter-modality and connectivity: such data falls under the specific regime defined in the VTMIS Directive[29] and the High-level Steering Group for Governance of the Digital Maritime System and Services[30]. The proposal for a Regulation on the deployment of **alternative fuels infrastructure**[31] 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**

The 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[32], where the digitalisation of the Single Market is characterized by a high degree of trust, security, safety and choice for

21 GreenData4All initiative (REFIT) | Legislative train schedule | European Parliament (europa.eu)
22 OJ L 108, 25.4.2007, p. 1–14.
23 OJ L 158, 14.6.2019, p. 54–124.
24 OJ L 158, 14.6.2019, p. 125–199.
25 OJ L 337, 23.12.2015, p. 35–127.
26 OJ L 151, 14.6.2018, p. 1–218; OJ L 60, 2.3.2013, p. 1–51.
27 OJ L 207, 06.08.2010, p. 1-13.
28 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.
29 OJ L 308, 29.10.2014, p. 82–87.
30 OJ L 96, 12.4.2016, p. 46–49.
31 COM/2021/559 final
32 COM/2020/67 final.

Obtenu par CONTEXTE

consumers, as well as strong competitiveness based on a framework which promotes transparency, competition and innovation, and which is technology neutral. It supports the **Recovery and Resilience Facility**[33], learning lessons from the COVID-19 pandemic and the benefits of more easily accessible data where necessary.

It supports the critical role of data in achieving the European **Green Deal objectives** in boosting the understanding of governments, businesses and individuals of societal and environmental impacts of products, services and materials across entire supply chains, and in mobilising the existing wealth of relevant private sector data to address the climate, biodiversity, pollution[34] and natural resource challenges in-line with objectives of the European Green Deal[35] , relevant Council conclusions[36] and positions[37] of the European parliament , by closing knowledge gaps and for managing related crises through enhanced mitigation, preparedness, response and recovery actions.

In line with the **Industrial Strategy**[38], the proposal addresses highly strategic technologies such as cloud computing and artificial intelligence systems where the EU has unrealised potential at a time of the next industrial data wave. It implements the **Strategy for Data**[39] goal for businesses to be able better to innovate and compete based on EU values and the principle of **free flow of data within the internal market** and follows the **Intellectual Property Action Plan**[40] in which the Commission undertook to review the Database Directive.

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 complete a single market for data in which data from the public sector, businesses and individuals are put to the best possible use, while respecting rights in relation to such data and investments made into their collection. The provisions on switching between data processing services aims to establish fair and competitive market conditions for the single market in cloud, edge and related services.

Furthermore, protection of confidential business data and trade secrets is important to the well-functioning of the internal market, as it would also be 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 EU to benefit from the scale of the internal market, since connected products and related services are often developed using data from different Member States, and later commercialised across the EU.

---

33 OJ L 57, 18.2.2021, p. 17.
34 COM(2021) 400 final
35 COM/2019/640 final
36 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
37 Climate and environmental emergency - Thursday, 28 November 2019 (europa.eu)
38 COM/2021/350 final.
39 COM/2020/66 final.
40 COM/2020/760 final.

Ontenu par CONTEXTE

Moreover, 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 EU 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 several areas of impact of the Data Act, the issues tackled by this proposal cannot be effectively addressed at the Member State level. Fragmentation resulting from adoption of national rules should be avoided, as it would lead to increased transactional costs, lack of transparency, legal uncertainty, and undesirable forum shopping. Avoiding this is particularly important in all situations concerning data aspects of business-to-business relations, including fair contractual terms and obligations on manufacturers of IoT products and related services, where it is essential that the framework is homogeneous throughout the EU.

Similarly, an assessment of cross-border aspects of data flows in the area of business-to-government data sharing also demonstrates the need to act at EU level. Many private actors that have relevant data are multinational companies, and such companies should not be confronted with a fragmented legal regime.

Cloud computing services are rarely offered within one Member State only. In line with the rights established in the GDPR and the Free Flow of Non-Personal Data Regulation that enables EU 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 single market. It is therefore crucial that provisions on switching data processing services are applied at European level, to avoid harmful fragmentation in an otherwise unified market for data processing services.

Only common action at the EU 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 represents a confident step forward in the realisation of the vision to create a genuine single market for data.

- **Proportionality**

The initiative balances the rights and interests of affected stakeholders with the general objective to facilitate wider use of data for a broad range of actors. The proposed legislation 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 sets a framework for future sectoral rules to avoid fragmentation and legal uncertainty. It clarifies existing rights and where necessary provides access rights to data and helps to develop an internal market for data sharing. The initiative leaves a significant amount of flexibility for application at sector-specific level.

The proposed Regulation will give rise to financial and administrative costs, which are to be borne mainly by national authorities and manufacturers and service providers in order to ensure compliance with the obligations set in this Regulation. However, the exploration of different options and their expected costs and benefits led to a balanced design of the

Obtenu par CONTEXTE

instrument. Similarly, the costs to data users and holders will be counterbalanced by the value emanating from broader access and use of data, as well as the market uptake of novel services.

- **Choice of the instrument**

The Commission puts forward a proposal for a Regulation as the legal instrument because it is the best mechanism to serve the broader policy goals of ensuring all EU businesses are put in a position to innovate and compete, consumers are better able to take control of their data, and European bodies and institutions are better equipped to tackle major policy challenges, including public emergencies. A Regulation is necessary 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 and responsibilities, to ensure consistent enforcement in all Member States as well as effective cooperation between the supervisory authorities of different Member States.

The proposal will strengthen the single market for data by increasing legal certainty and guaranteeing a fully 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[41]. The Database Directive introduced among other things a specific *sui generis* right for 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[42]. The evaluations have been supplemented with Commission's communications on policy for the data economy[43].

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 to protect the investments in the collection, not the creation of data[44] 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 means of physical components, such as sensors, of a connected product or a related service to such products. There is a need to balance the policy objectives of IP protection of such databases in the context of the data economy, where exclusivity of data as non-rival good is in general considered an impediment to innovation. To ensure consistency with the regulatory interventions proposed by this legislative proposal, the intervention on the sui generis right specifically addresses the identified problematic application of the *sui generis* right's in the IoT context. In addition, the Commission is currently preparing the evaluation of Regulation

[41] 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.

[42] European Commission (2005), First evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 146 final, section 5.4.2.

[43] COM/2017/09 final; COM/2020/66 final; COM/2020/760 final.

[44] 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)

Obtenu par CONTEXTE

2018/1807, which is 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 already during the past Commission mandate to identify the problems that are currently preventing Europe 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 on "Building a European data economy"[45], 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 the B2B data sharing principles and guidance and the Commission online open consultation on the Data Strategy[46] that ran from February to May 2020.

An Inception Impact Assessment was published on the Better Regulation portal on 28 May 2021 and was open for feedback for 4 weeks. The Commission received 91 contributions on the Better Regulation Portal[47], essentially from businesses.

A public online consultation on the Data Act was subsequently published on 3 June 2021 and 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 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 – protection of databases and safeguards for non-personal data in international context. After carrying out an in-depth analysis of the replies, the Commission published a summary report on its website[48].

In total, 449 contributions were received from 32 countries. Business entities constituted the largest share, comprising 122 business associations and 105 companies/ business organisations. In addition, 100 respondents were public authorities and 58 were citizens. Generally, the responses confirmed that there is an array 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 that experienced difficulties identified obstacles such as those of technical nature (formats, lack of standards – 69% of respondents), outright refusal to grant access not linked to competition concerns (55%) or abuse of contractual imbalance (44%). On contractual issues, almost half of respondents supported an unfairness test (46%), more than double of those not in favour (21%). While SMEs showed strong support (50%), a significant number of large companies were also in favour (41%). Similarly 46% of the stakeholders across sectors showed support for general access rules based on fair, reasonable and non-discriminatory terms (46%). 60% of the respondents, SMEs and micro companies in particular (78%), agreed that model contract terms could contribute to increased data sharing. Importantly, 70% of stakeholders expressed the opinion that there is a fairness problem with data generated from the Internet of Things (IoT), and that manufacturers of connected products and related services should not be able to decide unilaterally on what happens to the

[45] COM/2017/09 final.

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

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

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

Obtenu par CONTEXTE

data generated by such products. Some 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 IoT data.

Legal uncertainty and barriers, commercial disincentive, and lack of appropriate infrastructure were amongst the main factors impeding B2G data sharing identified by respondents. Almost all public authorities consider that action (EU or national) on business-to-government is needed, as compared to 80% of academic/ research institutions and 38% of company/ business organisations/ associations. Moreover, a clear majority of stakeholders (in particular citizens and public administrations) 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 the domains of emergencies and crisis management, for official statistics, for protecting the environment and for a healthier society.

Respondents also confirmed the usefulness of a right to switchability for business users of cloud computing services. Finally, as regards the 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 this 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 B2B and B2G data sharing, and a final validation workshop organised in spring 2021.

Study on **model contract 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**. It included an online survey on a representative sample of SMEs and start-ups using cloud computing for conducting their business.

Study on the **switching of cloud service providers**, which included a cross-sectorial workshop in Q2 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 their interlinked objectives.

Methodological support to impact assessment of using privately **held data by official statistics**. This exercise provides input to the ongoing research and deliberations towards a better understanding of B2G 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 on business-to-government data sharing in the

Obtenu par CONTEXTE

EU and offers a set of recommendations in order to ensure scalable, responsible and sustainable business-to-government data sharing for the public interest. In addition to the recommendation to the Commission to explore a legal framework in this area, it presents several ways to encourage private companies to share their data. These include both 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. It was discussed how the organisation of the **data sharing in certain areas** such as environment, agriculture, energy or health could benefit the 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 Staff Working Document of 25 April 2018[49].

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

The **Opinion of the European Data Protection Supervisor** (EDPS) on the European strategy for data[50]. 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[51], which was 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 products and services, the legislative proposal will ensure that the sui generis right will not interfere with the provided access right mechanism for business and consumers. The clarification will align the

[49] COM(2018)232 final; SWD(2018)125 final of 25.4.2018.

[50] EDPS Opinion 3/2020 on the European Strategy for Data.

[51] **[Links to final document and to the summary sheet to be added.]**

Obtenu par CONTEXTE

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 single market and for the data economy.

By facilitating data access and use, the Data Act should reduce burden mainly as a result of lowering transaction costs and by inducing efficiency gains, both in the public sector and among businesses.

- **Fundamental rights**

The proposal is in full compliance with the EU legislation on the protection of personal data and foresees additional safeguards where access to personal data can be concerned as well as 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 EU 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 IoT object. The owner may benefit from an improved use experience and a wider range of e.g. repair and maintenance services.

The IoT data access right for third parties upon the user's request limits the freedom to conduct a business and freedom of contract of the manufacturer or designer of a product or related service. The limitation is justified to enhance consumer protection, in particular to promote consumer's economic interests. Consumers using products and related services are further empowered to meaningfully control how the data generated by their use of the product and related service is used. Consumers can therefore benefit from a wider choice in aftermarket services, such as repair and maintenance, and do no longer depend on only the manufacturer's services. The provision facilitates the portability of the user's data to third parties and thereby allows for a competitive offer of aftermarket services. The limitation of the manufacturer's or designer's freedom to contract and to conduct a business is proportionate as the impact is mitigated by the unaffected ability of the manufacturer or designer to also use the data, and 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 restricted use of the data by the third party.

In Chapter IV, a fair and effective system of protection against unfair contractual clauses in data sharing will contribute to micro, small and medium enterprises ability to conduct a business. The 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 party on a micro, small and medium enterprise. This is justified as SMEs are archetypically in a weaker bargaining position and often left with no other choice than to accept 'take it or leave it' contract terms. The contractual freedom largely remains unaffected as only excessive and abusive clauses are invalidated, and the concluded contract, if possible, remains valid without the unfair clauses. Furthermore, the parties can still individually negotiate a specific contract term.[52]

In Chapter VI, the provisions on switching of data processing providers enhances the position of the business customers and 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 on the cloud and edge market and improve the choice for business users and

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

Obtenu par CONTEXTE

individuals of data processing services.

In Chapter X, the amendment 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. The amendment clarifies that there is no intellectual effort involved in the machine-generated creation of data e.g. through the use of sensors.

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 EU.

The impact on SMEs, namely their perception of problems related to data access and use, will be assessed with a 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 EU Data Strategy, 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 for the assessment of 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 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 and related services which they own or lease. Manufacturers and designers have to design the products in a way that the data is easily accessible by default, and they would have to be transparent on what data will be accessible and how to access them. Provisions in 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 upon the request of the user to third parties. Users would be entitled to authorise the data holder to give access to the data to third party service providers, such as providers of aftermarket services. Small and micro enterprises would 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 another enterprise as in Chapter II or in other Union or national legislation, the general framework addresses the compensation when making data available and conditions for making data available. Any conditions would have to be fair and non-discriminatory, and any compensation must be reasonable. Any compensation set for SMEs cannot exceed the costs incurred for making the data available,

Obtenu par CONTEXTE

unless otherwise specified in sectoral legislations. Dispute settlement bodies certified by the Member States assist parties that disagree on the compensation or other conditions to find an agreement.

Chapter IV addresses unfairness of contractual terms in data sharing between businesses, in situations where a contract term is unilaterally imposed by one party on a micro, small and medium enterprise. The 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 that includes a general provision defining unfairness of a data sharing-related contract term complemented by a list of clauses that are either always unfair or presumed to be unfair. In situations of unequal bargaining power it 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.[53]

Chapter V creates a harmonised framework for the use by public sector bodies and Union institutions, bodies and agencies of data held by enterprises in certain situations where there is an exceptional data need. The framework is based on an obligation to provide data and would only apply in the case of public emergencies and in situations where public sector bodies have an exceptional need to use certain data that cannot be obtained in a timely manner through enacting new legislation, by means of existing reporting obligations or on the market. In case of emergencies, such as pandemics and disasters, data would be made available for free. For other exceptional data needs, the enterprises providing the data should be entitled to compensation which include costs related to making the relevant data available plus 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 to 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.

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, it should be ensured 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, but requires that services are compatible with open standards or interfaces where these exist.

Chapter VII provides for the adoption of implementing acts to adopt common specifications to potentially address the lack of harmonized standards that provide for to improve interoperability and compliance with the essential requirements for the use of smart contracts.

Chapter VIII addresses concerns about potentially unlawful third party access to data processing services offered on the EU market. This Regulation does not affect the legal basis of data access requests made to data held by EU citizens or businesses and would be without prejudice to the EU'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 could potentially conflict with competing obligations to protect such

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

Obtenu par CONTEXTE

data under EU law, unless strict conditions are met. The Regulation complies with the EU's international commitments in the WTO and in bilateral trade agreements.

Chapter IX lays down the implementation and enforcement framework with competent authorities in each Member State. A complaints mechanism regarding the right in Article 4 covers the enforcement. The Commission shall recommend voluntary model contract terms on data access and use. Penalties shall apply for infringements of this Regulation.

Chapter X contains a provision for the review of Directive 1996/9/EC to exclude databases containing machine-generated data from the protection of *sui generis* right established therein.

Chapter XI allows the Commission to, under Article 37, adopt delegated acts to introduce a monitoring mechanism on switching charges imposed on the data processing service providers' market in Article 25(4), adopt common specifications under Article 28(1), mandate the use of open standards, open interfaces and common specifications under Article 28(2) and adopt common specifications with regard to smart contracts under Article 29(6). Article 38 clarifies the relation to other Union legal acts governing data sharing rights and obligations.

Obtenu par CONTEXTE

Obtenu par CONTEXTE

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ensuring fairness in the allocation of value across the data economy (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[54],

Having regard to the opinion of the Committee of the Regions[55],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) A balanced allocation of the value created from data is essential to create a competitive and fair Internal Market. It supports the green and digital transformations of the economy and society, in particular in the wake of the COVID-19 pandemic and its damaging impact on vulnerable individuals and small businesses. Competitiveness, innovation and sustainable growth in all sectors of the EU economy require high-quality and interoperable data from different domains. The same dataset may potentially be used and reused for a variety of purposes to an unlimited degree, without any loss in its quality or quantity, creating new knowledge, enabling the emergence of innovative business models and services, and where necessary to support climate, health and environmental policy objectives and actions, including responding in general to natural or emergencies, including pandemics.

In recent years, data-driven technologies have had transformative effects on all sectors of the economy. The Union aims to support the development of adequate governance frameworks and infrastructures for European businesses and public bodies to share data in a lawful manner. Barriers to data sharing include lack of incentives for data holders to enter voluntary sharing agreements, uncertainty about rights and obligations, costs of contracts 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 the data access, a lack of common data sharing practice and abuse of contractual imbalances with regards to data access and use. Contracts for purchase or leasing of machinery or devices and related services may not provide the basis for data sharing. In sectors characterised by the presence of microenterprises and SMEs, there is often a lack of

[54] OJ C , , p. .

[55] OJ C , , p. .

Obtenu par CONTEXTE

digital capacities and skills to collect, analyse and use data, and access is frequently restricted where it is held by one actor in the system or due to a lack of interoperability between data, data services or across borders.

In order to respond to the needs of the digital economy and in particular to address the barriers to a well-functioning data economy, it is necessary to develop the existing legal framework. Creating such a harmonised framework will contribute to making the Union's transition to a green digital economy a success and to stimulating overall sustainable growth.

The proliferation in products and related services connected to the Internet of Things has significantly increased the volume and potential value of data for businesses, consumers and society. Such products are equipped with sensors, cameras, microphones, gyroscopes, radar, lidar and similar modules to record data on the functioning of the product and its components, how it is used and potentially also on the environment in which it operates. Such data generation is the result of the actions of at least two actors, namely the designer and/or manufacturer and the user of the product. It is necessary to clarify who is entitled to use data generated by such objects and on what basis. It also gives rise to questions of fairness in the digital economy as the data recorded by such products and related services are an important input for aftermarket, ancillary and other services. In practice, not all data generated by users' products and related services are easily accessible to them, and there are limited possibilities for the portability of data generated by consumer Internet of Things devices. 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, original equipment manufacturers *de facto* are often able to determine, through their control of the technical design of the product and related services, what data are generated and how they can be accessed, even though they have no *de jure* right under applicable statutory rules. In order to realise the important economic benefits of data as a non-rival good for the economy and society, in general an approach of assigning access and usage rights on data is preferable to awarding exclusive rights of access and use.

Legislative adaptations for promoting the digital transition are also required in several areas. Entities that hold data in any sector of the Internal Market and that are under legal obligations, such currently exist in the areas of banking, vehicles and electricity, to make data available to other enterprises should be able to rely on consistent rules regarding conditions and compensation. 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[56]. 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. In the interests of society and the environment generally, businesses and public sector bodies require a proportionate and predictable mechanism for data held by businesses to be used in emergencies and other exceptional situations. Businesses should be able easily to 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 require an interoperability framework of procedural, legislative and

[56] Ref: Sustainable Product Initiative

Obtenu par CONTEXTE

measures to enhance trust and improve efficiency. The creation of common European data spaces for strategic sectors of the economy and domains of public interest, should 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. A Regulation is necessary in order to ensure legal certainty and transparency for economic operators, including micro-, small- and medium-sized enterprises, to provide legal and natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities, and to ensure consistent enforcement in all Member States as well as effective cooperation between the supervisory authorities of different Member States.

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, in particular Regulation (EU) 2016/679. 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.

Overall, sharing value from processing of data, whether or not personal, does not always necessitate the transmission of raw or structured data themselves between parties. In accordance with, *inter alia*, the principle of data minimisation, the EU and its Member States should encourage the use of the technical means that are increasingly available and permit algorithms to be brought to the data to allow valuable insights.

This Regulation provides for unified access rules applicable to users, and to third parties at the request of users, of data generated by the use of a product or related service, and fully harmonises the rules for the prevention of exploitation of contractual imbalances that hinder fair data access and use between businesses, to the making available of data held by private entities to public sector bodies in exceptional situations, to facilitating switching between data processing services and to enhancing the interoperability of data and data sharing mechanisms and services. 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 the fully harmonised rules applicable to the data holders in accordance with the objectives of this Regulation.

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 the health, safety and economic interests, in particular Directive 2005/29/EC of the European Parliament and of the Council[57], Directive 2011/83/EU of the European Parliament and of the Council[58] and Directive 93/13/EEC of the European Parliament

[57] 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').

[58] 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

Obtenu par CONTEXTE

and of the Council, as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council[59].

This Regulation is without prejudice to existing and future Union law setting physical design and data requirements for products to be placed on the European Union market.

This Regulation is without prejudice to Union legal acts and 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 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.

This Regulation should apply to physical, movable products that obtain, generate or collect, by means of their physical 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 collectively as the 'Internet of Things'). 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 events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered as necessarily 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.

This Regulation should not apply to those physical products that generate data as result of intentional human input to display or play content, or to record and transmit content, typically for the use by an online service. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.

This Regulation should apply to a connected product that incorporates or is interconnected with a service in such a way that the absence of the service would prevent the product

---

Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[59] 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.

Obtenu par CONTEXTE

from performing its functions. Such related services are likely to be set out in the sales, rental or lease agreement between the seller and the user, or they 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. For example, a "smart" speaker or TV set may include a standardised pre-installed voice command, or an e-Bike may require connection to a mobile app to ensure its full functionality. These 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 sales, rental or lease contract, this Regulation should apply, including in the case of virtual assistants.

Data generated by the use of a product or related service include data recorded intentionally by the user, such as when taking measurements. Such data include also data generated as a by-product of the user's action, such as diagnostics data on the performance of the product, and without any action by the user, such as when the product is in 'standby mode', data recorded by a voice assistant before its activation by the wake word, and data recorded on a backend server of the manufacturer or elsewhere during periods when the product is entirely switched off. Such data should include data in the form and format in which they are generated by the device, 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.

The user of a product should, under this Regulation, be understood as the legal or natural person, such as a business or consumer, which has purchased, rented or leased the product. Such a user accordingly bears the risks and enjoys the benefits of using the connected product. The user should therefore be entitled to derive benefit from data generated by that product and any related service. This should include cases of short-term rental of vehicles or equipment whose use generates substantial amounts of data that enable the business to ascertain the efficiency or effectiveness of its activities, for example in digital farming. When considering a lease as 'short-term', account should be taken of several factors, namely the duration but also the relevance of the data for that specific user.

In case several persons or entities have ownership titles over a product or are party to a lease or rental 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. This relates for instance to situations of joint ownership or lease of an object or to situations where the owner or lessee is permitted to sub-lease the object. In order to ascertain what efforts are reasonable, account shall be made of the following factors: the relative strength of the title permitting lawful use (e.g. ownership vs right to use under a sub-lease or similar arrangement), the economic risks borne by the parties in relation to the deterioration of the product, the duration of the title permitting the lawful use (short-term rental vs. long-term lease) and the right of the user in obtaining access to the specific data in question, in particular where such data are user's personal data. Reasonable efforts may include, e.g. the design of relevant user accounts, interfaces or companion apps in a manner for several users to jointly use one account or to permit separate user

Obtenu par CONTEXE

accounts linking relevant data to individual users, including short term users. Users of objects with digital functionalities typically require a user account to be set up. This allows for identification of the user(s) by the manufacturer as well as a means to communicate in view of exercising and processing the data access request. Manufacturers of objects that are typically used by several persons, e.g. members of the same household should put in place the necessary functionalities that allow separate user accounts for individual persons, where relevant, or the possibility for several persons to use the same user account.

Personal data may only be requested by a controller or a data subject. Accordingly, where the user is an enterprise, including a sole trader, intending to request personal data generated by a product or related service, the user is considered to be a controller within the meaning of Regulation (EU) 2016/679 and is required to have a legal basis for processing the data under Article 6(1) of that Regulation, such as the consent of the data subject or legitimate interest. Where the user is the data subject, the user is already entitled under Regulation (EU) 2016/679 to access personal data concerning the user, and such rights are unaffected by this Regulation. It should be understood that the user, once data has been made available, may in turn become a data holder. The data holder should be understood as the enterprise with the right, or the obligation under this Regulation or other Union or national laws, or, to the extent non-personal data are concerned, the ability, to make data available. The data holder can only be an enterprise that is a controller under Regulation (EU) 2016/679. The present Regulation confers the obligation on the data holder to make data available in certain circumstances. This Regulation does not create a legal basis under Regulation (EU) 2016/679 for the data holder to provide access to personal data when requested by a user that is not a data subject.

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 generated when a user interacts with a product via a virtual assistant provided by entities other than the manufacturer of a product connected to the internet-of-things.

Connected products and related services should be manufactured or designed in such a way that the data generated by the use of a product or related service is easily accessible to the user, including continuously, directly, and in real-time. The manufacturer or service provider should make all reasonable efforts to ensure, through the design of the access request process, that the user can easily access the data irrespective of which legal entity has technical control over the remote server. 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.

Before the conclusion of the contract for the purchase, rent, or lease of the product or the provision of the related service, the enterprise, prior to placing the product on the market for purchase, rent or lease, or a provider of a related service should provide

Obtenu par CONTEXTE

clear and sufficient information on how the data generated may be accessed. This may be provided through the user's account page on a website or the mobile application for registering the product and managing its functionalities, so that it is clear to the user what data are likely to be generated, and how they can be accessed. The identity and contact details of the data holder, who may not be the original manufacturer of the product, should also be provided. In order for third parties to be able to propose relevant services, such information should also be available to the general public.

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. The server may be the manufacturer's own local server capacity or that of a third party or a cloud service provider. They may be designed to permit the user or a third party to process the data on the device or on a computing instance of the manufacturer. However, the product should not be designed to permit the manufacturer, or its subsidiary, sister company or parent company, or other entity acting on behalf of the foregoing, to monitor the activities of the user or third party, such as when or how often the data accessed or processed. Such monitoring could, inter alia, give the manufacturer an unfair competitive advantage.

Users, including consumers and business customers, who have purchased, rented or leased a product or related service should be able to access easily data generated from their use of the product or related service.

The use of a product or related service may, in particular when the user is a consumer, generate data which relates to an identified or identifiable natural person (the data subject). Processing of such data is subject to the rights and obligations under Regulation (EU) 2016/679, including where personal and non-personal data in a data set are inextricably linked[60]. The data subject may be the user and/or another natural person. A user under this Regulation who is a natural person, is entitled to access all data generated by the product, personal and non-personal. Where the user is not the data subject, the data subject should be provided with necessary information including the identity of the controller. Where the user is not the data subject, in most circumstances the user would then be the controller and 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 under the Regulation (EU) 2016/679. The data made available should only be processed by the user on the basis of a valid legal basis under Article 6(1) of Regulation (EU) 2016/679. 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. Access in these circumstances to any data stored in and accessed from terminal equipment is subject to Directive 2002/58/EC and requires the explicit consent of the subscriber or user within the meaning of that Directive.

This Regulation aims to create favourable conditions for, in particular, small businesses and start-ups offering innovative and sustainable data-based solutions in all sectors of the economy, achieving a better balance between the rights of users and preserving the incentives for manufacturers to invest in high quality data generating products. This is particularly necessary in sectors such as agriculture, where the concentration of a small number of companies supplying machinery has severely limited the options available

[60] OJ L 303, 28.11.2018, p. 59–68.

Obtenu par CONTEXTE

to farmers and other small businesses wishing to derive insights and value from the data generated by their equipment they purchase or lease. In such circumstances, contractual agreements are often insufficient to achieve the objective of user empowerment, with the data tending to remain under the control of the same suppliers, and consequently limited incentive for smaller players to participate in common data spaces. This Regulation should therefore build on positive recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement. This Regulation should not therefore be interpreted as conferring any new entitlement on the data holder to use data generated by the use of a product. The basis for the data holder to use data should be an agreement between the data holder and the user. This agreement on the use of the data generated may be contained in the sales, rental or lease contract pertaining to the product. This Regulation does not, prevent the data holder from proposing contractual conditions relating to the purchase, rental or lease of the product, whose effect is to allow the data holder itself also to access and use the data. Any such condition should be transparent to the user including with regards to the purpose of the data use by the data holder. In consumer contracts, Directive 93/13/EEC of the European Parliament and of the Council, as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council[61] applies to ensure that a consumer is not subject to unfair contract terms. For unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise within the meaning of Commission Recommendation 2003/361/EC[62] this Regulation foresees that such unfair terms shall not be binding on that enterprise. 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.

The user should not abuse the access right to exploit any vulnerabilities in the data access interface or to gain access data to which the user is not entitled. The user should also respect any trade secrets or intellectual property rights in handling the data. The user should not use the data to develop a product that competes with the product that generated the data or share the data with a third party for that purpose.

Where the use of a product or related service generates data valuable to its user, the user should not be locked into the processing environment of any single provider of aftermarket or other services, but should also be able to choose which third parties may use such data in order to maintain or repair the product or provide another data-based service. Such a third party may be an enterprise, a research organisation or a not-for-profit organisation.

This Regulation accordingly builds on the right provided under Article 20 of Regulation (EU) 2016/679. Article 20 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)(a) or Article 9(2)(a) or on a contract pursuant to Article 6(1)(b). Data subjects also have the right to have the personal data transmitted directly from one

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

Obtenu par CONTEXTE

controller to another, but only where technically feasible. Article 20 of Regulation (EU) 2016/679 specifies that it pertains to data "provided" by the data subject but does not specify whether this necessitates an active behaviour on the side of the data subject or whether it also applies to situations where a service or device 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 thus complements the right to receive and port personal data under Article 20 of Regulation (EU) 2016/679 in several ways. It extends to any data generated by 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. Furthermore, it goes beyond the technical obligations provided for in Article 20 of Regulation (EU) 2016/679 by mandating an ensuring the technical feasibility of third party access. It also allows the data holder to set reasonable compensation to be met by third parties, but not from the user, for any cost incurred in providing direct access to the data generated by the user's product. In the event that 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, including the right to data portability, by seeking remedies in accordance with that Regulation.

Third party access to data generated by a product or related service should be in accordance with applicable rules on data protection and on the confidentiality of communications. Having received data, the third party should process the data exclusively for the purposes agreed with the user, without interference from the data holder.

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 [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 obligation 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 [Digital Markets Act], and given the unrivalled ability of these companies to acquire data, it would be unnecessary and disproportionate to include them within the scope of the third parties to whom a user might, under this Regulation, direct a data holder to provide data generated by the user's product or related service. This means that an undertaking providing core platform services cannot request or be granted access to users' data generated by an IoT object 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. The third party may not, for instance, sub-contract the service provision to a 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. This does not, however prevent third parties from using data processing services offered by a designated gatekeeper.

Obtenu par CONTEXTE

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. 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. 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 which 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 of the European Parliament and of the Council, Directive 2011/83/EU of the European Parliament and of the Council, Directive 2000/31/EC of the European Parliament and of the Council and Directive 98/6/EC of the European Parliament and of the Council.

To prevent distortions and exploitation consumers and enterprises, certain restrictions on use are necessary. The third party should only process the data for the purposes agreed with the user and share it with another party only if this is necessary to provide the service requested by the user. Furthermore, the third party should refrain from using the data in order to compete with the enterprise obliged to make the data available by developing products that compete with those from which the data obtained under the data access right originate. 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, which may include personalised services.

At the current state of technology it would be overly burdensome to impose further design obligations on micro- and small enterprises. This exemption should not apply where a micro- or small enterprise is a sub-contractor to manufacturer of the product. In such a situation, the manufacturer of the product is deemed able to compensate appropriate the sub-contractor. The data holder may, however, be a micro- or small enterprise where it is not the manufacturer of the product.

This Regulation contains general access rules 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 statutory data access right is established, whenever a data holder is obliged by law to make data available to a data recipient. These general access rules should apply where a data holder is obliged to make data available to a third party under Chapter II or under data access rights established in future legislation. Voluntary data sharing remains unaffected by these rules. While specific legislation should identify the situations where a data holder should be obliged to make data available to another enterprise and establish, where necessary, such data access rights, the conditions for such data access as laid down in this Chapter should apply.

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 rules for making data available.

Obtenu par CONTEXTE

In order to ensure that the conditions for mandatory data access are fair for both parties, the general rules on data access rights established under this Regulation or in subsequent sector-specific legislation should refer to the rules in this Regulation on avoiding unfair contract terms.

Contract terms implementing the data access rights established under this Regulation or in subsequent sector-specific legislation should not discriminate between comparable categories of enterprises to which the data is made available. The data holder may use different contract conditions for different enterprises only if there is an objective reason.

Transparency is an important principle to ensure that the conditions for data access rights established under this Regulation or in subsequent sector-specific legislation are reasonable and non-discriminatory. It is therefore necessary to put the enterprises to which the data is made available in a position to assess if a reasonable compensation is agreed and conditions for making data available are non-discriminatory.

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 and non-discriminatory compensation when legally obliged to make data available to another enterprise. These provisions should not be understood as paying for the data itself, but rather for the costs incurred and investment required for collecting and making the data available.

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 met by them shall not exceed the direct cost of making the data available.

Direct costs for making data available are costs necessary for data reproduction, dissemination via electronic means and storage but not of data collection or production. The dissemination costs also include the costs of setting up and maintenance of the necessary infrastructure, e.g. technical interfaces and of related software as well as connectivity, within the limits of what is necessary to make data available for access and use. The compensation should be limited to the share attributable to the individual requests, taking into account that the necessary infrastructure, 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 other enterprises, 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.

It is not necessary to intervene in the case of data sharing between large companies, or when the data holder is an SME and the data recipient is a large company. In such cases, large companies are considered capable of negotiating any compensation provided that it is reasonable, taking into account factors such as prevailing market conditions and reasonable return on investment for collecting the data.

Where a data holder requests such compensation, it is obliged to request such compensation also from partner enterprises or linked enterprises (within the meaning of Commission Recommendation 2003/361/EC) in order comply with the non-discrimination obligation under this Regulation, or – where the data holder itself is active on secondary markets developing products or offering services on the basis of data concerned by the obligation under this Regulation – is obliged to ensure non-discrimination through other means.

Obtenu par CONTEXTE

All the components of the full amount of compensation should be calculated in accordance with the accounting principles applicable to the data holder.

Such general rules on conditions and compensation that apply where a data holder is obliged by law to make data available to another enterprise should ensure consistency and legal certainty for businesses across the Internal Market. These rules should apply where the data holder is required to make data available to a third party at the request of the user under this Regulation as well as under future EU legal instruments, governing business to business data access in specific sectors and for specific products or product groups. They do not apply to obligations to make data available under Regulation (EU) 2016/679.

Ensuring access to alternative ways of resolving domestic and cross-border disputes which 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 fair, reasonable and non-discriminatory terms of making data available dispute settlement bodies offer a simple, fast and low-cost solution to the parties.

To avoid that two or more dispute settlement bodies are seized of the same dispute, particularly in a cross-border setting, a dispute settlement body should be able to reject to 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.

The right to an effective remedy and the right to a fair trial are fundamental rights laid down in Article 47 of the Charter of Fundamental Rights of the European Union. This Regulation should not prevent parties from exercising their right of access to the judicial system. Therefore, submitting their disputes to the dispute settlement body should not deprive the parties of their rights to seek redress before the courts when cases of a lack of agreement or disputes could not be solved by the dispute settlement body. The competent court should be determined in accordance with applicable law, in particular Regulation (EU) 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters[63].

Where one party is in a stronger bargaining position, there is a risk that this party excessively abuses such a position to the detriment of the other contractual party when negotiating contracts. The resulting unfair contract terms particularly harm micro, small and medium-sized businesses 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 for micro, small or medium-sized enterprises when they have been unilaterally imposed on them. Where unfair contract terms in data sharing agreements put an unfair burden on an innovative start-up or small company and make access to data commercially less viable and sometimes economically prohibitive, they restrict the ability of these parties to develop or run innovative digital business models. Preventing such effects promotes innovation and ensures a fair allocation of value creation in the data economy.

Rules on unfair contract terms acknowledge the principle of contractual freedom as an essential concept in business-to-business relationships. Therefore an unfairness test should not apply to all contract terms, but only to those contract terms which are not

[63] Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

Obiectiu pat CONFIDENTIAL

individually negotiated but unilaterally-imposed on micro, small and medium sized enterprises within the meaning of Commission Recommendation 2003/361/EC. This concern 'take-it-or-leave-it' situations where one party supplied a certain contract term and the micro, small and medium sized enterprise could not influence it despite the attempt to challenge it. A contract term that is simply provided by one party and accepted by the micro, small and medium sized enterprise or a term which is negotiated and subsequently agreed in an amended way between contractual parties should not be considered as unilaterally imposed.

Furthermore, the rules on unfair contract terms included in this Regulation should only apply to those elements of a contract which are related to making data available, i.e. contract 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 not related to making data available would not be subject to the rules on unfair contract terms.

An unfairness test aims only at those excessive clauses, where a stronger bargaining position is abused. The very large majority of contractual clauses, including those which are normal in business-to-business contracts, because they are simply commercially more favourable to one party than to the other, are a normal expression of the principle of contractual freedom and shall continue to apply.

If a contract term in question is not included in the list of clauses that are always unfair or that are presumed to be unfair, courts will apply and interpret as a safety net the benchmark of the general unfairness clause and decide if a specific contract term is unfair. In this regard, the clauses enumerated in the lists of unfair clauses serve as a useful yardstick to interpret the general clause. In the same vein, default rules of the applicable national contract law may also serve as a point of reference giving an indication if a contract term is not unfair. Finally, model contract 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. Voluntary data sharing through contracts should also be subject to applicable rules on personal data protection.

In situations of exceptional need, it may be necessary for public sector bodies, Union institutions, agencies or bodies to use data held by an enterprise to respond to public emergencies and where the unavailability of data make the fulfilment of their legal obligations impossible. In such cases, the public good resulting from the use of the data outweighs the interests of the data holders to freely dispose of the data they hold. Such data holders should therefore be under an obligation to make the data available to the public sector body, Union institution, agency or body upon their request. The burden on businesses should nevertheless be minimised, with small and micro-enterprises exempt from obligations to make data available.

In establishing the existence of a public emergency, the public sector body or Union institution, agency or body should carefully assess and justify the existence of all elements of the definition provided for in article 2 of this Regulation. As regards the existence of exceptional needs justified on grounds other than public emergency, the public sector body or Union institution, agency or body should demonstrate that the lack of access to and the use of such data effectively prevents them from fulfilling their legal obligations. At the same time, the request on grounds other than the necessity to address a public emergency should make evident that no alternative means for the obtaining of the relevant data exist and that the data cannot be obtained in a timely manner through the laying down of the necessary data provision obligations in

Obtenu par CONTEXTE

legislation. This covers situations where the existence of a reporting obligation for the provision of the data in scope of the request exists but is in itself insufficient to guarantee the availability of data of the necessary quality, granularity, and timeliness or where the said obligation is otherwise not fit for the specific use purpose sought. It also refers to situations where the body requesting the data cannot avail itself of the data through purchase on the market or procurement. The existence of an exceptional need will also be justified if the public sector body or Union institution, agency or body demonstrates that it is prevented from fulfilling its legal obligations due to the lack of relevant data and it can also prove that obtaining such data under this regulation will result in a considerable reduction of burden for enterprises in comparison to existing data provision mechanisms.

This regulation addresses situations where mandatory data access and use is justified by exceptional needs and where data requests have to be issued on an ad-hoc basis. It does not apply to voluntary arrangements for the exchange of data between private and public entities. It is also without prejudice to obligations to provide data by enterprises motivated by needs of 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 is the case with reporting obligations and single market obligations. It is without prejudice to requirements to access data to verify compliance with applicable rules.

This Regulation should not apply to the tasks of public authorities within which the obligation to provide data is already subject to separate safeguards and specific procedures. This specifically refers to the 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. For the exercise of their tasks in the public interest in those areas, public sector bodies should rely on their powers under sectoral legislation, and not the provisions of this Regulation. This Regulation accordingly does not affect the existing or future instruments for the sharing, access and use of data in those areas.

A proportionate, limited and predictable framework at EU level is necessary both to provide legal certainty to public sector bodies and enterprises and to minimise administrative burdens on the latter. To this end, the data requests addressed to the enterprise should be transparent and proportionate in terms of scope of content and its granularity. The purpose of using the data, and how it serves the objectives of applicable EU law, should be specific and clearly explained, while allowing appropriate flexibility for the public sector body to perform its tasks in the public interest. The requests should also respect the legitimate interests of the data holders. The burden on businesses should be minimised, with small and micro enterprises, in principle, exempt from obligations to make data available, and public bodies obliged to respect the once-only principle to prevent the same data being requested more than once by more than one public body where data is needed to respond to a public emergency. Finally, they should be transparent to the general public. The requests should therefore be made public without undue delay by the entity requesting the data. In addition, online public availability of all requests justified by public emergency should be ensured by the competent authorities described in Chapter IX.

In order to reduce the costs of making the data available by the enterprises and to promote common practices for data sharing between the private and the public sector, including voluntary arrangements, the Commission may issue non-binding guidance specifying the technical arrangements for making the data available. Such guidance may include requirements for data and metadata interoperability, pseudonymisation and

Obtenu par CONTEXTE

anonymisation techniques or methods of data transmission such as application programming interfaces.

The objective of the obligation to provide the data is to ensure that public sector bodies have the knowledge necessary to respond to public emergencies or to maintain the capacity to fulfil their legal obligations. It does not require the data obtained by them to be made public or to constitute a basis for value-added services. Indeed, such data may be commercially sensitive. Therefore, Directive (EU) 2019/1024 (Open Data Directive) should not apply to data made available under the provisions of the Data Act and should not be considered as open data available for reuse by third parties. This however should not affect the applicability of the Open Data Directive to the reuse of official statistics for the production of which data obtained pursuant to the Data Act was used, provided the re-use does not include the underlying data. In addition, it should not affect the possibility of sharing the data for the purpose of conducting research, provided the conditions laid down in article 21 of this regulation are met.

As a principle, public sector bodies or Union institutions, agencies and bodies should be allowed to immediately use data, free of charge, when they are necessary to respond to public emergencies. Where the data holders have a justified reason not to make the requested data available immediately, they should have a possibility to either ask for a modification of the request or its cancellation in a timeframe of 5 or 15 working days depending on the nature of the exceptional need invoked by the requestor. A justification will be valid when the addressee of the request does not hold the requested data, when the request is disproportionate or otherwise non-compliant with the conditions for requests in Article 17. In case of requests motivated by public emergency, a justification will also be valid if it can be shown that the request is similar or identical to a previously submitted request for the same purpose by another public sector body or Union institution agency or body. A data holder rejecting the request or asking for its modification should communicate the underlying justification needs to the public sector body requesting the data.

Data made available should, insofar as possible, be anonymous. Therefore, in complying with a request, enterprises should apply the test of identifiability outlined in Recital 26 of Regulation (EU) 2016/679, according to which 'to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.'

Where strictly necessary to include personal data in these data sets, provision of data, as well as its subsequent use by the public sector bodies, Union institutions, agencies and bodies must fully comply with applicable rules on personal data protection 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 legal basis for the data holder to make such personal data available should be considered compliance with a legal obligation under Article 6(1)(c) of Regulation (EU) 2016/679. The data holder should take reasonable efforts to anonymise the data or, where such anonymization proves impossible, the data holder should apply technological means such as pseudonymisation and aggregation, prior to making the data available. The data holder

Obtenu par CONTEXTE

should inform the data subject in accordance with applicable rules concerning the processing of personal data. In case of the use of data made available to Union institutions, agencies and bodies, Regulation (EU) 2018/1725 shall apply.

The data made available to public sector bodies and Union institutions, agencies and bodies, either to respond to a public emergency or where the unavailability of data make the fulfilment of their legal obligations impossible, should only be used for the purpose for which it was requested unless the enterprise has expressly agreed for the data to be used for other purposes. The data should be deleted once it is no longer necessary for the purpose stated in the request, or agreed subsequently, and the enterprise should be informed thereof.

When reusing data provided by enterprises, public sector bodies and Union institutions, agencies and bodies must 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 Union institutions, agencies or bodies is strictly necessary to fulfil the purpose for which the data has been requested, confidentiality of such disclosure shall be ensured to the data holder.

When the safeguarding of a significant public good is at stake, such as is the case of responding to public emergencies, the public sector should not be expected to compensate enterprises for the data obtained. Public emergencies are rare events and not all 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 having recourse to the provisions of the Data Act. In addition, the public sector bodies should apply the principles of proportionality, transparency as well as adopt a 'once-only' approach to their requests, ensuring that the rights under the Data Act are exercised judiciously. However, as cases of an exceptional need other than a public emergency might be more frequent, the data holders should 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 Union institution, agency or body. The compensation should not be understood as constituting the payment for the data itself. The compensation should likewise not be understood as being compulsory. The data holders may provide the data free of charge or against compensation lower than the permissible upper limit described in this regulation. In practice, the compensation should take into account the marginal costs, such as the costs of adapting the technical infrastructure (e.g. setting up interfaces, cloud space, acquisition of necessary software and hardware), transmission costs, re-formatting costs, costs of metadata enrichment and anonymization or pseudonymisation costs.

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 where this is needed to carry out scientific research activities, processing or assessments of the data it cannot perform. 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 shall be informed about the further sharing of the data it had provided. Individuals or organisations conducting research with whom these data may be shared may include universities or other higher education institutions and their libraries, and entities such as research institutes and hospitals that carry out research. They should act either on a not-for-profit basis or in the context of a public-interest

Obtenu par CONTEXTE

mission recognised by the State. Such a public-interest mission could, for example, be reflected through public funding or through provisions in national laws or public contracts. Conversely, organisations upon which commercial undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, such as through their quality of shareholder or member, which could result in preferential access to the results of the research, should not be considered research organisations for the purposes of this Regulation.

Cooperation and assistance between public sector bodies and Union institutions, agencies and bodies is needed for an effective and efficient application of the provisions included in this Chapter.

When a public sector body in a Member State needs data from an enterprise based in another Member State, such public sector body shall consult the competent authority of that Member State before sending any request to the data holder. A Union institution, agency or body would have to do the same. In case of requests justified by public emergency, the competent authority will also inform the public entity that needs the data if a public sector body in that Member State has already been provided the same data set.

The ability for customers, including both consumers and business customers, to switch between data processing services, such as cloud and edge services, while maintaining a minimum functionality of service, is a key condition for a more competitive cloud and edge market with lower entry barriers for new actors.

Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union required the Commission to encourage service providers to effectively develop and implement, by 29 May 2020, self-regulatory codes of conduct at EU covering best practices for, *inter alia*, facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data. In view of the limited scope of self-regulatory approaches compared to the requirements of Regulation (EU) 2018/1807, and the general unavailability of such open standards and interfaces, a set of minimum regulatory obligations is required to ensure that contractual, economic and technical barriers to effective switching are eliminated to the maximum extent possible.

This Regulation covers data processing services provided to natural and legal persons across the full spectrum of the 'computing continuum': from centralised cloud computing relying on data centres to highly distributed 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. Furthermore, the Regulation covers different service models, from simple data storage and processing (Infrastructure-as-a-Service (IaaS) to the processing of data on platforms (Platform-as-a-Service (PaaS)) or in applications (Software-as-a-Service (SaaS)). Where data storage or other processing does not fall under these service models of centralized and distributed data processing and is merely ancillary to a service provided in a different sector of the economy, it is not regarded as a 'data processing service' by this Regulation.

Without prejudice to existing rights relating to data portability and the termination of contracts, including those introduced by Regulation (EU) 2016/679 and Directive (EU) 2019/770, this Regulation presents obligations on data processing service

Obtenu par CONTEXTE

providers, such as cloud and edge providers, with the objective of allowing customers to switch to a different provider. Switching encompasses all conditions and actions that are necessary for a customer to terminate a contractual arrangement of a data processing service, to conclude one or multiple new contracts with other 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. 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.

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.

Whereas cooperation between cloud service providers to facilitate switching for users is considered good practice, the related provisions in this Regulation should not be interpreted as requiring service providers to develop new categories of services within or on the basis of the IT-infrastructure of other service providers to guarantee functional equivalence in an environment external to their own systems. Nevertheless, service providers are required to offer all assistance and support that is required to make the switching process effective.

Contractual aspects are an essential factor for the ability to switch between data processing services. In this regard, the rights and obligations of the user and the provider should be clearly described and set out in a written contract. Data processing service providers should consider the use of implementation and/or compliance tools, notably those published by the Commission in the EU Cloud Rulebook, as defined in COM/2020/66. 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.

Open standards and open interfaces 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 open standards and open interfaces that facilitate effective cloud interoperability at the PaaS and SaaS levels, this Regulation empowers the Commission to mandate the development of such standards, in accordance with Regulation (EU) No 1025/2012. Open standards may be developed by recognised standardisation bodies or by other open and inclusive coalitions of stakeholders. In particular, the principles of openness, fairness, objectivity and non-discrimination are fundamental requirements of the standardisation processes pursuant to this Regulation, as outlined in COM/2011/0311, which recognises the importance of industrial for a and consortia in contributing to standardisation. Open standards will be referenced by the European Commission if in compliance with the principles of this Regulation and the Commission's initial request.

Obtenu par CONTEXTE

Third countries may adopt laws, regulations and other legal acts which aim at directly transferring or providing governmental access to non-personal data 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 the obligation to transfer or provide access to non-personal data arising from a third country law conflicts with a competing obligation to protect such data under Union or national law, in particular as regards the protection of fundamental rights of the individual or the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data and the protection of intellectual property rights, and including its contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, transfer or access should only be allowed if it has been verified that the third country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent court in the third country, which is empowered to take duly into account the relevant legal interests of the provider of such data. Moreover, data processing services, such as cloud and edge services, should ensure, when signing contractual agreements with other private parties, that non-personal data held in the Union are only accessed in or transferred to third countries in compliance with the law of the Union or the law of the relevant Member State.

To foster further trust in the data, it is essential that safeguards in relation to Union citizens, the public sector and businesses are implemented to ensure control over their data that may be strategically important or sensitive. In addition, Union law, values and standards should be upheld in terms of (but not limited to) security, data protection 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 through the encryption of data, the frequent submission to audits, the verified adherence to relevant security reassurance certification schemes, and (where relevant) the modification of corporate policies. To this end, it is necessary that data processing services adhere to relevant technical standards, codes of conduct and certifications at Union level.

Standardisation and semantic interoperability should play a key role to provide technical solutions to providers to ensure interoperability. This Regulation lays down the requirement for interoperability of the common European data spaces. In order to facilitate the conformity with the requirements necessary to ensure interoperability, it is necessary to provide for a presumption of conformity for interoperability solutions that meet harmonized standards or parts thereof drawn up and published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council, for the purpose of expressing detailed specifications in relation to those requirements. Pursuant to that Regulation, the European Commission will issue a standardisation request to the European Standardisation Organisations for the preparation of harmonized standards that will provide presumption of conformity with those interoperability requirements. Member States and the European Parliament should be able to object to any harmonized standard which, in their view, does not entirely satisfy the accessibility requirements

Obtenu par CONTEXTE

laid down in this Regulation. Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards. The Commission could adopt common technical 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 technical 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. 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.

Data holders should be able to make data available and should be able to ensure that data recipients, in line with applicable Union and national law, are able to access and use data across sectors in accordance with this Regulation. The sector-specific common European data spaces should take due account of common recommendations on interoperability, trust requirements and standards ensuring the appropriate level of findability, accessibility, interoperability and reusability (FAIR).

Use of APIs, based on, in particular, open API specifications, is also a relevant technique for disseminating dynamic data, automating data access and reducing friction in reusing information.

Except where data sharing is legally compulsory, data sharing on a voluntary basis presupposes that data holders can sufficiently trust enterprises to which data are made available, and that conditions of agreements are respected. For efficiency reasons, data holders and recipients may agree to use "smart contracts" on electronic ledgers for instance for recording consent, for processing data sharing, and for automatically sanctioning the breach of any conditions for data sharing. In the absence of common standards, smart contracts are currently not interoperable across economic sectors and across regions. It is therefore necessary to determine minimum standards for smart contracts that facilitate interoperability in the data economy.

This Regulation lays 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. Compliance with these essential requirements will promote the inter-operability of smart contracts in data sharing applications. In order to facilitate the conformity of such smart contracts with those common essential requirements, it is necessary to provide for a presumption of conformity for smart contracts that meet harmonised standards or parts thereof drawn up and published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council, for the purpose of expressing detailed specifications in relation to those requirements. Pursuant to that Regulation, the European Commission will issue a standardisation request to the European Standardisation Organisations for the preparation of harmonised standards that will provide presumption of conformity with those requirements. Member States and the European Parliament should be able to object to any harmonised standard which, in their view, does not entirely satisfy the accessibility requirements laid down in this Regulation. Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards.

As this Regulation concerns the Internal Market for data in general, involving rights and obligations of a wide range of actors, including businesses, consumers and public

Obtenu par CONTEXTE

bodies, institutionalised and structured cooperation is required between several competent oversight authorities, including data protection authorities. This cooperation should ensure in particular that all relevant information can be exchanged with the relevant authorities so they can fulfil their complementary role, while acting in accordance with their respective institutional mandate. Such cooperation is necessary to ensure efficiency, coherence and the avoidance of duplication, as well as simplicity, in particular, from the perspective of consumers and micro-, small and medium enterprises who should not be expected to have easy access to the legal advice necessary to ascertain the particular authority competent for individual potential violations of this Regulation. Therefore Member States should designate one or more competent authorities to supervise the implementation of the Data Act who should cooperate as appropriate with each other and, in the case of more than one authority, should also designate a coordinating competent authority. This should include the authority responsible for the supervision of compliance with data protection rules, who should supervise the exercise of requests for access and data sharing where it is made by a user that is a natural person. In areas where sectoral legislation requires data holders to make data available, the competent authority designated under that sectoral legislation may be designated as a competent authority for those areas under this Regulation.

Anyone should be entitled to seek redress for the infringements of their rights under the Data Act by lodging complaints with any of the designated competent authorities, and those authorities should be obliged to cooperate to ensure the complaint is appropriately handled and resolved.

Member States authorities should ensure that infringements of the obligations laid down in this Regulation are sanctioned by administrative fines or financial 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. Financial penalties and administrative fines shall in each individual case be effective, proportionate and dissuasive, with due regard to the provision of sufficient and accessible procedural safeguards, and in particular to ensure consistency in the application of this Regulation.

The exercise by the competent authorities of their powers under this Regulation should be subject to appropriate procedural safeguards in accordance with Union and national law, including effective judicial remedy and due process.

In order to help enterprises to draft and negotiate contracts, the Commission should develop and recommend non-mandatory model contract terms for business-to-business data sharing contracts. These model contract terms are primarily a practical tool to help in particular smaller enterprises to conclude a contract. The parties can decide whether and to what extent they will use the recommended model contract terms or can even adapt them. When used widely and integrally, these model contract terms will 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 in the different market sectors when accessing and sharing data.

The user access right provided for in Chapter II of this Regulation should be balanced against the rights of parties other than the manufacturer of a product or the provider of a service, or any party involved by the manufacturer or service provider in the design

Obtenu par CONTEXTE

manufacturing or commercialisation of the product or service. As underlined in the Intellectual Property Action Plan[64], intellectual property rights, namely. patents, designs, copyright, in particular under Directive (EU) 2019/790, the protection awarded to databases under Article 3 of Directive 96/9/EC, along with the protection of trade secrets against unlawful use, acquisition or disclosure under Directive (EU) 2016/943 (Trade Secrets Directive), help entrepreneurs and companies to derive value from their intangible assets. Intellectual Property rights, with the exception of the *sui generis* right under Article 7 of Directive 96/9/EC with regard to data generated or obtained by a user's product or related service, are unaffected by this Regulation. Rights of the manufacturer of a product or the provider of a service, or any party involved by the manufacturer or service provider in the design manufacturing or commercialisation of the product or service under the aforementioned regulations should not stand in the way of exercising the rights provided under Chapter II of this Regulation. In case the data covered by the access right qualify for protection under the aforementioned regulations, the obliged enterprise should communicate this fact in the conditions accompanying the provision of access so that the beneficiaries of the access right (user and potentially third parties) can take all relevant measures to safeguard those rights. As concerns their rights under the provisions of the Trade Secrets Directive, the provisions of this Regulation should not be read to make data that a user may demand access to "generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question" and be no longer considered to be "subject to reasonable steps under the circumstances" in the sense of Article 2(1)(a) and (c) of that Directive. This Regulation should thus not be read to limit a manufacturer's right to keep information secret from other parties.

The Court of Justice of the European Union[65] has ruled that the *sui generis* protection for databases, enshrined in the Database Directive (96/9/EC of 11 March 1996 on the legal protection of databases), is limited to those cases where the investment's direct aim is to produce databases and not where databases are produced incidentally as a by-product of other activities, as it is the case with data generated by connected devices. Therefore, the sui generis right, provided for in Article 7 of that Directive does not apply to databases containing data obtained or generated by means of physical components, such as sensors, of a connected product or a related service. However, the risk exists that holders of those data could nevertheless attempt to claim the *sui generis* right protection against the effective application of this Regulation, and at odds with the intended purposes of database protection in EU law. For the avoidance of doubt, it should therefore be clarified that a *sui generis* right on databases containing data obtained from or generated by connected products and related services cannot be invoked to hinder the effective exercise of the access right and of the right to make available foreseen in this Regulation.

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 to introduce a monitoring mechanism on switching charges imposed by data processing service providers on the market.

---

64 COM/2020/760 final.

65 Cf. 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).

Obtenu par CONTEXTE

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission 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 smart contracts. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[66].

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 which 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 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. Where justified by sector-specific regulatory objectives, the general rules for making data available between businesses, contained in this Regulation may be complemented, to the extent necessary, by sector-specific rules and requirements that are consistent with the objectives of this Regulation. The sector-specific rules could in particular set out additional requirements in the form of technical aspects of the data access (e.g. API architecture), mandate sector-specific data formats or include detailed rules on cybersecurity to ensure secure access to certain data. Other provisions complementing the rules in the Data Act could regulate issues going beyond data access and use, such as enforcement mechanisms, enabling access to functions of a connected device or sourcing data to the connected device.

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.

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an 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 for making data available by:

[66] 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).

Obtenu par CONTEXTE

(a) ensuring that users of a product or related service in the Union can access, in a timely manner, the data generated by their use of that product or related service and that those users can use those data, including by sharing them with third parties of their choice;

ensuring consistent conditions, including on compensation, that apply whenever a data holder is legally obliged to make data available to a data recipient;

preventing the exploitation of contractual imbalances that hinder fair data access and use for micro-, small- or medium-sized enterprise within the meaning of Commission Recommendation 2003/361/EC;

ensuring that data holders make available to public sector bodies or to a Union institutions, agencies or bodies, where there is an exceptional need, the data that are necessary for the performance of a task carried out in the public interest;

facilitating switching between data processing services;

enhancing the interoperability of data and data sharing mechanisms and services.

2. This Regulation applies to:

(a) Manufacturers of connected products and providers of related services placed on the market in the Union and the users of such products and services;

enterprises obliged or able to make data available to data recipients in the Union;

data recipients in the Union to whom data are made available;

Member State public sector bodies and Union institutions, agencies or bodies that request data holders to make data available for use where there is an exceptional need;

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

3. Union law on the protection of personal data shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall be without prejudice to 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 these Articles, the provisions of this Regulation complement the right under Article 20 of Regulation (EU) 2016/679.

This Regulation is without prejudice to 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 of 29 April 2021 on addressing the dissemination of terrorist content online and the [e-evidence proposals [COM(2018) 225 and 226] once adopted, and international cooperation in that area, and to 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.

Obtenu par CONTEXTE

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;

'product' means a tangible, movable item that obtains, generates or collects, data concerning its use or environment, and that is able to communicate such data via a publicly available electronic communications service and whose primary function is not the storing and processing of data;

'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;

'user' means a natural or legal person that owns, rents or leases a product;

'data holder' means a legal or natural person who has the right or obligation, in accordance with applicable Union or national law, and in the case of non-personal data, the ability, to make available certain data;

'data recipient' means a legal or natural person, other than the user of a product or related service, who 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 and to whom the data holder makes data available, following an request to that effect by the user or in accordance with a legal obligation under Union law;

'virtual assistants' means software that is incorporated or inter-connected with a product, that can process demands, tasks or questions based on audio, imaging or other cognitive-computing technologies, including augmented reality services, and based on those demands, tasks or questions access their own and third party services or control their own and third party devices

'common European data spaces' mean purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, development of new products and services, scientific research or civil society initiatives;

'Union institutions, agencies and bodies' means the Union institutions, bodies, offices and agencies set up by, or on the basis of, the TEU, the TFEU or the Euratom Treaty;

'public sector body' means Member State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law;

'public emergency' refers to exceptional situations negatively affecting a major part of a Member State(s) population or their fundamental rights, with a risk of serious and lasting repercussions on living conditions and the economic stability of the Member State(s). Public emergencies include major natural disasters, public health emergencies as well as human-induced major disasters, such as those caused by terrorism;

'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,

Obtenu par CONTEXTE

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘data processing service’ means a digital service, provided by a service provider 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;

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

‘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;

‘open standard’ mean technical specifications, for repeated or continuous application, publicly available for implementation and use on reasonable terms (including for a reasonable fee or free of charge), adopted through an inclusive, collaborative, consensus-based and transparent process from which materially affected and interested parties cannot be excluded;

‘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;

‘electronic ledger’ means an electronic ledger within the meaning of point 53 of Article 3 of the [Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014];

‘electronic ledger system' means a system that implements an electronic ledger;

‘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;

‘interoperability’ means the ability of two or more data spaces or communication networks, systems, devices, applications or components to exchange and use data in order to perform required functions;

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

CHAPTER II
BUSINESS TO BUSINESS AND BUSINESS TO CONSUMER DATA SHARING

Article 3
Obligation to make data generated by the use of products and 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 accessible to the user.

Virtual assistants offered independently of the provision of a product, or by design capable of being incorporated into or of interacting with different products not limited to those

Obtenu par CONTEXTE

offered by the provider of such virtual assistants and partner companies and linked companies in the sense of Commission Recommendation 2003/361/EC, shall be designed in such a manner that data generated by their interaction with the user are, by default, easily accessible to the user.

Before the conclusion of a contract for the purchase, rent or lease of a product or a related service or of a virtual assistant 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 from the use of the product or related service;

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

whether any enterprise intends to use the data itself or allow a third party to use the data and, if so, the purposes for which the data will be used;

how the user may access this data; 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;

the means of communication which enable the user to contact the data holder quickly and communicate with it efficiently;

how the user may request that this data be shared with a third-party;

the user's right to lodge a complaint of alleged violation of provisions of this Chapter with the competent supervisory authority referred to in Article 30.

Article 4

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

1. Upon request by a user, the data holder shall make available to the user the data generated by the use of a product or related service or by a virtual assistant without undue delay, free of charge and, where applicable, continuously and in real-time.

The data holder shall not require the user to provide any information beyond what is necessary to verify its quality as a user pursuant to paragraph 1.

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

The user shall not use the data to develop a product that competes with the product from which the data accessed originate.

Any personal data generated by 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. The data holder shall also have a contractual agreement with the user to use such personal data.

The data holder may use any non-personal data generated by the product or related service only on the basis of a contractual agreement with the user.

Obtenu par CONTEXTE

Article 5
Right to share data with third parties

1. The data holder shall, upon request by a user, or by a third party authorised by the user, 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, and, where applicable, continuously and in real-time.

Any undertaking providing core platform services for which one or more of such services have been, pursuant to Digital Markets Act, designated as a gatekeeper shall not be considered an eligible third party and therefore shall not:

(a) solicit or commercially incentivize a user in any manner, including by providing a monetary or any other compensation, to supply to one of its services data that the user has obtained as a result of the obligation under Article 4(1) or solicit or commercially incentivize the user to request the data holder to make data available to one of its services on the basis of the right under paragraph 1 of this article ;

accept to receive from a user data that the user has obtained as a result of the obligation under Article 4(1) .

The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or authorised third party pursuant to paragraph 1.

The user or 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 the data.

Any personal data generated by 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.

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.

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.

Article 6
Obligations of third parties receiving data at the request of the user

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

The third party shall not:

Obtenu par CONTEXTE

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

use the data made available 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;

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

make the data available to an undertaking providing core platform services for which one or more of such services have been, pursuant to the Digital Markets Act, designated as a gatekeeper;

use the data to develop a product or related service that competes with the product or related service from which the data originate or share the data with another third party for that purpose.

prevent the user, including through contractual commitments, from making data available to other parties.

Article 7
Exclusion of micro and small enterprises

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 within the meaning of Commission Recommendation 2003/361/EC, provided those enterprises are not economically dependent on another enterprise which does not qualify as a micro or small enterprise.

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 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.

A data holder shall agree with a data recipient the terms for making the data available. Any contractual term shall not be binding if the term fulfils the conditions of paragraphs 2, 3 and 4 of Article 13, in which case paragraph 6 of Article 13 shall apply, or if the term excludes the application of, derogates from or varies the effect of the user's rights under Chapter II if applicable.

Data holders shall not discriminate between comparable categories of data recipients in the making available of data, including partner enterprises or linked enterprises of the data holder within the meaning of Commission Recommendation 2003/361/EC.

Obtenu par CONTEXTE

Where the other enterprise considers conditions to be discriminatory, it shall be for the data holder to prove that there has been no such discrimination.

Data shall not be made available to a data recipient on an exclusive basis.

A data holder or data recipient shall not be required to provide any information beyond what is necessary to verify compliance with the agreed contractual terms, this Regulation or other applicable Union law or national law implementing Union law.

Unless otherwise provided for by Union law, including in Article 6, or by national law implementing Union law, an obligation to make data available to a data recipient does 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 the data recipient for making data available shall be reasonable and non-discriminatory.

Where the data recipient is a micro-, small or medium enterprise within the meaning of Commission Recommendation 2003/361/EC, any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and is attributable to its request.

Paragraph 2 shall be without prejudice to other Union legislation or national legislation implementing Union legislation that excludes compensation or provides for lower compensation.

The data holder shall provide to the data recipient, the basis for the calculation of the compensation with a sufficient degree of detail that it can be verified that the requirements of paragraphs 1 and 2 are complied with.

Article 10
Dispute settlement

1. Data holders and data recipients shall have access to dispute settlement bodies, certified in accordance with paragraph 2, 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.

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 decision in accordance with clear and fair rules of procedure;

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 of those terms;

it is easily accessible through electronic communication technology;

it is capable of issuing a decision in a swift, efficient and cost-effective manner and in at least one official language of the Union.

Obtenu par CONTEXTE

If no dispute settlement body is certified in a Member State [by 12 months after the date of entry into force of this Regulation], that Member State shall establish and certify a dispute settlement body in line with the conditions set out in points (a) to (d) of this paragraph.

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.

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.

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

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, those bodies shall provide those parties with the submissions of the other party and any statements made by experts and those bodies shall grant those holders and recipients the possibility to comment on those submissions and statements.

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.

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.

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

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 the data available.

A data recipient that has provided inaccurate or untruthful information to the data holder, has deployed coercive means or has abused evident gaps in the technical infrastructure of the data holder designed to protect the data for the purposes of obtaining the data, or has used those data 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 user directs otherwise,

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

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.

Obtenu par CONTEXTE

Paragraph 2 (b) shall not apply in either of the following cases:

(a) the use of the data in question did not cause significant harm to the data holder;

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

Such technical protection measures shall not be used as a means to hinder the user's right to effective data sharing with third parties pursuant to Article 5 or any right of a third party under Union legislation or national legislation implementing Union legislation, referred to in Article 8(1).

Article 12

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

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

Any contractual term 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.

This Chapter shall only apply in relation to provisions of Union law or national law implementing Union law which enter into force after [12 months after the date of entry into force of this 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 on a micro, small or medium-sized enterprise within the meaning of Commission Recommendation 2003/361/EC shall not be binding on that enterprise if it is unfair.

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.

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;

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;

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.

Obtenu par CONTEXTE

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 the obligations of the contract or the liability in case of breach of obligations;

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

prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the term 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;

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 term of the contract or within a reasonable period after the termination thereof;

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.

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 which supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed.

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

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.

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 provide data 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.

Obtenu par CONTEXTE

This Chapter shall not apply to small and micro enterprises within the meaning of Commission Recommendation 2003/361/EC.

Article 15
Exceptional need to use data held by enterprises

An exceptional need to use data within the meaning of this Chapter shall be deemed to exist where:

(a) the data requested is necessary to respond to a public emergency, or

where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling its legal obligations; and

the public sector body or Union institution, agency or body have been unable to obtain such data by alternative means, including by purchasing the data on the market or by relying on existing obligations to provide the data and found them not fit for purpose, and where the adoption of new legislative measures cannot ensure the timely availability of data; or

where obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for enterprises.

Article 16
Relationship with other obligations to make data available

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.

The rights of 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 is without prejudice to 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 in the field of customs and taxation.

Article 17
Requests for data to be made available

1. A public sector body or a Union institution, agency or body, where submitting a request for access to data in view of an exceptional need shall:

(a) specify what data are required;

specify the timescale within which the data are to be provided or within which the data holder may request the requesting Union institution, body or agency institution, body or agency to modify or withdraw the request

demonstrate the exceptional need for which the data is requested;

explain the purpose of the request and the intended use of the data requested;

state the legal basis for requesting the data;

Obtenu par CONTEXTE

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

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;

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;

concern, insofar as possible, non-personal data;

make the request publically available online without undue delay;

inform the data holder of the penalties that shall be imposed pursuant to Article 32 by a competent authority referred to in Article 30 in the event of non-compliance with the request.

A public sector body or a Union institution, agency or body shall not make data obtained pursuant to this Chapter available for reuse. Directive (EU) 2019/1024 shall not apply to the data held by public sector bodies obtained pursuant to this Chapter. In the case of an exchange of data between public sector bodies purely in the pursuit of their public tasks, the purpose limitations set out in Article 15 and Article 21 shall continue to apply.

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, agency or body without undue delay.

Without prejudice to specific needs regarding the availability of data defined in sectoral legislation, no later than 5 working days following the receipt of a request for the data necessary to respond to a public emergency and no later than 15 days in other cases of exceptional need, the data holder may decline or seek modification of the request on one of the following grounds:

(a) the data is unavailable; or

the request fails to respect the conditions laid down in Article 17(1).

In case of the request for data necessary for responding to a public emergency, the data holder may also decline or seek modification of the request if it 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)(b).

When declining or seeking modification of the request in accordance with paragraph 3, the data holder shall indicate the identity of the public sector body or Union institution agency or body that previously submitted the request.

Where compliance with the request to make data available for use 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.

Where the public sector body or Union institution agency or body wish to challenge the refusal to provide the data as requested, or where the data holder wishes to challenge

Obtenu par CONTEXTE

the request, the matter shall be brought to the competent authority referred to in Article 30.

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 accessed data pursuant to Article 14 shall:

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

   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.

The public sector body or the Union institution, agency or body shall not use the data in a manner that may harm the data holder that made the data available.

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

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

Where the data holder claims compensation for providing the data in compliance with the request made pursuant to Article 15(b), such compensation shall not exceed the costs incurred to comply with the request including, where necessary, the costs of anonymization and of technical adaptation, plus a reasonable margin.

Article 21
Contribution of scientific research

1. Notwithstanding Article 17(2), a public sector body or a Union institution, agency or body shall be entitled to transmit or make available data received under this Chapter to individuals or organisations in view of carrying out scientific research related to the purpose for which the data was requested, or to national statistical institutes and Eurostat for the compilation of official statistics.

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, and 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. Confidentiality of any trade secrets disclosed shall be preserved by appropriate measures.

Where such data is transmitted or made available under paragraph 1, the public sector body or Union institution, agency or body shall notify the data holder by whom the data was originally made available.

Obtenu par CONTEXTE

Article 22
Mutual assistance and cross-border cooperation

1. Public sector bodies and Union institutions, agencies and bodies shall endeavour to cooperate and assist one another, including through the sharing of information, to implement the provisions of this Chapter in a consistent manner.

Any information exchanged in the context of assistance requested and provided under paragraph 1 shall be used only in respect of the matter for which it was requested.

A public sector body, prior to requesting data from a data holder based in another Member State, shall notify the competent authority of that Member State as referred to in Article 30. This requirement shall also apply to requests by Union institutions, agencies and bodies.

When notified under paragraph 3, the competent authority shall advise the public sector body on the need, if any, to cooperate with public sector bodies based in that Member State with the aim to reduce the administrative burden on the data holder. The public sector body shall take the advice of the 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 in Articles 24, 25 and 26 to ensure that customers of the service can switch to a data processing service, covering the same service type, which is provided by another service provider. In particular, the data processing service provider shall remove obstacles of commercial, technical, contractual and organisational nature, which inhibit users of the service from:

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

   concluding new contracts with another provider of data processing services;

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

   maintaining functional equivalence of the service in the IT-environment of the concerned other providers of data processing services covering the same service type, in accordance with Article 26.

Paragraph 1 shall only apply to obstacles that are related to the services, contractual agreements or commercial practices of the provider concerned.

Article 24
Contractual terms concerning switching between providers of data processing services

1. The rights of the customer and the obligations of the data processing service provider in relation to switching between providers of data processing 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:

Obtenu par CONTEXTE

(a) clauses allowing the customer to, upon request, switch to a data processing service offered by another data processing service provider 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 days, during which the data processing service provider:

will assist and, where technically feasible, complete the switching process; and

shall ensure full continuity in the provision of the respective functions or services.

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 meta-data created by the customer and by the use of the service during the period of service provision, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service;

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

Where the mandatory transition period as defined in paragraph 1(a) and (c) is technically unfeasible, the service provider 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 surpass 6 months. In accordance with paragraph 1, full service continuity shall be ensured throughout the alternative transition period against reduced charges, as defined in Article 25(2).

Article 25
Gradual withdrawal of switching charges

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

From [date X-3yrs] until [date X], providers of data processing services may impose reduced charges on the customer for the switching process.

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.

The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement this Regulation by introducing a monitoring mechanism on switching charges imposed by data processing service providers on the market.

Article 26
Technical aspects of switching

1. For 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 do not provide access to the operating services, software and applications that are stored, otherwise processed or deployed on those infrastructural elements, service providers shall ensure that, after switching

Obtenu par CONTEXTE

to a service covering the same service type offered by another service provider, the customer enjoys functional equivalence in the use of the new service.

For services other than those covered by paragraph 1, service providers shall ensure compatibility with open standards or open interfaces for interoperability that exist in the functional domain concerned, with a view to support customers to effectively switch between data processing services covering the same service type, while ensuring functional equivalence.

Where the open standards or open interfaces referred to in paragraph 2 do not exist for the service type concerned, the provider shall, on 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.

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 governmental access would create a conflict with Union law or national law of the relevant Member State, without prejudice to paragraph 2 or 3.

Any 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 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.

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 of an administrative authority of a third country to transfer from or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only:

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

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

(c) the competent court issuing the order or reviewing the decision of an administrative authority is empowered under the law of that country to take

Obtenu par CONTEXTE

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.

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 of the request.

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
Interoperability

1. Interoperability schemes referred to in paragraph 3 that meet the harmonised standards or parts thereof drawn up and published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the essential requirements necessary to ensure interoperability, to the extent those standards cover those requirements.

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

The Commission shall be empowered, by way of implementing acts, adopted in accordance with the examination procedure referred to in Article 38 (2),, to adopt common specifications, in case it considers that the relevant harmonised standards referred to under paragraph 1 are insufficient, where necessary, with respect to any or all of the following:

(a) core vocabularies for semantic interoperability;

technical means, such as application programming interfaces, for enabling automatic access and transmission of data between parties including continuous or real-time with machine-readable format;

switching between data processing services;

interoperability of smart contracts;

the interoperability requirements 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 not covered under points (a) to (d), taking into account Union or national sectoral legislation.

The Commission shall be empowered by means of implementing acts and taking into account Union or national sector legislation, to enable the interoperability provided by open standards and open interfaces referred to in Article 26(2), by mandating the use of

Obtenu par CONTEXTE

such open standards, open interfaces and common specifications. Such implementing acts shall be adopted in accordance with the examination procedure referred to in Article 38 (2).

Article 29
Minimal requirements regarding smart contracts for data sharing

1. 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, at a minimum:

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

   ensure, insofar as the smart contract automates the compensation in the context of agreements to make data available, that a mechanism exists to interrupt the continued execution of transactions;

   ensure that the design of the smart contract ensures continuity or an orderly termination in case of an interruption of the smart contract or an upgrade of the protocol of the related electronic ledger.

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 requirements under paragraph 1 and, on the fulfilment of the requirements, issue an EU declaration of conformity.

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.

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 in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the essential requirements according to paragraph 1 to the extent those standards cover those requirements.

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

Where harmonised standards referred to in paragraph 4 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 in a cross-border context, the Commission may, by means of implementing acts, adopt common specifications in respect of the requirements set out in paragraph 1. Such implementing acts shall be adopted in accordance with the examination procedure referred to in Article 38 (2).

Obtenu par CONTEXTE

CHAPTER IX

IMPLEMENTATION AND ENFORCEMENT

Article 30
Competent authorities

1. Member States 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.

Without prejudice to paragraph 1,

(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 users that are natural persons.

for specific sectoral data exchange issues related to the implementation of this legislation, the competence of sectoral authorities shall be respected;

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

Member States shall ensure that the respective tasks and powers of the competent authorities 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;

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 supervisory authority is necessary;

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

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;

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

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;

ensuring the online public availability of requests for data to be made available for re-use by public sector bodies in the case of emergencies under Chapter V;

Obtenu par CONTEXTE

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 data processing service providers;

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

Where a Member State designates more than one competent authority, the competent authorities shall, in the exercise of the tasks assigned to them under paragraph 3, 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, Member States shall designate a coordinating competent authority.

Member States shall communicate the name of the designated competent authorities and their respective tasks and, where applicable, the name of the coordinating competent authority to the Commission.

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.

Article 31
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 national 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.

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.

Without prejudice to the specific cooperation mechanisms provided for by Chapters VI and VII of Regulation (EU) 2016/679, competent authorities shall cooperate to handle and resolve complaints, including by exchanging all relevant information by electronic means, without undue delay.

Article 32
Penalties

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

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

For infringements of the obligations laid down in Chapter II, III and V, 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

Obtenu par CONTEXTE

Regulation (EU) 2016/679 and up to the amount referred to in Article 83(5) of that Regulation.

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

Article 33
Model contract terms

The Commission shall develop and recommend non-binding model contract terms on data access and use which can help the parties to draft and negotiate a contract with balanced contractual rights and obligations.

CHAPTER X

SUI GENERIS RIGHT UNDER DIRECTIVE 1996/9/EC

Article 34
Impossibility of relying on certain sui generis rights

The sui generis right provided for in Article 7 of Directive 96/9/EC cannot be invoked on databases containing data obtained from or generated by a product or related service as defined in Article 2(2) and (3) to hinder the effective exercise of the access right provided for in Article 4 or of the right to make available provided for in Article 5.

CHAPTER XI

FINAL PROVISIONS

Article 35
Amendment to Regulation (EU) No 2017/2394

In the Annex to Regulation (EU) No 2017/2394 of the European Parliament and of the Council the following point is added:

‘28. [Data Act].’

Article 36
Amendment to Directive (EU) 2020/1828

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

‘67. [Data Act]’

Article 37
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.

Obtenu par CONTEXTE

The power to adopt delegated acts referred to in Articles 25(4) shall be conferred on the Commission for an indeterminate period of time from […].

The delegation of power referred to in Articles 25(4) 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.

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

A delegated act adopted pursuant to Article 25(4) 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 38
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.

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

Article 39
Other Union legal acts governing data sharing rights and obligations

1. The specific obligations for the making available of data between businesses, between businesses and consumers, and on an *ad hoc* or exceptional basis between businesses and public bodies, in Union legal acts that entered into force on or before [xx XXX xxx], and existing and future delegated or implementing acts based thereupon, shall remain unaffected. Where it is required to review these legal acts, the Commission shall take into account the provisions and principles of this Regulation.

Where a sector-specific Union legal act further specifies the rights and obligations relative to data access and use set out in Chapters II and III where necessary for specific sectors and consistent with this Regulation, and complements these rights and obligation where needed for specific operational needs of the sector, in particular in relation to technical aspects of the data access, including cybersecurity or data formats as well as in relation to aspects going beyond data access and use those provisions of that sector-specific Union legal act or national law shall also apply.

When the Commission reviews, in accordance with the review clauses stipulated therein, existing legal acts that touch upon the subject matter or scope of this Regulation, it shall assess the need to align them with this Regulation and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the making available of data between businesses, between businesses

Obtenu par CONTEXTE

and consumers, and between businesses and public bodies within the scope of this Regulation.

Article 40
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].

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 exceptional needs in the sense of Article 15 for which the public sector may request use of data held by enterprises;

(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 transition period defined in Article 25.

Done at Brussels,

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

Obtenu par CONTEXTE