交大法學評論，第 14 期，頁 133（2024）

Supply Chain Data Sharing: Evaluating Challenges and Opportunities of EU Data Law

Nils Wiedemann [*], Maximilian Leicht [**]

Abstract

After regulating the processing of personal data with the GDPR, the EU is now aiming to govern the emerging data economy. The different acts of this so-called data law shall create a single market for data. To this end, the legislation intends to break up data monopolies and incentivise the sharing of both non-personal and personal data. We argue that the data law will have a major impact on international supply chain data sharing – especially, because this involves complex layers of different stakeholders. Especially the Data Act (DA) will have a significant effect on data sharing. The regulation lays down harmonising rules on how to access and share data generated by products of the "Internet of Things" (IoT), which covers not only smart home devices but also industrial machines

* PhD student, Chair of Legal Informatics, Saarland University.
** PhD student, Chair of Legal Informatics, Saarland University.
This research was supported by the "PAIRS" project which is funded by the German Federal Ministry for Economic Affairs and Climate Action (grant reference: 01MK21008H). Further information on the research project can be found at https://www.pairs-projekt.de/en/https://www.pairs-projekt.de/en/.
投稿日：2023 年 12 月 28 日；採用日：2024 年 2 月 21 日

connected to the internet. The DA applies to products placed in and data transferred to the EU. It is a horizontal framework which the EU intends to complement with several sector-specific regulations for the creation of so-called “data spaces”. The Commission has recently published a proposal for the first data space – the European Health Data Space (EHDS). Further data spaces shall cover other supply-chain-related areas like manufacturers or mobility. This paper analyses the effects of the European Data Law on supply chain data sharing as one of the most promising scenarios and illustrates both chances and challenges of the regulatory framework. For a comprehensive view, it highlights relevant parts of the new cybersecurity framework for products with digital elements (mainly the Cyber Resilience Act) and their influence on data sharing.

Keywords: Data Act, Cyber Resilience Act, Data Sharing, Data Law, Cybersecurity, Supply Chain

1. INTRODUCTION

In recent years, the rapid increase in the amount of data generated worldwide in conjunction with various market failures in the data economy has revealed an urgent need for a new governance of data processing. The volume of the data generated annually worldwide is expected to reach 175 zettabytes (equals to 175.000.000.000.000.000.000.000 bytes) in 2025.[1] In parallel, the European Commission (EC) expects that the way data is stored and processed will change dramatically. Based on an assessment by Gartner, the EC estimates that 80% of the data processing will take place in "smart connected objects, such as cars, home appliances or manufacturing robots, and in computing facilities close to the user ('edge computing')" rather than a processing of data in "data centres and centralised computing facilities."[2] In other words, the EC expects that a substantial part of the world's trade goods will include so-called digital elements which allow a certain processing of data. This emerging trend is described as the Internet of Things (IoT) or, for industrial purposes, the Industrial Internet of Things (IIoT). Furthermore, the value of data generated by products of the industrial IoT – like sensors and robots within a production line or for logistic purposes – should not be underestimated as it may allow companies to enhance procedures and drastically increase efficiency. However, companies are disincentivised to share data that is

1 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data*, at 2, COM (2020) 66 final (Feb. 19, 2020).

2 *Id*. at 2. While these exact numbers may not materialise in this way, the estimations show on which trend the EC's deliberations were founded. Interestingly enough, other estimations, also by Gartner, show slightly different numbers, *see* Rob van der Meulen, *What Edge Computing Means for Infrastructure and Operations Leaders*, GARTNER (Oct. 3, 2018), https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders.

generated and transmitted to them by the sold products as it may disclose trade secrets or create an unfair advantage for competing companies. Thus, despite the companies' interest in the sharing of data, for most companies – especially small and middle-sized companies (SME) – it is a big risk to take the first step to share data on a large scale.

In 2020 the European Commission published its proposal for a European strategy for data.[3] The strategy's aim is "to increase the use of, and demand for data and data-enabled products and services throughout the Single Market."[4] According to the EC's data strategy, this shall create a single market for data where "data can flow within the EU across sectors for the benefit of all" but where "European rules, in particular privacy and data protection, as well as competition law, are fully respected" and where "the rules for access and use of data are fair, practical and clear."[5] In order to achieve this goal, the EU intends to enact legislation to break up data monopolies and incentivise the sharing of both non-personal and personal data.[6] For this purpose, the EC subsequently proposed the Data Governance Act (DGA)[7] – which applies since 24 September 2023 – and the

3 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data*, *supra* note 1, at 1.

4 *Id*.

5 *European Data Strategy*, EUROPEAN COMMISSION, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (last visited Oct. 31, 2023).

6 *Commission Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)*, at 17, COM (2022) 68 final (Feb. 23, 2022) [hereinafter *DA-P*].

7 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act), 2022 O.J. (L 152) 1 [hereinafter DGA].

Data Act (DA)[8], whose final version could – depending on the ongoing legislative process – enter into force at the end of 2023. Unlike the EU's infamous General Data Protection Regulation (GDPR)[9], the material scope of these two "Acts" does not distinguish between personal and non-personal data but applies to both of them.[10] Therefore this kind of law can be denoted as "data law". It is most likely that the data law will reshape the data economy within the EU but affect the international data economy as well, since – beside the People's Republic of China and the United States – the EU is one of the largest global players in international trade and in 2020 accounted for around 14% of the world's trade in goods.[11]

Furthermore, as an answer to ongoing cybersecurity threats, the EU introduced various new legal acts concerning the cybersecurity of products and the cyber resilience of certain infrastructure. The EU identified cyber-attacks on supply chains as one of the top risks.[12] The new legislature therefore involves extensive requirements both for manufacturers of so-called "products with digital elements" as well as for companies whose products are supposed to be used in critical infrastructure or other critical sectors. These sectors include e.g. the manufacturing of electronic products, of electrical equipment or of motor vehicles. This probably will result in corresponding contractual obligations in the supply chain as well as in

8 *DA-P*, *supra* note 6.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

10 *DA-P*, *supra* note 6, at 37-38; DGA, *supra* note 7, art. 1, 2(1), at 18.

11 *Facts and Figures on the European Union economy*, EUROPEAN UNION, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (last visited Oct. 31, 2023).

12 *Top Cyber Threats in the EU*, COUNCIL OF THE EU AND THE EUROPEAN COUNCIL, https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/ (last visited Oct. 31, 2023).

modifications of the production process, even if the contract partners are not based in the EU/EEA. Therefore, this will have a reasonable impact on international supply chains.

This contribution illuminates the implications of EU data law (section III.) and the cybersecurity framework (section IV.) and evaluates the impact on the data sharing within international supply chains (section V.). For this purpose, the contribution illustrates the complex legal system of the EU and how the recent regulations affect its current legal framework (section II.). The evaluation of the impact is based on a fictional international supply chain in order to elucidate the effects on both international and EU stakeholders.

2. CURRENT LEGAL SYSTEM OF THE EUROPEAN UNION

The legal system of the EU is complex as it is an amalgam consisting of supranational Union law and the national law of its twenty-seven Member states. Thus, this contribution gives a brief overview of the EU's legal system (1.) and subsequently illustrates the current legal system in the European Union for the processing of both personal and non-personal data. As the current legal framework is vast, the scope is limited to the implications of Data Protection Law and the GDPR (2.), the ePrivacy Directive (3.), intellectual property and trade secret law (4.), and the Data Governance Act and the Digital Markets Act (5.). It provides a short summary of the current framework's shortcomings (6.). Finally, it outlines the current cybersecurity framework (7.).

2.1 Introduction to the Legal System of the EU

This part shall give a short overview of the history of the EU and its current legal system. The EU supersedes the European Community and was established

with the Treaty on European Union, which entered into force on 1 November 1993.[13] It was amended by the Treaty of Lisbon,[14] which entered into force on 1 December 2009. The treaties transfer certain competences of the Member states to the institutions of the EU and enable them to adopt legislation, which is subsequently implemented by the Member states.[15] The legal system of the EU differentiates between primary and secondary law (see Figure 1). The primary law sets out the distribution of competences between the EU and EU Member States and includes, for example, the Treaty on the European Union (TEU)[16], the Treaty on the Functioning of the European Union (TFEU)[17], and the Charter of Fundamental Rights (EU Charter).[18] The secondary law primarily consists of the enacted regulations, directives and decisions.[19] Regulations have "general application" and are binding in their entirety and directly applicable in all Member States of the EU.[20] Many regulations – like, for example, the GDPR – provide some opening clauses which allow the Member States to implement more specific law.[21] However, the Member States must satisfy the conditions laid down in the

13 Treaty on European Union, 1992 O.J. (C 191) 1 (Also known as Treaty of Maastricht).

14 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 2007 O.J. (C 306) 1.

15 Treaty on European Union, *supra* note 13, art. 5, at 18.

16 Consolidated Version of the Treaty on European Union, 2012 O.J. (C 326) 1.

17 Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. (C 326) 47 [hereinafter TFEU].

18 Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1. For a comprehensive overview *see The European Union's Primary Law*, EUROPEAN UNION (Dec. 12, 2022), https://eur-lex.europa.eu/EN/legal-content/summary/the-european-union-s-primary-law.html.

19 TFEU, *supra* note 17, art. 288; note that the scope of this contribution is limited to regulations and directives.

20 *Id*. art. 288(2).

21 *See, e.g.*, GDPR, *supra* note 9, art. 85-89, at 83-85.

opening clause and implement law that is more specific than the regulation itself.[22] Directives, on the other hand, are "binding, as to the result to be achieved, upon each Member State to which [they are] addressed, but shall leave to the national authorities the choice of forms and methods."[23] Thus, in the majority of cases directives are implemented via national legislation which must fulfil the directive's requirements. However, the directive can have direct effect if a Member State fails to transpose the directive by the end of the deadline and the directive's provisions are unconditional and sufficiently clear and precise.[24]

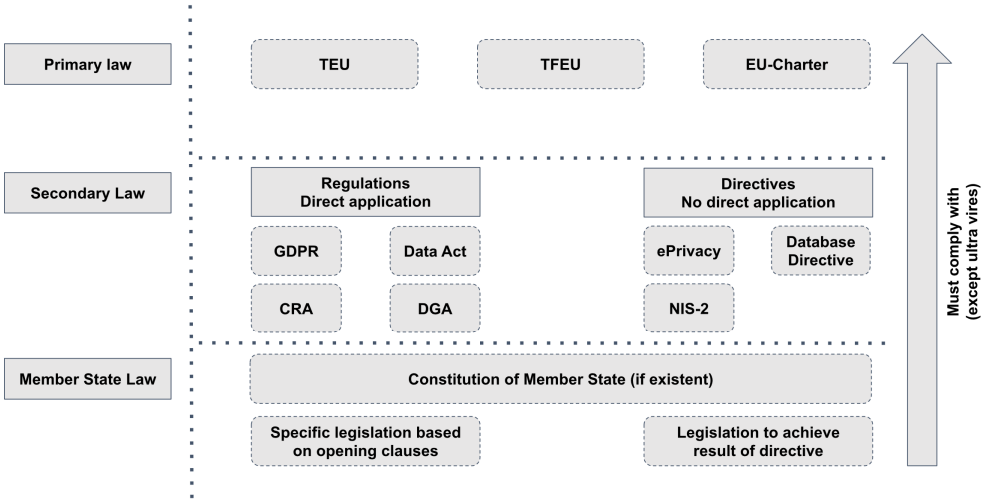

Figure 1: Legal System of the EU

22 Case C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums, ECLI:EU:C:2023:270, ¶75 (May 22, 2023).

23 TFEU, *supra* note 17, art. 288(3).

24 Case C-41/74, Yvonne van Duyn v Home Office, ECLI:EU:C:1974:133, ¶1352 (Dec. 4, 1974).

Another core aspect of the legal system is the principle of the primacy of EU law that has been developed over time through the case law of the Court of Justice of the European Union (CJEU) and which stipulates that where a conflict arises between Union law and a law of an EU Member State, the EU law will prevail.[25] However, as the EU derives its competences from the Member States, the German Federal Constitutional Court held that the constitutional organs of a Member State must counter an act of the EU that violates the constitutional identity or manifestly exceeds the competences transferred (so-called ultra vires).[26] Since there has not been a case of such violation so far, the actual legal implications remain unsolved.

2.2 Data Protection Law and the GDPR

A core aspect for the sharing of personal data is data protection law, in particular the GDPR. The processing of personal data entails risks for the fundamental rights of natural persons. The EU regulators addressed these risks enacting the Data Protection Directive[27] back in 1995. However, as a directive it

25 *See generally* Case 26/62, Van Gend en Loos v Nederlandse Administratie der Belastingen, ECLI: EU:C:1963:1, ¶16 (Feb. 5, 1963); Case 6/64, Costa v E.N.E.L., ECLI:EU:C:1964:66, ¶587-88 (July 15, 1964); Case 11/70, Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, ECLI:EU:C:1970:114, ¶1139 (Dec. 17, 1970); Case 106/77, Administrazione delle Finanze dello Stato v Simmenthal SpA, ECLI:EU:C:1978:49, ¶641, 643 (Mar. 9, 1978); Case C-106/89, Marleasing SA v La Comercial Internacional de Alimentacion SA, ECLI:EU:C:1990:395, ¶4160-61 (Nov. 13, 1990).

26 BVerfG, 2 BvR 2728/13, June 21, 2016, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/06/rs20160621_2bvr272813en.html; Case C-62/14, Peter Gauweiler and Others v Deutscher Bundestag, ECLI:EU:C:2015:400, ¶6-9 (June 16, 2015).

27 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 31.

was unable to achieve full harmonisation[28] and thus it was repealed when its successor – the GDPR – was enacted in 2016. The GDPR became a model for many data protection laws around the world, like the California Consumer Privacy Act.[29] Therefore, it has been described as the "gold standard of data protection, both at home and abroad."[30] The GDPR is based on Article 8 EU Charter and applies to the processing of personal data only.[31] However, the GDPR's definition of personal data is rather broad as it includes "any information relating to an identified or identifiable natural person"[32] where "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[33] An information relates to the data subject "where the information, by reason of its content, purpose or effect, is linked to a particular person."[34] Furthermore, it is not necessary that "all the information enabling the identification of the data subject must be in the hands of one person" if the person has means "likely reasonably be used in order to identify the data subject, with the assistance of other persons."[35] Thus, both static and dynamic IP addresses may constitute personal data and thus

28 GDPR, *supra* note 9, recital 9, at 2.

29 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199.

30 *The European Commission's Statement Ahead of the 5th Anniversary of the General Data Protection Regulation*, EUROPEAN UNION (May 24, 2023), https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2884.

31 GDPR, *supra* note 9, art. 2(1), at 32.

32 The so-called 'data subject', *see id*. art. 4(1), at 33.

33 *Id*.

34 Case C-434/16, Nowak v Data Protection Commissioner, ECLI:EU:C:2017:994, ¶34-35 (Dec. 20, 2017).

35 Case C-582/14, Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779, ¶31-49 (Oct. 19, 2016).

the GDPR could apply to their processing.[36] Furthermore, pursuant to the regulation for the free flow of non-personal data (FFR)[37] the GDPR applies where "personal and non-personal data in a data set are inextricably linked."[38]

The GDPR lays down rules relating to the protection of the natural persons fundamental right to data protection under Article 8 of the Charter of the European Union.[39] In parallel, it relates to the "free movement of personal data" as the "free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[40] However, the GDPR mainly contains provisions that are supposed to protect the fundamental rights and the freedom of natural persons. The GDPR differentiates between controllers and processors. A controller is a natural or legal person "which, alone or jointly with others, determines the purposes and means of the processing of personal data."[41] On the other hand, a processor is a "natural or legal person (...) which processes personal data on behalf of the controller."[42] If two or more controllers jointly determine the purposes and means of processing, they are joint controllers and must conclude an arrangement which determines their respective responsibilities for the compliance with the GDPR.[43] According to the case law of the CJEU, the threshold for a joint

36 *Id*. ¶49.

37 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on Framework for the Free Flow of Non-personal Data in the European Union, 2018 O.J. (L 303) 59 [hereinafter FFR].

38 *Id*. art. 2(2), at 65.

39 Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391-407.

40 GDPR, *supra* note 9, art. 1(3), at 32.

41 *Id*. art. 4(7), at 33.

42 *Id*. art. 4(8), at 33.

43 *Id*. art. 26(1), at 48.

controllership is rather low.[44] Controllers must be able to demonstrate a legal basis for the lawful processing of personal data, like the data subject's consent, a contract, or a legitimate interest.[45] Furthermore, they must provide certain rights to data subjects regarding the processing of their personal data, for example, the right of access[46] or the right to erasure.[47] For this purpose but for other purposes as well, transparency is key for both the data subjects and the controllers. Controllers who are unable to explain the relevant aspects of the processing of personal data simply cannot comply with the provisions of the GDPR.[48] Naturally, compliance with these rather strict transparency provisions under Articles 12-14 GDPR is challenging, especially in the context of complex processing of data like the training of machine learning algorithms.[49] In addition, controllers must implement technical and organisational measures to secure the processing of personal data and they are obliged to implement these measures prior to the processing and by default.[50]

In the context of data sharing, the controllers' obligation to provide data subjects their right to data portability is of particular significance.[51] This right

---

44 Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein v Wirtschaftsakademie SchleswigHolstein GmbH, ECLI:EU:C:2018:388, ¶44 (May 6, 2018); Case C-25/17, Tietosuojavaltuutettu v Jehovan todistaja uskonnollinen yhdyskunta, ECLI:EU:C:2018:551, ¶75 (Oct. 7, 2018); Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, ¶76-85 (July 29, 2019).

45 GDPR, *supra* note 9, art. 5(1)(a), (2), 6(1), at 35-36.

46 *Id*. art. 15, at 43.

47 *Id*. art. 17, at 43.

48 Especially *id*. art. 12-14, at 39-41.

49 Foresight Unit (STOA), Eur. Parliamentary Rsch. Serv., *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, at 32, 44, 53-56, PE 641.530 (June, 2020).

50 GDPR, *supra* note 9, art. 25, 32, at 48, 51.

51 *Id*. art. 20, at 45.

enables the data subject to "receive the personal data concerning him or her which he or she has provided to a controller, in a structured, commonly used and machine-readable format" and to "transmit those data to another controller without hindrance from the controller to which the personal data have been provided", subject to certain requirements.[52] At first glance, this right appears to be a powerful tool enabling the sharing of personal data. However, it is restricted to actively provided data and it suffers from the absence of harmonised standards providing a sufficient level of interoperability. As a result, its practical significance can be described as marginal at best.

Moreover, the provisions of the GDPR for the transfer of personal data to third countries are of utmost importance for the sharing of data within an international supply chain.[53] A transfer of personal data to a third country – a country outside of the European Economic Area (EEA), which consists of the EU Member States, Iceland, Liechtenstein, and Norway – may take place where the EC has issued a so-called adequacy decision, which attests that the third country ensures an adequate level of protection (see Figure 2).[54] So far the EC has issued such decisions for Andorra, Argentina, Canada (for commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (for commercial organisations only) and Uruguay.[55] In the absence of an adequacy decision, the transfer is subject to appropriate safeguards like standard data

52 *Id*. art. 20(1), at 45.

53 *Id*. art. 44-50, at 60-65.

54 *Id*. art. 45, at 61.

55 *Adequacy Decisions*, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Oct. 31, 2023).

protection clauses or binding corporate rules.[56] However, the CJEU has held that an "adequate level of protection" requires a level of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU.[57] Hence, it struck down successively two decisions of the EC in relation to the United States – the so-called "Safe Harbour Agreement" and the so-called "EU-US Privacy Shield".[58] Thus, the CJEU may strike down other adequacy decisions – especially the one regarding the United States[59] – if it deems the third country's level of protection as inadequate.

（續接次頁）

56 GDPR, *supra* note 9, art. 46, at 62.

57 Case C-362/14 Maximillian Schrems v Data Protection Commissioner, ECLI:EU: C:2015:650, ¶74-78 (Oct. 6, 2015); Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, ECLI: EU:C:2020:559, ¶129, 135 (July 16, 2020).

58 Case C-362/14 Maximillian Schrems v Data Protection Commissioner, ECLI:EU: C:2015:650, ¶107; Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, ECLI: EU:C:2020:559, ¶202, 203.

59 Commission Implementing Decision EU 2023/1795, of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data under the EU-US Data Privacy Framework, 2023 O.J. (L 231) 118.

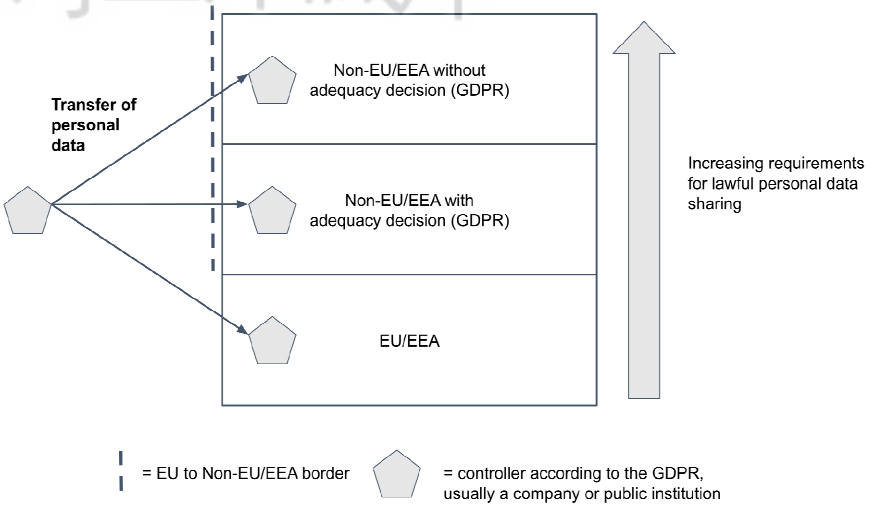

Figure 2: Transfer of Personal Data

Non-compliance with the provisions of the GDPR can lead quickly to undesired legal implications like a liability for damages or the imposition of administrative fines up to 20.000.000 EUR[60] or up to 4 % of the affected undertaking's total worldwide annual turnover of the preceding financial year.[61]

In summary, the GDPR primarily provides high safeguards for the protection of the data subjects' fundamental right to data protection. At the same time, it imposes many obligations on controllers, who must invest quite a lot of time and effort for the compliance with these obligations. Thus, it appears as the free movement of personal data falls short for the sake of high safeguards. As a consequence, despite the benefits of such high safeguards for the protection of fundamental rights, the GDPR has been criticised as severely hindering technical

60 Equals 690.058.800,00 686.075.094,60 New Taiwan Dollar (with a conversion rate of 1 EUR = 34,5030 TWD as of 31 October 2023) or 21.279.900,00 United States Dollar (with a conversion rate of 1 EUR = 1,06 USD as of 31 October 2023).

61 GDPR, *supra* note 9, art. 82, 83(4), 84, at 81-83.

innovations, like Artificial Intelligence (AI) systems or extensive data sharing mechanisms.[62] Furthermore, the data sharing mechanisms of the GDPR are devoid of practical significance since the main mechanism – the right to data portability – suffers from exuberant restrictions and the absence of harmonised standards for structured, commonly used, and machine-readable formats.[63]

2.3 ePrivacy Directive

In addition to the provisions of the GDPR, the sharing of data is somewhat affected by the ePrivacy Directive (ePD).[64] It is particularly relevant in scenarios where information is stored in or accessed from certain products. Although the ePD predominantly concerns the protection of privacy in the electronic communications sector, it provides further rules regulating other aspects of privacy. Thus, the scope of some of its provisions is extensive. This applies to Article 5(3) ePD as well, which is the only relevant provision for this analysis. It states, that "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information."[65] The interpretation of this provision is

62 Andreas Streim & Isabelle Stroot, *After 5 Years: GDPR Only Receives the Grade "Sufficient"*, BITKOM, https://www.bitkom.org/EN/List-and-detailpages/Press/5-years-GDPR-receives-grade-sufficient (last visited July 12, 2024).

63 Emmanuel Syrmoudis, Stefan Mager, Sophie Kuebler-Wachendorff, Paul Pizzinini, Jens Grossklags & Johann Kranz, *Data Portability Between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20*, 2021 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 351, 366 (2021).

64 Directive 2002/58/EC, of The European Parliament and of The Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37 [hereinafter ePD].

65 *Id*. art. 5(3), at 44.

ambiguous. However, according to a convincing position in the literature, Article 5(3) ePD shall protect the "integrity of terminal equipment".[66] Since the integrity of the terminal equipment is independent of the classification of the stored data as personal or non-personal, the user of terminal equipment shall be protected from third parties that may want to store information in the device or want to gain access to information already stored in the device. Therefore, Article 5(3) ePD states rather strict requirements for these actions.[67] There are only two exemptions to this rule, (1) if the sole purpose for the storage or access of the information regards the transmission of communication over an electronic communications network, or (2) if the storage or access is strictly necessary to provide an information society service explicitly requested by the user.[68] While the article is commonly associated with the implementation of the omnipresent Cookie-Banners on EU websites – and while it is the main reason for them[69] –, the word "terminal equipment" is understood much more broadly. Therefore, Article 5(3) ePD almost always has to be at least considered, when discussing Data Law and the CRA.

This processing of information regulated under Article 5(3) ePD often involves personal data. This raises the question how Article 5(3) ePD relates to the

66 See *Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive. Adopted on 14 November 2023*, EUROPEAN DATA PROTECTION BOARD, https://www.edpb.europa.eu/system/files/2023-11/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_en.pdf (last visited July 12, 2024).

67 This is especially true if one compares these requirements with the requirements of the GDPR for the lawfulness of the processing of personal data, which unlike the directive for example include the possibility for weighing and balancing interests of the processor and the data subject, *see* GDPR, *supra* note 9, art. 6(1)(f), at 36.

68 *See* ePD, *supra* note 64, art. 5(3), at 44.

69 Other reasons however include the possible transfer of data outside of the EU and extensive data processing that requires consent. However, even the most "privacy-friendly" cookies, that are not strictly necessary to provide an information society service, can only be implemented via consent, *see* ePD, *supra* note 64, art. 5(3), at 44.

GDPR. While Article 95 GDPR is supposed to clarify this relationship, its wording is ambiguous, resulting in an ongoing discussion among scholars in European literature.[70] One of the reasons is that Article 95 GDPR stipulates that the GDPR does not impose additional obligations if the obligations of the GDPR and the ePD have "the same objective".[71] However, it is not entirely clear what kind of objective each obligation pursues and thus, while some approaches for a solution of this relationship have been suggested, the relationship between the GDPR and the ePD remains ultimately undetermined.[72] Another reason for this ambiguity is to some extent historical. During the legislative process of the GDPR, the EU originally intended to revise the ePD by adopting an ePrivacy Regulation.[73] As a consequence, the ePrivacy Regulation and the GDPR would have applied from the same date onwards. However, until now, the EU could not agree on this legislative act.[74] Therefore, up to this point, an ePrivacy Regulation does not exist and it is not clear whether it will be adopted in the near future, further delaying the possible clarification of the relation between Article 5(3) ePD and the GDPR.

2.4 Implications of Intellectual Property and Trade Secret Law

Despite the economic importance of digital data, the EU's current legal framework is devoid of any explicit property law status for data.[75] For personal

---

70 Piedade Costa de Oliveira, *Article 95 Relationship with Directive 2002/58/EC*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 1294, 1297 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., 2020).

71 *Id*.

72 *Id*.

73 *Id*. at 1299.

74 *Id*. at 1300.

75 Simon Geiregat, *The Data Act: Start of a New Era for Data Ownership?* 4 (Ghent Univ., Working Paper, 2022), https://dx.doi.org/10.2139/ssrn.4214704.

data the GDPR provides certain rights to the data subject but these do not exist in the current legal framework for the majority of non-personal data.[76] In the absence of both data ownership and rights for non-personal data, the data holders seek to protect non-personal data through intellectual property law and trade secret law.[77]

For data – especially machine-generated data – the majority of the provisions of copyright protection often do not apply as the data often lack the criterion of "originality".[78] This criterion is key for the protection of a work under EU copyright law and requires that the work is the "author's own intellectual creation".[79] As a consequence, the Database Directive[80] introduced a *sui generis* right for the protection of databases. The threshold to protect a database can be described as rather low[81] because it protects the "maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part,

76 Wolfgang Kerber, *Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives*, 72 GRUR INT. 120, 122 (2023).

77 Peter Georg Picht & Heiko Richter, *EU Digital Regulation 2022: Data Desiderata*, 71 GRUR INT. 395, 401 (2023).

78 Enrico Bonadio, Nicola Lucchi & Giuseppe Mazziotti, *Will Technology-Aided Creativity Force Us to Rethink Copyright's Fundamentals? Highlights from the Platform Economy and Artificial Intelligence*, 53 IIC 1174, 1188 (2022).

79 See for more information and a summary of the relevant case law: Daniel Inguanez, *A Refined Approach to Originality in EU Copyright Law in Light of the ECJ's Recent Copyright/Design Cumulation Case Law*, 51 IIC 797 (2020).

80 Directive 96/9/EC, of The European Parliament and of The Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20 [hereinafter Database Directive].

81 Josef Drexl et al., *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)* 98 (Max Planck Inst. for Innovation & Competition Rsch. Paper No. 22-05, 2022), https://dx.doi.org/10.2139/ssrn.4136484.

evaluated qualitatively and/or quantitatively, of the contents of that database."[82] However, the right is subject to the criterion of "originality" as well since for copyright protection the database must, "by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation."[83] Despite the CJEU's clarification that the author's "labour and skill" are irrelevant for the determination of copyright,[84] the concept of "creative choice" may allow a broad interpretation of the scope of protection.[85] As a consequence, certain data and also data generated by machines could be protected as a database if the arrangement of the data in a dataset is derived from some sort of personal creativity.[86] Therefore, it depends on the stakeholder's creativity in the investment of data which ultimately leads to legal uncertainties; especially in distributed data networks with multiple stakeholders.[87]

Furthermore, data can be protected if they constitute a trade secret under the Trade Secret Directive.[88] In order to achieve such protection, the data must be kept secret and have commercial value as a consequence of such secrecy.[89] However,

82 Database Directive, *supra* note 80, art. 7(1), at 25.

83 *Id*. art. 3(1), at 25.

84 Case C-604/10, Football Dataco Ltd and others v Yahoo! UK Ltd and others, ECLI:EU: C:2012:115, ¶42 (Mar. 1, 2012).

85 Drexl et al., *supra* note 81.

86 *Id*.

87 Andreas Wiebe, *The Data Act Proposal—Access Rights at the Intersection with Database Rights and Trade Secret Protection*, 72 GRUR INT. 227, 229 (2023).

88 Directive (EU) 2016/943, of The European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) against their Unlawful Acquisition, Use and Disclosure (Trade Secret Directive), 2016 O.J. (L 157) 1 [hereinafter Trade Secret Directive]; *id*. at 232.

89 Trade Secret Directive, *id*. art. 2, at 9.

the trade secret prevents certain acts only, like the use or disclosure of trade secrets,[90] and in addition is subject to specific exceptions.[91]

2.5 Implications of the Data Governance Act and the Digital Markets Act

Furthermore, the DGA[92] and the Digital Markets Act (DMA)[93] are rather recently enacted regulations that must be considered for the sharing of both non-personal and personal data. The DGA introduced basic requirements for data governance in order to develop further the borderless digital internal market.[94] Amongst other things, it lays down conditions for the re-use of certain categories of data held by public sector bodies, a framework for so-called data intermediation services, and the establishment of the European Data Innovation Board.[95] However, the DGA does not directly address the sharing of data within the private sector as it is devoid of any rights to access, obligations to share data, or obligations to ensure interoperability.

Furthermore, the DMA has been enacted to break up the considerable economic power of large undertakings providing a core platform service and whose position is difficult to challenge for other market operators to an extent that increases the likelihood of the underlying market's dysfunction.[96] For this

90 *See id*. art. 4, at 10.

91 *Id*. art. 5, at 11.

92 *See* DGA, *supra* note 7, recital 3, at 3.

93 Commission Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2021 O.J. (L 265) 1 [hereinafter DMA].

94 DGA, *supra* note 7, recital 3, at 3.

95 *Id*. art. 1(1), at 18.

96 DMA, *supra* note 93, recital 3, art. 3(1), at 2, 30.

purpose, the EC can designate certain undertakings as a so-called "gatekeeper".[97] As a consequence, the designated gatekeepers must fulfil several obligations which shall prevent the abuse of their economic powers like the prohibition to combine or cross-use personal data from other core platforms or services provided by the gatekeeper.[98] On 6 September 2023, the EC designated twenty-two core platform services of six gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft.[99] Despite the DMA's restriction of the economic power of these undertakings, it does not provide any rights for other undertakings or stakeholders to access the data generated by these gatekeepers. In the absence of such rights, these undertakings are still able maintain full control over the data generated through their core services.

2.6 The Current Legal Framework's Shortcomings for Data Sharing

The implications of the different regulations that are outlined above reveal several shortcomings. The current legal framework of the EU is heavily influenced by the distinction between personal and non-personal data. Whilst the GDPR provides certain rules for the sharing of personal data, these rules simply do not exist for non-personal data. Furthermore, the protection of non-personal data is rather difficult since intellectual property law and trade secret law are limited in both their scope of application and the protection they provide. This absence of a coherent legal framework for the protection and the sharing of non-personal data within the EU disincentivises undertakings to share their data – since it entails economical and legal risks. In addition, manufacturers are incentivised to exercise

97 *Id*. art. 3, 4, at 30-33.

98 *Id*. art. 5-13, at 33-42.

99 *Digital Markets Act: Commission Designates Six Gatekeepers*, EUROPEAN COMMISSION (Sept. 6, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.

control over the data and gain competitive advantages by designing products without an access to the data generated by the use of the products. Furthermore, large undertakings can abuse their exclusive control over a vast amount of both personal and non-personal data, which negatively affects data economy since it hampers the competition between companies. In parallel, the lack of interoperability – as a consequence of the absence of common data sharing procedures and standards – hinders the sharing of personal data, too. In conclusion, it becomes apparent that the shortcomings of the current legal framework do not prevent market failures but rather incentivises them.

2.7 The Current Cybersecurity Framework

In December 2020, the EU Commission presented a new EU Cybersecurity Strategy, which is supposed to "bolster Europe's collective resilience against cyber threats."[100] Similar to other reports, the EU Agency for Cybersecurity identified the most relevant cyber threats in the EU between 2021 and 2022.[101] The biggest threats include ransomware attacks as well as attacks that are based on vulnerabilities in the supply chain of organisations. Interestingly for this analysis, "supply chain incidents accounted for 17% of intrusions in 2021 compared to less than 1% in 2020."[102] Subsequent to the Cybersecurity Strategy, the EU adopted various legal acts to address these cybersecurity threats. These acts include the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive),[103] the Directive on the resilience of critical entities (CER-

100 *New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient*, EUROPEAN COMMISSION (Dec. 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

101 *Top Cyber Threats in the EU*, *supra* note 12.

102 *Id*.

103 Directive (EU) 2022/2555, of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union,

Directive),[104] the Regulation on digital operational resilience for the financial sector (Digital Operation Resilience Act, DORA)[105] or a Commission Delegated Regulation supplementing the Radio Equipment Directive (RED).[106]

Regarding the existing legislation, mainly the NIS 2 Directive is relevant for this analysis. The Directive addresses so-called "essential" or "important" entities, which in general means that these public or private entities at least reach a certain size and are of a type referred to in the Annex I or II of the Directive.[107] There, the Directive defines sectors of high criticality (like energy, transport, health, digital infrastructure) and "other critical sectors" (like digital providers or the production/manufacturing of chemicals, food, medical devices, motor vehicles, etc.).[108] These entities have to implement appropriate and proportionate

Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022 O.J. (L 333) 80 [hereinafter NIS 2 Directive].

104 Directive (EU) 2022/2557, of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC, 2022 O.J. (L 333) 164.

105 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, 2022 O.J. (L 333) 1.

106 Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive; Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the Harmonisation of the Laws of the Member States Relating to the Making Available on the Market of Radio Equipment and Repealing Directive 1999/5/EC, 2014 O.J. (L 153) 6.

107 NIS 2 Directive, *supra* note 103, art. 3, at 127.

108 *Id*. Annex I, II, at 143-49.

cybersecurity measures.[109] Therefore, they have to assess the risk and take into account some other criteria (like the state-of-the-art and the cost of implementation) to lawfully select the measures that have to be implemented.[110] The measures also have to address supply chain security; there are some additional regulations for critical supply chains.[111] Moreover, the NIS 2 Directive requires Member States of the EU to adopt a national cybersecurity strategy, which, inter alia, must include policies that address cybersecurity in the supply chain for information and communication technology products.[112] Furthermore, the Directive establishes a European Cooperation Group which is supposed to facilitate and support strategic cooperation and the exchange of information among Member states.[113] This Cooperation Group has to carry out different tasks to achieve this goal, including a coordinated security risk assessment of critical supply chains.[114] This shows the importance of supply chain security as it is viewed by the European legislator. Especially the requirement for addressed entities to provide supply chain security will also influence entities outside of the EU, as the addressed entities are required to provide security "concerning the relationships between each entity and its direct suppliers or service providers."[115]

Adding to these regulations there are other proposals addressing cybersecurity which are currently debated and will have effects on supply chains and possibly data sharing therein, like the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements Cyber Resilience Act (CRA).[116]

---

109 *Id*. art. 21(1), at 127.
110 *Id*.
111 *See id*. art. 21(3), 22, at 127-28.
112 *Id*. art. 7(2)(a), at 115.
113 *Id*. art. 14(1), at 121.
114 *Id*. art. 14(4)(i), at 121.
115 *Id*. art. 21(2)(d), at 127.
116 *Proposal for a Regulation of the European Parliament and of the Council on Horizontal*

This proposal is supposed to strengthen the cybersecurity of these products in the EU and will be analysed further in IV.

3. IMPLICATIONS OF THE DA

This part gives an overview of the implications of the upcoming Data Act. For this purpose, it describes the goals of the DA and subsequently outlines the provisions for the sharing of data generated by the use of so-called connected products and related services (section 1). Finally, it assesses the implications of the DA (section 2).

3.1 Overview of the Proposal

The EC published its proposal for a Data Act in February 2022.[117] Since its publication, several amendments of the proposal have been suggested until the Commission, the European Parliament and the Council eventually agreed upon a version as a result of the so-called "trilogue".[118] It is likely that this version will enter into force by the end of autumn 2023 and will be subject to some editorial

Cybersecurity Requirements or Products with Digital Elements and Amending Regulation (EU) 2019/1020, COM (2022) 454 final (Sept. 15, 2022) [hereinafter *CRA*].

117 *DA-P*, *supra* note 6, at 1.

118 *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017 /2394 and Directive (EU) 2020/1828 (Data Act)*, 2022/0047 COD (July 14, 2023) [hereinafter *DA-Tri*]. The so-called "trilogue" is an "informal interinstitutional negotiation" between the European Commission, the European Parliament, and the Council of the European Union. Its aim is "to reach a provisional agreement on a legislative proposal that is acceptable to both the Parliament and the Council" but the agreement must subsequently be adopted through formal procedures. *See Trilogue*, EUROPEAN UNION, https://eur-lex.europa.eu/EN/legal-content/glossary/trilogue.html (last visited Oct. 31, 2023).

changes only.[119] Since the bodies of the European Union have not published a revised final version yet,[120] this contribution refers to both the provisions of the Commission's proposal (DA-P) and the recently published amended provisions as a result of the trilogue (DA-Tri). According to the Commission's proposal, the DA regulates the users' access to data generated by their use of a product or a related service. It addresses the access of data recipients (third parties which receive the data) to this data, too.[121] In this way, it shall empower users and strengthen their control over the data generated by their use of a product whilst making data available to other businesses but at the same time preserving incentives for companies to invest in the generation of data.[122] In parallel, the DA shall facilitate the switching between data processing services and shall provide rules for the "development of interoperability standards for data to be accessed, transferred and used."[123] Furthermore, it addresses the access to data of public sector bodies in a case of an "exceptional need",[124] which – for the sake of conciseness – will not be addressed by this contribution.[125]

---

119 Whilst this was true when the authors submitted this article, please note that as of 22 December 2023 the final version of the Data Act was published in the Official Journal of the European Union, *see* Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), O.J. (L). As predicted, the differences are limited to editorial changes, like relocating some paragraphs, without a significant change of the content. Therefore, the following statements are, to this extent, still up to date.

120 *Id*.

121 *DA-P*, *supra* note 6, at 37-38.

122 Kerber, *supra* note 76.

123 *DA-Tri*, *supra* note 118, at 56.

124 *DA-P*, *supra* note 6, at 48-52.

125 *See generally* Angelica Fernandez, *The Data Act: The Next Step in Moving Forward to a European Data Space*, 8 EUR. DATA PROT. L. REV. 108 (2022).

The provisions of the DA shall reflect the "proliferation in products connected to the Internet of Things" (IoT) which increased the volume of high quality data generated from different domains that "may potentially be used and reused for a variety of purposes and to an unlimited degree, without any loss in its quality or quantity."[126] For this purpose, the DA introduces various provisions to incentivise and facilitate the sharing of this kind of data.

3.1.1 Access to Data Generated by a Connected Product or a Related Service

The decisive factor for the application of the DA's provisions for the access to data generated by use is whether it is generated by a "connected product" or a "related service".[127] In contrast to the GDPR, the DA defines data as "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"[128] and covers both personal and non-personal data.[129]

According to the provisions of the DA, connected product means "an item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate product data via an electronic communications service, a physical, connection or on-device access and whose primary function is not the storing, processing or transmission of data on behalf of third parties, other than the user."[130] The EC's proposal clarified that the restriction of this definition shall exempt, for example, "personal computers, servers, tablets and smart phones, cameras, webcams, and sound recording systems and text scanners" as they require

126 *DA-P*, *supra* note 6, at 17.
127 *DA-Tri*, *supra* note 118, at 56.
128 *Id*. at 59.
129 *Id*. at 56.
130 *Id*. at 60.

human input to generate data.[131] This delineation has been criticised as rather unclear[132] and it is no longer a part of the DA in the trilogue version.[133] However, despite its removal in the final version, it could still serve as an indication of the extent of the definition's restriction since an alternative provision is absent.

The term "data generated by the use", on the other hand, is rather extensive and covers raw data, meaning "product data which are not substantially modified" as well as "data having been pre-processed for the purpose of making it understandable and usable prior to further processing and analysis."[134] However, this does not pose an obligation on the data holder to "make substantial investments in cleaning and transforming the data."[135] Furthermore, the term does not cover information derived from the raw data, unless "agreed otherwise between the user and the data holder."[136] The DA clarifies that this "could include, in particular, information derived by means of sensor fusion."[137]

Related service, on the other hand, means "a digital service other than an electronic communications service, including software, which is connected with the product at the time of the purchase in such a way that its absence would prevent the product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the product."[138] It does not cover services that do not

131 *DA-P*, *supra* note 6, at 20.
132 Moritz Hennemann, Gordian Ebner & Benedikt Karsten, *The Data Act Proposal: Literature Review and Critical Analysis* 21 (Univ. of Passau IRDG Rsch. Paper Series No. 23-01, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4360961.
133 *See DA-Tri*, *supra* note 118, at 9.
134 *Id*. at 8.
135 *Id*.
136 *Id*. at 9.
137 *Id*.
138 *Id*. at 60.

impact the operation of the connected product and do not involve the transmitting of data or commands to the product by the service provider.[139] The DA also applies to related services that are provided by a third party – meaning a party that is not a seller, rentor, or lessor.[140] However, the supply of the connectivity and the power supply are not related services under the DA.[141]

3.1.2 Territorial Scope of the DA

The provisions of the DA combine the personal scope with the territorial scope.[142] Similar to the GDPR, the DA does not apply solely to actors within the EU but to non-EU actors, as well. The territorial scope of the DA-P includes – amongst other actors – "manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services"[143], to "data holders that make data available to data recipients in the Union"[144], and data recipients in the Union to whom data are made available."[145] The DA-Tri further specifies the territorial scope and emphasises that the DA shall apply to "manufacturers of connected products and providers of related services placed on the market in the Union, *irrespective of the establishment*"[146], "users of such connected products or related services in the Union"[147], "data holders, *irrespective of their place of establishment*, that make data available to data recipients in the

139 *Id*. at 10.
140 *Id*.
141 *Id*.
142 *See DA-P*, *supra* note 6, at 37; Hennemann et al., *supra* note 132, at 12.
143 *DA-P*, *supra* note 6, at 38.
144 *Id*.
145 *Id*.
146 *DA-Tri*, *supra* note 118, at 57; emphasis added by the authors.
147 *Id*.

Union"[148] and "data recipients in the Union to whom data are made available."[149] Therefore, non-EU manufacturers and providers must design their connected products and related services in accordance with the provisions of the DA if they intend to place the product on the market in the Union. In addition, non-EU actors fall within the territorial scope of the DA if they are data holders pursuant to the provisions of the DA.

3.1.3 Main Actors

The DA differentiates between three different actors for the sharing of data generated by a connected product or a related service: (1) the user, (2) the data holder, and (3) the data recipient.

3.1.3.1 User

The DA-Tri defines a "user" as a "natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services."[150] This definition is ambiguous and despite the subsequent amendments many legal issues in a case of multiple potential users remain unsolved. According to a recital of the DA multiple potential entities can be equally considered as users, for example, the owner, renter or lessee of a product.[151] However, it remains unclear whether ownership and the contractual basis are the sole decisive factors or whether a factual situation like possession may classify an entity as a user, too.[152] In addition, it remains unclear whether actors equally considered to be users shall have full access to the data generated by the use of the product – regardless of the

148 *Id*.; emphasis added by the authors.
149 *Id*.
150 *Id*. at 61.
151 *Id*. at 10.
152 Hennemann et al., *supra* note 132, at 22.

different degrees of risks they bear and their potentially varying interests in the different formats of data generated. The different degrees of contribution and interests are acknowledged by the DA[153] but not further addressed.[154]

3.1.3.2 Data Holder

In contrast to a user, a data holder is "a legal or natural person who has the right or obligation, in accordance with [the DA], applicable Union law or national legislation implementing Union law, to use and make available data, including where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service."[155] Prior versions of the DA further identified a data holder as a legal or natural person who "can enable access to the data through control of the technical design or means of access, in the case of non-personal data"[156] but this has been removed during the trilogue. Despite several amendments of this definition, it remains vague and its impact is unforeseeable as far as the obligation to use and make data available is concerned (since the determination of such obligation according to the DA depends on the classification as data holder). Thus, the determination of a data holder through the obligations of the DA is an example of circular reasoning. However, the right to use and make data available could be determined through either the factual ability to make data available or contractual obligations. Although the latter could lead to circular reasoning as well if the contractual obligation itself depends on the definition of a data holder, too. Ultimately, it becomes apparent from the recitals and the purpose of the DA that natural or legal persons have to be classified

153 *See DA-Tri*, *supra* note 118, at 10.

154 *Id*. at 12-13.

155 *Id*. at 61.

156 *See Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)—Third Presidency Compromise Text*, at 41, 2022/0047(COD) (Dec. 8, 2022).

as data holders if they are able – either by legal or factual means – to make data available to the user.[157]

Furthermore, the legal implications in a case of multiple data holders remain unclear since – unlike the GDPR and its joint controllership – the DA does not provide any rules or guidance for this scenario. However, the recitals of the DA state that in a case of several manufacturers or related service providers, the "user should turn to each of the parties with whom it has a contractual agreement."[158] This indicates that the provisions of the DA shall not be applied similar to a joint controllership but rather shall be based on the contractual obligations only.

Lastly, the obligations of the DA do not apply to data holders that qualify as micro or small enterprises – enterprises which employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed 10.000.000 Euro[159] – or to medium enterprises which surpassed this threshold less than a year ago.[160]

3.1.3.3 Data Recipient

Finally, the term "data recipient" refers to "a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or a related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national

157 *See* Nils Wiedemann, Thorsten Conrad & Simone Salemi, *Bereitstellung von Daten nach dem Data Act—Offene Fragen und verbleibende Probleme*, 27 K&R 157, 159 (2024).

158 *DA-Tri*, *supra* note 118, at 12.

159 Commission Recommendation of 6 May 2003 Concerning the Definition of Micro, Small and Medium-sized Enterprises, annex, art. 2, 2003 O.J. (L 124) 36, 39.

160 *DA-Tri*, *supra* note 118, at 73.

legislation implementing Union law."[161] The users' sharing of non-personal data can occur for both commercial and non-commercial purposes.[162]

3.1.4 Data Sharing

The DA includes several different chapters that regulate the access to and the sharing of data. Chapter 2 of the DA regulates the user's access to data generated by the use of connected products.

3.1.4.1 Access of the User to Data and Sharing of Data with Third Parties

For the purpose of sharing data generated by the use of connected products and related services, the DA stipulates the obligation of "access by default" and thus the obligation to design connected products and to provide related services in such way that the data, "including the relevant metadata necessary to interpret and use the data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly use and machine-readable format, and, where relevant and technically feasible, directly accessible to the user."[163] Furthermore, the user must receive certain information regarding the connected product or the related service.[164]

However, where data cannot be directly accessed by the user, the user can request access to readily available data and the relevant metadata "without undue delay, easily, securely and in a comprehensive, structured commonly used and machine-readable format, free of charge and, where relevant and technically feasible, of the same quality as is available to the data holder continuously and in real-time."[165] The similarities between the right to access pursuant to the DA and

---

161 *Id*. at 61.
162 *Id*. at 16.
163 *Id*. at 64.
164 *Id*. at 64-66.
165 *Id*. at 66.

the right to data portability under the GDPR are obvious as the DA's right builds upon the right to data portability of the GDPR.[166] For this reason, the right to access under the DA complements the right to access and the right to data portability of the GDPR.[167] As a result, the provisions of the DA for the access to data generated by products replace the provisions of the GDPR so far as they go beyond the scope of the GDPR's rights or are independent of certain restrictions (for example, compared to the right to data portability).[168] However, if the provisions of the DA would diminish the rights of the GDPR, the GDPR would prevail.[169] On the other hand, the DA precludes the user from using the data obtained for the development of competing products.[170]

The user is further entitled to share the data with third parties (data recipients) under the same conditions as their own access[171] with the exception that the data holder is entitled to request compensation from the data recipient for the sharing of the data in accordance with the provisions of the DA.[172] However, the absence of an agreement between the data holder and the third party does not hinder the transmission of personal data based on the right to data portability since the rights of the GDPR must prevail.[173] In parallel, the sharing of personal data depends on a legal basis, which is particularly relevant where the user is not the data subject.[174] Furthermore, designated gatekeepers – in accordance with the

166 Clément Perarnaud & Rosanna Fanni, *The EU Data Act: Towards a New European Data Revolution?*, CEPS POL'Y INSIGHTS, No. 2022-05, Mar. 2022, at 4.
167 *DA-Tri*, *supra* note 118, at 58.
168 *Id*. at 22.
169 *Id*. at 58.
170 *Id*.
171 *Id*. at 69.
172 *Id*. at 69, 74-76.
173 *Id*. at 70.
174 *Id*.

provisions of the DMA[175] – are ineligible third parties and therefore cannot receive data from a user obtained through the provisions of the DA.[176]

3.1.4.2 Trade Secrets and Intellectual Property Law

The provisions of the DA reflect the current legal framework's protection of non-personal data through trade secret law and intellectual property law. It stipulates that trade secrets should be preserved and that the user's access to data is restricted as far as the protection of trade secrets is endangered.[177] As a result, in order to obtain the data, the user must implement sufficient measures to preserve the confidentiality of the shared data. The data holder can withhold the data if the user fails to implement these measures or if the data holder is "highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisation measures taken by the user."[178] However, the data holder must substantiate the decision and notify the competent authority while the user can challenge the data holder's decision.[179] The same protection of trade secrets applies for the sharing of data with a third party.[180]

In the context of intellectual property law and copyright protection, the DA stipulates that the *sui generis* right for the protection of databases shall not apply to data generated by a connected product or a related service if it falls within the scope of the DA.[181] This provision applies in particular for the user's access to and sharing of data.[182] As a consequence, the DA eradicates a majority of the above-mentioned legal uncertainties regarding the protection of databases – but

175 *See* the above mentioned implications of the DMA.
176 *DA-Tri*, *supra* note 118, at 70.
177 *Id*. at 67.
178 *Id*. at 67-68.
179 *Id*. at 68.
180 *Id*. at 70-71.
181 *Id*. at 119.
182 *Id*.

shortcomings remain.[183] However, the DA does not preclude measures based on applicable copyright protection, for example, for literary works.[184、185]

3.1.4.3 Contractual Agreements as a Basis of Data Sharing

In stark contrast to the provisions of the GDPR for the right to data portability, the provisions of the DA build on contractual agreements between the different parties for the processing and sharing of data.[186] As a result, the data holder can only use non-personal data on the basis of a contractual agreement with the user.[187] In addition, the data holder and user can agree contractually on restricting or prohibiting the access, use or further sharing of data but only if the processing would undermine the security requirements of the product, thus creating "adverse effects on the health, safety or security of human beings."[188] However, the DA does not further address the implications of contract law and it is likely that the parties will have to resort to Union law or national contract law in addition. Moreover, the data recipient can only process the data obtained from the user on the basis of a contractual agreement and must delete the data if the agreed purpose is fulfilled, unless otherwise agreed contractually.[189] In parallel, the data holder and the data recipient shall agree on the modalities of the data sharing through a

183 See for these shortcomings: Wiebe, *supra* note 87, at 231; Estelle Derclaye & Martin Husovec, *Why the Sui Generis Database Clause in the Data Act Is Counter-productive and How to Improve It?*, SSRN (2022), https://dx.doi.org/10.2139/ssrn.4052390.

184 Directive 2001/29/EC, of The European Parliament and of The Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2002 O.J. (L 167) 10, 16 [hereinafter HCRIC].

185 Drexl et al., *supra* note 81.

186 Kerber, *supra* note 76, at 123.

187 *DA-Tri*, *supra* note 118, at 68-69.

188 *Id*. at 66.

189 *Id*. at 72.

contractual agreement, too.[190] In order to ensure fairness between the parties, the DA prohibits unfair contractual terms related to data access and use between enterprises.[191] However, this prohibition does not apply between enterprises and consumers since the latter are already protected under EU consumer law.[192]

3.1.4.4 Summary of the Sharing of Data Generated by Products

In summary, the provisions of the DA provide a user-centric sharing of data generated by connected products or related services, which is based on contractual agreements between the different parties. This is visualised in Figure 3.

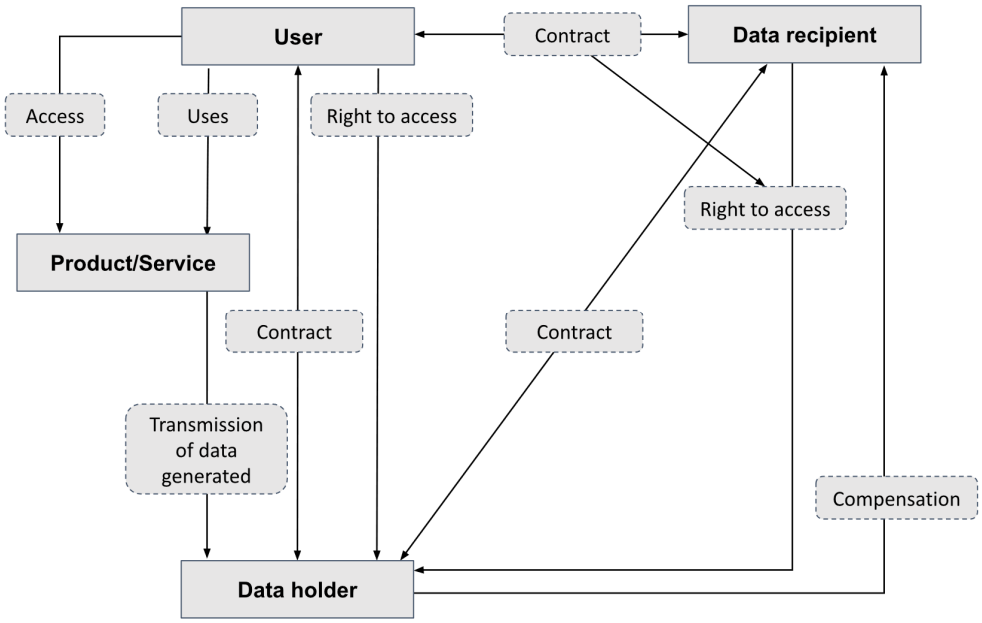

Figure 3: Access to and Sharing of Data Pursuant to the Provisions of the Data Act

190 *Id*. at 74.
191 *Id*. at 80-82.
192 *Id*. at 17.

3.1.5 Horizontal Rules and Common European Data Spaces

The DA's provisions are intended to be "horizontal" (cross-sectoral and not sector-specific) and therefore they shall be followed by "sectoral legislation to account for the specific situations of the respective sectors."[193] For this purpose, the European Union intends to implement several "Common European Data Spaces" with such sectoral legislation in sectors like health, agriculture, mobility, green deal but also in the sector of industry and manufacturing.[194] This sectoral legislation will likely include more specific provisions for contracts, licences, and access rights, which may facilitate the processing of data protected under Union law, too.[195] The first proposal for such a sector-specific regulation concerns the processing of electronic health data – the European Health Data Space (EHDS).[196] It enables, for example, the processing of electronic health data for the development of AI systems[197] while – at the same – stipulating the data holders' obligation to make available electronic health data for such "legitimate purposes".[198] However, the EU's ultimate goal is to ensure interoperability between Common European Data Spaces of the same or different sectors in order to enable efficient data sharing and thus the DA empowers the EC to enact harmonised standards.[199] Furthermore, the Common European Data Spaces shall be open to international stakeholders if they adhere to EU law.[200]

---

193 *Id*. at 4.

194 *Building a Data Economy—Brochure*, EUROPEAN COMMISSION, https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure#Strategy (last visited Oct. 31, 2023).

195 *See European Data Strategy*, *supra* note 5.

196 *Proposal for Regulation of the European Parliament and of the Council on the European Health Data Space*, COM (2022) 197 final (Mar. 5, 2022).

197 *Id*. at 70.

198 *Id*. at 68.

199 *DA-Tri*, *supra* note 118, at 103-06.

200 *Commission Staff Working Document on Common European Data Spaces*, at 4-6, SWD

3.2 Overall Implications of the Provisions

The DA's provisions for access to and sharing of data will likely allow an unprecedented sharing of data generated by connected products and related services. In this way it provides the users a negotiating power and extends the DMA in the context of gatekeepers.[201] However, the DA's provisions are built upon the right to data portability of the GDPR and thus are prone to the same weaknesses. Despite the EU's efforts to reduce the legal obstacles of the DA's right to access and to share data, the practical issue of a lack of interoperability – due to an absence of harmonised standards for common machine-readable formats in many sectors – may decisively hamper the sharing of data as envisaged by the DA. However, the EC's ability to implement harmonised standards for the interoperability in the context of Common European Data Spaces may eventually alleviate this situation.

4. IMPLICATIONS OF THE CRA

This section first outlines the proposal of the CRA (section 1) and then describes the impact of certain provisions (section 2).

4.1 Overview of the Proposal

Regarding the supply chain scenario analysed here, mainly the proposed Cyber Resilience Act (CRA)[202] is relevant. While the EU framework prior to the CRA already covered certain aspects, the CRA, as a horizontal (cross-sectoral) regulation, is supposed to ensure a higher security of hardware and software

(2022) 45 final (Feb. 23, 2022).

201 Picht & Richter, *supra* note 77, at 402.

202 *CRA*, *supra* note 116.

products in the Union.[203] It therefore introduces mandatory cybersecurity requirements for products with digital elements, placing responsibility on the manufacturer but along the supply chain (on importers and distributors), too.[204] The proposal stipulates that manufactures have to ensure that when placing a product with digital elements on the market, the product has to be designed, developed and produced in accordance with the essential cybersecurity requirements set out in Section 1 of Annex 1 of the proposal.[205] In order to comply with this obligation, manufacturers have to assess the cybersecurity risk associated with their product.[206] This risk assessment has to be included in the technical documentation.[207] If manufacturers integrate components sourced from third parties, they are obliged to exercise due diligence and have to ensure that the components do not compromise the security of the product with digital elements.[208] This outlines the holistic approach the CRA takes to the cybersecurity level of products with digital elements. Similar, adjusted obligations are regulated for importers and distributors of these products.[209]

4.2 Overall Implications of the Provisions

First, in order to illustrate the implications of the cybersecurity obligations set out in the CRA, this contribution outlines to which extent the CRA shall be

203 *See Cyber Resilience Act Factsheet*, EUROPEAN COMMISSION (Dec. 1, 2023), https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

204 Yannick Zirnstein, *Better Cybersecurity Due to Increased Regulation? The Final European Cyber Resilience Act—The First Comprehensive, Horizontally Applicable Approach for More Cybersecurity in Digital Products*, 25 COMPUTER L. REV. INT'L 65, 65-67 (2024).

205 *CRA*, *supra* note 116, at 38.

206 *Id*.

207 *Id*.

208 *Id*. at 39.

209 *Id*. at 42-43.

applicable, according to the current draft. The regulation applies to products with digital elements.[210] However, the definition of this term is quite broad. While there are some exemptions for products that are regulated by more specific legislation – like certain medical devices[211] – the CRA addresses, in general, "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately."[212] The term "remote data processing" essentially addresses data processing at a distance, which is essential for at least one of the functions of the product.[213]

Beside this first layer of regulation, the CRA further defines certain products with digital elements as critical products. These are subject to a more strict assessment or examination procedure.[214] As specified in Annex III of the CRA, critical products include, for example, certain security software, microprocessors, microcontrollers, industrial automation & control systems, secure elements, hardware security models and secure cryptoprocessors, certain robot components and controllers, smart meters and other IIoT devices.[215] Apart from these product categories, the CRA empowers the European Commission to specify "highly

---

210 *Id*. at 31-32.

211 *Id*. at 32 (referring to the Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU).

212 *Id*. at 32.

213 More detailed definition, *see id*. at 33: "'remote data processing' means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions."

214 *Id*. at 48.

215 *Annexes to the Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020*, at 4-5, COM (2022) 454 (Sept. 15, 2022).

critical products with digital elements."[216] In this case the manufacturers are required to obtain a European cybersecurity certificate to be able to demonstrate conformity with the requirements of the CRA.[217] In order to determine which products are highly critical ones, the Commission has to take into account, inter alia, the future relevance of these products or their use by essential entities according to the NIS 2 Directive.[218] Furthermore, the Commission has to take into account the relevance of these products for the resilience of the overall supply chain (of products with digital elements) against disruptive events.[219]

Interestingly enough, the current proposal does not regulate Software-as-a-Service (SaaS) as such.[220] However, SaaS is included if it fulfils the definition of a remote data processing solution.[221] Apparently, the reason for this is – according to Recital 9 of the CRA – that SaaS as such would in many cases be already regulated by the NIS 2 Directive, which applies to SaaS as long as the providing entity meets or exceeds the threshold for medium-sized enterprises.[222]

The obligations for manufacturers, importers and distributors arise once the products are placed on the market (by manufacturers or importers; meaning making the products available for the first time),[223] respectively when the products are made available on the market (which may be the case multiple times by multiple distributors).[224] Because of the broad definition of which products are products

216 *CRA*, *supra* note 116, at 36.
217 *Id*. at 37.
218 *Id*.
219 *Id*.
220 *See id*. at 15, 21.
221 *Id*.
222 *Id*. at 15.
223 Meaning "the first making available of a product with digital elements on the Union market", *id*. at 35.
224 Meaning "any supply of a product with digital elements for distribution or use on the Union

with digital elements, the proposal of the CRA will have significant influence on entities acting in the Union market.

5. EVALUATING THE IMPACT ON SUPPLY CHAINS

The following example is supposed to highlight and exemplify the impact of the new data law and the cybersecurity framework on international supply chains. The chosen example (see Figure 4) is a compromise between a plausible, realistic and comprehensive supply chain, which at the same time is simplified in order to make a legal analysis possible. For example, there are only a few stakeholders, while a realistic supply chain would involve a lot more different companies. However, this example includes the most relevant stakeholders.

For this example, we assume the following presumptions:

(1) the data processing involves personal data;

(2) the relevant laws discussed here are in general applicable to the stakeholders in this example, so, e.g., they can not exempt themselves because they are a small company;

(3) subject of the analysis is only current and currently discussed EU law.

market in the course of a commercial activity, whether in return for payment or free of charge", *id*. at 34.

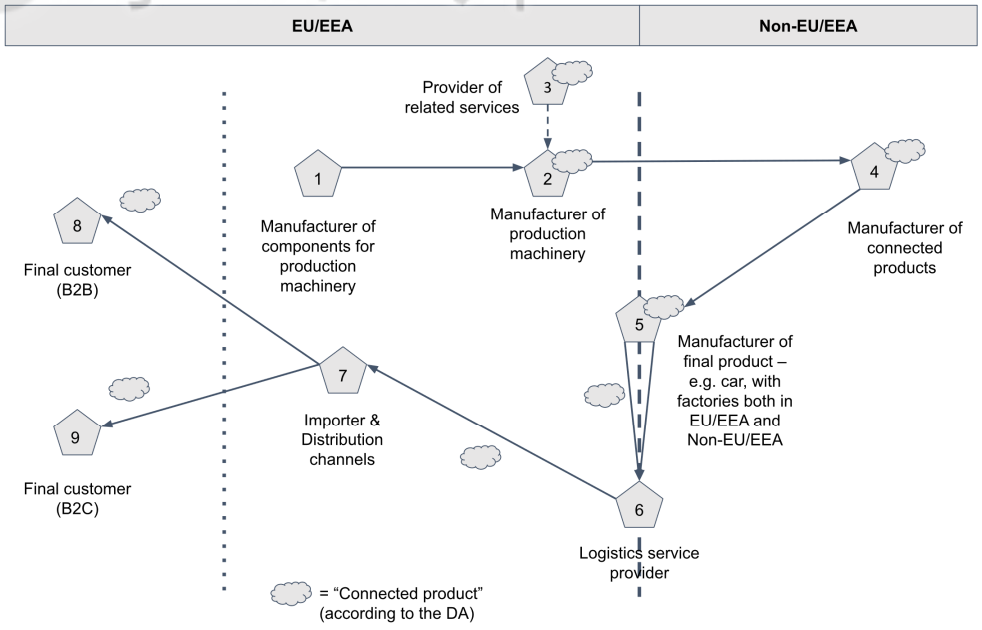

Figure 4: Example of an International Supply Chain

As Figure 4 shows, in the example there is a supply chain that involves connected products (in the sense of the DA). Table 1 describes the roles of each entity in the chosen example.

Table 1: Description of the Entities of Figure 4

Entity 1	Entity 1 is a manufacturer of components for production machinery and delivers these components to entity 2. However, these components do not qualify as "connected products" and entity 1 does not receive any data from entity 2 or entity 3.
Entity 2	Entity 2 is a manufacturer of production machinery. These machines qualify as connected products. It delivers the machines to a manufacturer of connected products, based outside the EU/EEA (entity 4). Entity 2 reverts to a provider of related services for parts of the production process (entity 3).

Entity 3	Entity 3 provides related services for parts of the production process to entity 2. These services are not only used in the production process itself but are "related services" according to the DA. This means they are connected with the product in such a way that their absence would prevent the product from performing at least one of its functions. This would include, for example, the operating system of an (I)IoT device.
Entity 4	Entity 4 is a manufacturer of connected products, based outside the EU/EEA. These products are then delivered to a manufacturer of the final product, e.g. a car (entity 5).
Entity 5	Entity 5 is the manufacturer of the final product. This entity has factories both in the EU/EEA and outside of the area.
Entity 6	Entity 6 is the logistics provider, which transports the final products to the importer & distributor in the EU/EEA (entity 7).
Entity 7	Entity 7 is an importer/distributor based in the EU/EEA.
Entity 8	Entity 8 is an example for a business as a customer.
Entity 9	Entity 9 is an example for a consumer as a customer.

5.1 Impact of the Data Sharing Obligations Set out in the DA

The impact of the data sharing obligations and the access rights to data pursuant to the provisions of the DA differ for each entity within the international supply chain. Therefore, the impact on the supply chain is described in Table 2.

Table 2: Impact of DA on Entities of International Supply Chain

Entity 1	Entity 1 falls within the territorial scope of the DA as it is based within the EU/EEA. Since entity 1 solely delivers components for entity 2, it does not design the connected product and thus does not fall within the material scope of the DA. Furthermore, it does not receive any data from entity 2 or entity 3 and therefore cannot be classified as data holder.
Entity 2	Entity 2 falls within the scope of the DA as it is a manufacturer within the EU/EEA and designs production machinery that generates data and thus can be classified as a connected product. Therefore, it has to fulfil the DA's obligation

	to design the production machinery with a direct access for the user and – if the data cannot be directly accessed – provide access to users within the EU. Furthermore, entity 2 must provide the user the information necessary to access the data.
Entity 3	Entity 3 must fulfil almost the same obligations as entity 2 except that it must provide information to the user in relation to the related service instead in relation to a connected product.
Entity 4	Entity 4 as a user: Entity 4 fulfils the DA's definition of a user. However, it cannot request access from neither entity 2 nor entity 3 since entity 4's establishment is not in the EU/EEA and thus it is not covered by the territorial scope of the DA. As a consequence, it may be beneficial for entity 4 to establish a subsidiary in the EU/EEA in order to gain the benefits of a user. Entity 4 as a data holder: On the other hand, entity 4 is a manufacturer of connected products and it receives data from entity 5 as a data holder. Therefore, entity 4 must adhere to the provisions of the DA if it intends to place the connected product in the market of the EU/EEA. As a consequence, entity 4 must provide access to the data generated by the use of the connected product by entity 5. However, this does not apply if entity 5's establishment is not within the EU/EEA. Furthermore, entity 4 must provide access to data generated by the use of the connected product by entity 8 or entity 9 respectively. In addition, it cannot process the data unless it has concluded a contractual agreement with the respective entity. However, it remains unclear whether it can base its processing of data generated by entity 8/9 on the contract between entity 5 and entity 8/9.
Entity 5	Entity 5 is both a user and a data holder pursuant to the provisions of the DA. Insofar as entity 5 generates data through the use of the connected product of entity 4, it has a right to access the data and to share them with a third party. On the other hand, entity 5 must grant access to and conclude contractual agreements with both entity 8 and entity 9 respectively. Since entity 5 has factories outside of the EU/EEA it must consider the GDPR's provision for the transfer of personal data to a third country if it transfer the data to a factory outside of the EU/EEA. In parallel, the subsidies outside of the EU/EEA cannot fall within the territorial scope of the DA even if they would be a user or a data recipient according to the DA.

Entity 6	Entity 6 falls within the territorial scope of the DA but since it does not receive any data generated by the connected product nor provides a related service, it does not fall within the material scope of the DA. However, it may contribute to a Common European Data Space in order to share data with other entities within the supply chain in order to improve their services
Entity 7	The same as for entity 6 applies to entity 7 since it does not receive any data generated by the use of the product.
Entity 8	Entity 8 is a user and therefore has the right to access and to share the data generated by the use of the connected product of entity 5. Furthermore, since entity 8 is a natural person, entity 8 can give its consent for the sharing of the data with any third party if the data generated is personal data concerning entity 8. In parallel, entity 8 can exercise its right to data portability and its right to access under the GDPR as alternative means to access and share data as far as it is personal data.
Entity 9	In contrast to entity 8, entity 9 is a legal person and thus will have to provide a legal basis for the sharing of personal data with a third party. Furthermore, if the data is generated by a natural person within entity 9, the respective data holder may be obliged to grant access to this natural person as user, too.

The analysis shown in Table 2 reveals that the entities within an international supply chain must consider different obligations depending on their place of establishment and the data they generate or receive as a consequence of a use by another entity. Especially the case of entity 4 shows that non-EU established entities have to comply with the obligations of the DA whilst not being able to receive the benefits as a user. Therefore, they could be incentivised to establish a subsidiary in the EU/EEA in order to reap the benefits of their use of a connected product provided by an EU entity.

5.2 Impact of the Cybersecurity Obligations Set out in the CRA

As shown above, the CRA regulates a strict regiment of essential cybersecurity measures for products with digital elements that are placed – or made

available – on the Union market. Because of the broad definition of products with digital elements, "connected products" according to the DA will often qualify as "products with digital elements" as well – at least, if there are no specific exemptions, like sector-specific regulation for certain medical devices. Therefore, for the chosen example, the most important question is which entities qualify as manufacturers, importers or distributors and which one of them eventually places the product on the Union market. In order to illuminate the differences between these terms and the accompanying obligations, see Figure 5. Note that, in general, the requirements increase continuously from distributors to manufacturers.

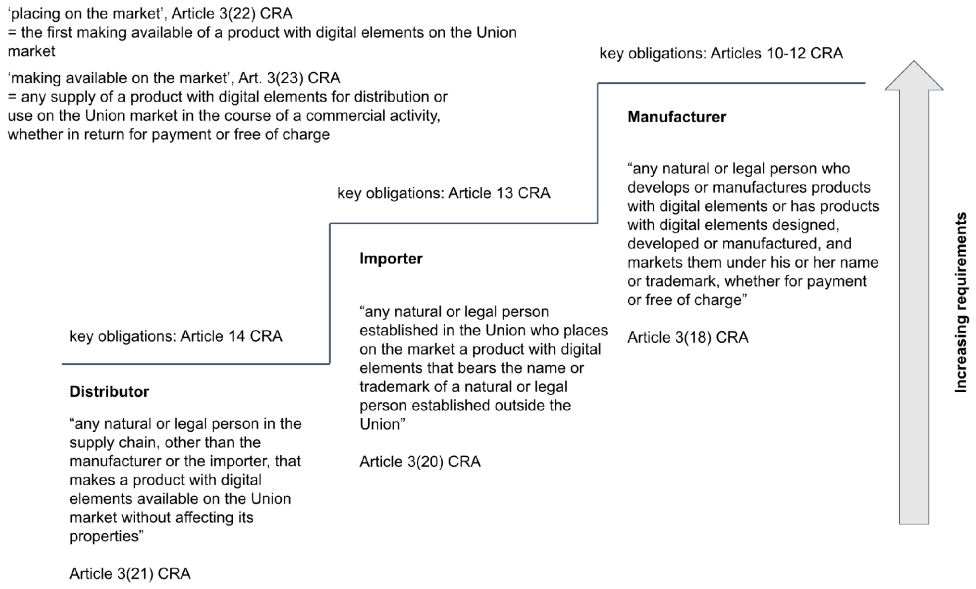

Figure 5: Different Types of Stakeholders in the CRA

Accordingly, Table 3 illustrates how the CRA affects the different entities in the chosen example.

Table 3: Impact of CRA on Entities of International Supply Chain

Entity 1	The components of entity 1 do not qualify as connected products, nor as products with digital elements (according to the CRA). Entity 1 therefore has no obligation to fulfil the obligations of the CRA.
Entity 2	Entity 2 is a manufacturer of production machinery which qualify as connected products as well as products with digital elements. Therefore, it has to comply with the CRA, especially with the obligations set out in Articles 10, 11 CRA. The entity reverts to a provider of related services (entity 3) for parts of the production process.
Entity 3	As a provider of related services, entity 3 could also qualify as providing "remote data processing solutions" according to the CRA. This depends on the concrete service/solution. However, the two definitions are quite similar as both require that the service/solution is connected to the product in such a way that its absence would prevent the product from performing at least one of its functions.[225] Therefore, the products of entity 3 are typically addressed by the CRA as well because this would qualify as developing the remote data processing solution "under the responsibility of the manufacturer."[226] However, if entity 3 does not place the solution on the market on its own, the obligation by law stays with the manufacturer, entity 2.
Entity 4	While the products produced by entity 4 fulfil the requirements of "products with digital elements", as long as entity 4 does not place them on the EU/EEA market, the entity does not have to fulfil the CRA requirements by law. However, with entity 5 selling on the EU/EEA market, this will influence the contractual obligations of entity 4. In addition, if entity 4 chooses to place its products on the Union market on its own, the entity would have to comply as a manufacturer just like entity 5.
Entity 5	Entity 5 is the manufacturer of the final product and has factories both inside and outside the EU/EEA. However, the location of the factories does not affect the application of the CRA. If entity 5 places its products on the EU/EEA market, it qualifies as a manufacturer according to the CRA – independent from the location of the entity. This also influences the role of entity 7, see

225 *See id*. at 33; *DA-Tri*, *supra* note 118, at 60.

226 *See CRA*, *supra* note 116, at 15.

	below. Nevertheless, as a manufacturer of vehicles, entity 5 would act in a "critical sector" according to the NIS 2 Directive. It, therefore, would have to fulfil the obligations stated by the Directive, especially those regarding supply chain security. In these cases, entity 4 would be influenced by this as well, depending on the type of products that entity 5 produces.
Entity 6	Since entity 6 is a mere logistics supplier and does not place products on the market nor makes them available to the market, it does not have to fulfil the CRA's requirements.
Entity 7	Entity 7 might qualify as an importer or a distributor, depending on the actions of entity 5: if entity 5 is active on its own in the Union market, by placing its products on the market on its own, entity 7 cannot qualify as an importer but solely as a distributor. However, if entity 5 is not active in the Union market, entity 7 may make the products of entity 5 available on the market for the first time. In this case, they qualify as an importer, resulting in additional requirements.
Entity 8, Entity 9	As customers of products with digital elements, entities 8 and 9 are not obligated to fulfil the CRA's requirements. However, in a different scenario, for example, if entity 8 is a critical infrastructure, it would be the main addressee of the obligations according to the NIS 2 Directive. This would result in implications for the whole supply chain, depending on the concrete scenario.

6. CONCLUSION

Although some of the most important legal acts have not been finalised yet, the EU's legislative strategy for a data economy becomes more and more apparent. While the EU's general objective appears to strike a fair balance between the interests of the different stakeholders, it remains to be seen whether a well-functioning data economy can eventually emerge in practice. Since the EU has decided to adopt a framework consisting of several different legal acts almost without amending any of the current legislation, this inevitably results in conflicts between the different goals of the legislative acts. This adds another layer of

complexity to the already rather complex current regulatory framework of the EU. Whilst any enactment of a new regulatory framework within the EU is a complex undertaking – both from a political as well as a legal perspective – various of these foreseeable conflicts could have been easily avoided, if the EU had established a clear distinction between the legislative acts. In conclusion, despite the EU's reasonable decision to leave the current data protection standards unaffected, this unnecessarily complex approach ultimately negatively affects the emerging data economy and will probably result in years of legal uncertainty that could have been reduced or, partially, even been avoided.

At the same time, the complexity of the new legislative framework is not only a challenge for European stakeholders but for international stakeholders, too. The extraterritorial effects of this framework have a severe impact on international supply chains and could especially negatively affect non-European stakeholders. Indeed, the DA will add the same obligations for both non-European and European stakeholders whilst providing benefits for the European stakeholders only.

Therefore, non-European stakeholders may be incentivised to establish a subsidiary in the EU/EEA in order to benefit from the EU data sharing mechanisms. Whilst acknowledging that there is a multitude of relevant considerations for such a decision and that the benefit from the DA regulations alone will not be the deciding factor, the potential benefits could be taken into account to consider setting up a subsidiary. Otherwise, non-EU entities will not be able to be classified as a data recipient.

However, they might still be able to gain access and receive data from the EU as a participant of the upcoming Common European Data Spaces, though the requirements are still unclear and could prove impossible to meet for stakeholders from certain non-European countries.

In addition, the regulations will already impact the design and production of products prior to their application because companies are incentivised to

preemptively avoid sanctions from the European authorities. Therefore, companies in- and outside of the EU/EEA will have to closely monitor the unfolding legislative acts in order to ensure that they will be able to comply with both European data law and the new cybersecurity framework.

In any way, the legislative approaches of the EU will likely entail strenuous efforts for participants of an international supply chain to ensure compliance and it remains to be seen whether these efforts can be outweighed by the benefits of an improved data sharing between the stakeholders.

References

Journals

Bonadio, Enrico, Nicola Lucchi & Giuseppe Mazziotti, *Will Technology-Aided Creativity Force Us to Rethink Copyright's Fundamentals? Highlights from the Platform Economy and Artificial Intelligence*, 53 IIC 1174 (2022).

Fernandez, Angelica, *The Data Act: The Next Step in Moving Forward to a European Data Space*, 8 EUR. DATA PROT. L. REV. 108 (2022).

Inguanez, Daniel, *A Refined Approach to Originality in EU Copyright Law in Light of the ECJ's Recent Copyright/Design Cumulation Case Law*, 51 IIC 797 (2020).

Kerber, Wolfgang, *Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives*, 72 GRUR INT. 120 (2023).

Perarnaud, Clément & Rosanna Fanni, *The EU Data Act: Towards a new European Data Revolution?*, CEPS POL'Y INSIGHTS, No. 2022-05, Mar. 2022.

Picht, Peter Georg & Heiko Richter, *EU Digital Regulation 2022: Data Desiderata*, 71 GRUR INT. 395 (2023).

Syrmoudis, Emmanuel, Stefan Mager, Sophie Kuebler-Wachendorff, Paul Pizzinini, Jens Grossklags & Johann Kranz, *Data Portability Between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20*, 2021 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 351 (2021).

Wiebe, Andreas, *The Data Act Proposal—Access Rights at the Intersection with Database Rights and Trade Secret Protection*, 72 GRUR INT. 227 (2023).

Wiedemann, Nils, Thorsten Conrad & Simone Salemi, *Bereitstellung von Daten nach dem Data Act—Offene Fragen und verbleibende Probleme*, 27 K&R 157 (2024).

Zirnstein, Yannick, *Better Cybersecurity Due to Increased Regulation? The Final European Cyber Resilience Act—The First Comprehensive, Horizontally Applicable Approach for More Cybersecurity in Digital Products*, 25 COMPUTER L. REV. INT'L 65 (2024).

Other Resources

Adequacy Decisions, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-

topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Oct. 31, 2023).

Building a Data Economy—Brochure, EUROPEAN COMMISSION, https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure#Strategy (last visited Oct. 31, 2023).

Costa de Oliveira, Piedade, *Article 95 Relationship with Directive 2002/58/EC*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 1294 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., 2020).

Cyber Resilience Act Factsheet, EUROPEAN COMMISSION (Dec. 1, 2023), https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

Derclaye, Estelle & Martin Husovec, *Why the Sui Generis Database Clause in the Data Act Is Counter-productive and How to Improve It?*, SSRN (2022), https://dx.doi.org/10.2139/ssrn.4052390.

Digital Markets Act: Commission Designates Six Gatekeepers, EUROPEAN COMMISSION (Sept. 6, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.

Drexl, Josef, Carolina Banda, Begona Gonzalez Otero, Jörg Hoffmann, Daria Kim, Shraddha Kulhari, Valentina Moscon, Heiko Richter & Klaus Wiedemann, *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)* (Max Planck Inst. for Innovation & Competition Rsch. Paper No. 22-05, 2022), https://dx.doi.org/10.2139/ssrn.4136484.

European Data Strategy, EUROPEAN COMMISSION, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (last visited Oct. 31, 2023).

Facts and Figures on the European Union Economy, EUROPEAN UNION, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (last visited Oct. 31, 2023).

Foresight Unit (STOA), Eur. Parliamentary Rsch. Serv., *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, PE 641.530 (June, 2020).

Geiregat, Simon, *The Data Act: Start of a New Era for Data Ownership?* (Ghent Univ., Working Paper, 2022), https://dx.doi.org/10.2139/ssrn.4214704.

Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive. Adopted on 14 November 2023, EUROPEAN DATA PROTECTION BOARD, https://www.edpb.europa.eu/system/files/2023-11/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_en.pdf (last visited July 12, 2024).

Hennemann, Moritz, Gordian Ebner & Benedikt Karsten, *The Data Act Proposal: Literature Review and Critical Analysis* (Univ. of Passau IRDG Rsch. Paper Series No. 23-01, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4360961.

Meulen, Rob van der, *What Edge Computing Means for Infrastructure and Operations Leaders*, GARTNER (Oct. 3, 2018), https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders.

New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient, EUROPEAN COMMISSION (Dec. 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

Streim, Andreas & Isabelle Stroot, *After 5 Years: GDPR Only Receives the Grade "Sufficient"*, BITKOM, https://www.bitkom.org/EN/List-and-detailpages/Press/5-years-GDPR-receives-grade-sufficient (last visited July 12, 2024).

The European Commission's Statement Ahead of the 5th Anniversary of the General Data Protection Regulation, EUROPEAN UNION (May 24, 2023), https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2884.

The European Union's Primary Law, EUROPEAN UNION (Dec. 12, 2022), https://eur-lex.europa.eu/EN/legal-content/summary/the-european-union-s-primary-law.html.

Top Cyber Threats in the EU, COUNCIL OF THE EU AND THE EUROPEAN COUNCIL, https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/ (last visited Oct. 31, 2023).

Trilogue, EUROPEAN UNION, https://eur-lex.europa.eu/EN/legal-content/glossary/trilogue.html (last visited Oct. 31, 2023).