International Journal of Law and Information Technology, 2023, **31**, 399–412
https://doi.org/10.1093/ijlit/eaae005
Advance access publication 25 February 2024
Article

The EU Data Act in context: a legal assessment

Federico Casolari[*], Carlotta Buttaboni[†] and Luciano Floridi[‡,**]

ABSTRACT

The present article analyses the main legal features of the EU Data Act, identifying some innovative aspects and shortcomings. Moving from the general approach elaborated by the Union towards data governance—a value-based approach flowing from the idea of enforcing the strategic autonomy of the Union—the article considers first the most relevant piece of legislation that complements the DA, that is, the EU Data Governance Act, and then assesses the DA in light of both the original proposal of the European Commission and the position adopted by the two EU co-legislatures—the European Parliament and the Council. An overview of the major competitive legal approaches to the governance of IoT data (namely, the USA and Chinese approaches) is also discussed, stressing possible synergies and conflicts with the EU's approach.

KEYWORDS: data governance; data sharing; Internet of Things; EU Data Act; EU fundamental values and identity; strategic autonomy doctrine.

INTRODUCTION

On 23 February 2022, the European Commission released the EU Data Act (DA), a long-awaited proposal for an EU Regulation to introduce harmonized rules on fair data access to and use. The proposal seeks to ensure fairness by removing barriers to consumers' and businesses' access to data generated by Internet of Things (IoT) devices.[1]

[*] Federico Casolari, Department of Legal Studies, University of Bologna, Via Zamboni, 27/29, 40126 Bologna, Italy. Tel: +39-051-2099651; Email: federico.casolari@unibo.it.
[†] Carlotta Buttaboni, Department of Legal Studies, University of Bologna, Via Zamboni, 27/29, 40126 Bologna, Italy. Tel: +39-346-9859896.
[‡] Luciano Floridi, Digital Ethics Center, Yale University, 85 Trumbull Street, New Haven, CT 06511, United States. Tel: +1-203-9966029.
[**] Luciano Floridi, Department of Legal Studies, University of Bologna, Via Zamboni, 27/29, 40126 Bologna, Italy.
We would like to thank the members of the IFAB's International Scientific Board, Ursula Rita Bassler, Mateo Valero Cortès, Thomas Lippert, Florence Rabier, and Alberto Sangiovanni Vincentelli, for their valuable inputs and contributions to the present work. The responsibility for the content and any remaining errors remain exclusively with the authors.
[1] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act)', COM (2022) 68 final, 23 February 2022. All EU law documents, including the decisions adopted by the Court of Justice of the European Union, mentioned in this paper are available at <https://eur-lex.europa.eu/homepage.html> accessed 1 October 2023.

To achieve its general goal, the DA introduces rules that are intended to (i) increase legal certainty for consumers and companies generating data when it comes to the use and transfer of such data, facilitating the data economy; (ii) prevent abuses deriving from contractual imbalances that may undermine data transfer; (iii) ensure that public sector bodies may access and use data held by the private sector during a public emergency or to implement a legal mandate if data are not otherwise available; (iv) enable consumers to switch easily between different providers of data processing services.

It is worth stressing that, according to Article 288 of the Treaty on Functioning of the European Union (TFEU), regulations are considered the main binding legal act to be adopted by the EU legislature. So, the DA is likely to produce a significant impact on the municipal law of EU Member States.

Against this background, in this article, we analyse the main legal features of the DA in the context of the EU's general approach towards data governance. We identify the DA's innovative aspects and its gaps and shortcomings, for which we propose amendments and changes to be considered by the EU legislature. More specifically, in 'Setting the Scene' section, we introduce the general strategic framework within which the DA is placed, that is, the EU Strategic Autonomy Doctrine (SAD). We discuss the general concept of 'Strategic Autonomy of the European Union', as it has been recently applied to the supranational government of digital transformation,[2] particularly regarding data policy.[3] We then consider the most relevant legislation that complements the DA, the EU Data Governance Act (DGA).[4] In 'Zoom-in: the EU Data Act in a Nutshell' section, we summarize DA's main features, as they are enshrined in the original proposal of the European Commission. In 'The EU Data Act: A Critical Evaluation' section, we assess the DA, discussing views and positions expressed in the literature and by other EU relevant actors, including the European Parliament and the Council, in the legislative procedure.[5] In 'The competitive, regulatory landscape' section, we provide a general overview of the competitive legal approaches to the governance of IoT data. In particular, we focus on the USA and Chinese approaches. In 'Concluding remarks' section, we summarize our main conclusions.

SETTING THE SCENE: FROM THE EU SAD TO A NEW SUPRANATIONAL GOVERNANCE FOR DATA

Introduced in 2013 to strengthen the position of the European Union as a global actor, the debate concerning the SAD of the Union has gained momentum during the last decade, also in light of the context of crises faced by the EU.[6] The SAD mainly refers to the EU's ability to act autonomously in the most sensitive policy areas, that is, independently of other countries

[2] cf. Commission, Communication on 2030 Digital Compass: the European way for Digital Decade, COM (2021) 118 final, 9 March 2021.

[3] cf. Commission, 'Communication on A European strategy for data, COM (2020) 66 final, 19 February 2020.

[4] 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] OJ L152/1.

[5] At the time of writing the European Parliament adopted amendments to the proposal at first reading. The issue was referred back to the committee responsible for inter-institutional negotiations. Cf. Amendments adopted by the European Parliament on 14 March 2023; doc. P9_TA(2023)0069. The mandate for negotiations with the Parliament on the DA has been adopted by the Council on 17 March 2023; doc. 7413/33. Following the outcome of the informal trilogue between the representatives of the European Commission, the European Parliament, and the Council of the European Union, held on 27 June 2023, a draft compromise text was agreed on 14 July 2023. See Council of the European Union, doc. A 004595, 18 July 2023. Therefore, the European Parliament should adopt its position at first reading, in accordance with Article 294.3 TFEU, in the form as set out in the compromise text. The Council should, in accordance with Article 294.4 TFEU, approve the European Parliament's position, thus leading to the formal adoption of the DA. For further details on the status of the procedure, see <https://oeil.secure.europarl.europa.eu/> accessed 1 October 2023.

[6] See Fabian Zuleeg, Janis A. Emmanouilidis and Ricardo Borges de Castro, 'Europe in the Age of Permacrisis' (*Welcome to EPC—European Policy Centre*, 11 March 2021) <https://www.epc.eu/en/publications/Europe-in-the-age-of-permacrisis~3c8a0c> accessed 1 October 2023.

and international organizations.[7] The all-encompassing nature and fuzzy scope of the SAD are illustrated by the fact that it has become a sort of mantra in legal discourse about the Union: from the Common Foreign Security Policy[8] to the screening of foreign direct investments,[9] from the management of energy and semiconductors shortage[10] to the protection of the values upon which the Union is based.[11] The Russian aggression on Ukraine has further strengthened the affirmation of that doctrine, which has been directly linked to the concept of 'European sovereignty'. This is clear in the 2022 Versailles Declaration, adopted by the Heads of Stated or Governments of the Member States two weeks after Russia's military aggression, where the EU States' leaders

> decided to take more responsibility for [...] security and take further decisive steps towards building [... the] *European sovereignty*, reducing [...] dependencies and designing a new growth and investment model for 2030.[12]

Unsurprisingly, the SAD has been called to play a pivotal role in the EU governance of the digital transformation. In line with the most recent developments just mentioned, its application to the digital domain led to the introduction of the concept of 'EU digital sovereignty'. Although such a concept has not yet received a univocal definition and appears subject to many interpretations, as underlined by Angela Merkel during her speech at the Internet Governance Forum 2019,[13] some scholars have described it as a 'powerful form of powercynetic [...] control' able, to some extent, to give rise to concerns about a possible 'democratic deficit'.[14] By heavily relying on the traditional notion of 'state sovereignty',[15] the concept of digital sovereignty refers to the EU's capacity to act in the digital domain independently and effectively, to protect its vital interests and those of its Member States.[16] Regardless of its precise definition, its rationale is the need to fight for the preservation of EU core values and principles in the digital world. This need has been stressed by the numerous international

[7] For further details, see Natalie Tocci, *European Strategic Autonomy: What It Is, Why We Need It, How to Achieve It* (IAI Istituto Affari Internazionali 2021) <https://www.iai.it/sites/default/files/9788893681780.pdf> accessed 1 October 2023; Niklas Helwig and Ville Sinkkonen, 'Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term' (2022) 27, Eur Foreign Aff Rev 1 <https://www.fiia.fi/wp-content/uploads/2022/04/intro_helwigsinkkonen_2022.pdf> accessed 1 October 2023; and the contributions to the 2022 Special Issue of the *European Foreign Affairs Review*.

[8] cf. European Council's conclusions, doc. EUCO 217/13, 19–20 December 2013, para 16.

[9] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, [2019] OJ L79I/1.

[10] cf. Commission, Communication on REPowerEU Plan, COM(2022) 230 final, 18 May 2022, and Commission, 'Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)' COM(2022) 46 final, 8 February 2022, respectively.

[11] European Parliament, 'EU Strategic Autonomy Monitor—From Concept to Capacity', July 2022.

[12] cf. Informal meeting of the Heads of State or Government, Versailles Declaration, 10–11 March 2022; emphasis added.

[13] Rede von Bundeskanzlerin Angela Merkel zur Eröffnung des 14. Internet Governance Forums 26. November 2019 in Berlin <https://www.bundeskanzler.de/bk-de/aktuelles/rede-von-bundeskanzlerin-angela-merkel-zur-eroeffnung-des-14-internet-governance-forums-26-november-2019-in-berlin-1698264> accessed 1 October 2023.

[14] Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially of the EU' (2020) 33 Philos Technol 369, 378.

[15] The principle of sovereignty, implying a supreme authority within a given territory, is a cornerstone of modern international law: see Samantha Besson, 'Sovereignty' (2022) MPEPIL <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472?print=pdf> accessed 1 October 2023. For a general reflection on the notion of 'European sovereignty', see Ségolène Barbou des Places, 'Taking the Language of 'European Sovereignty' Seriously' (2020) 5 European Papers <https://www.europeanpapers.eu/it/system/files/pdf_version/EP_eJ_2020_1_18_SS3_Insights_Intro_Segolene_Barbou_des_Places_00392.pdf> accessed 1 October; Thomas Verellen, 'European Sovereignty Now? A Reflection on What It Means to Speak of 'European Sovereignty' (2020) 5 European Papers <https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2020_1_21_SS3_Insights_Thomas_Verellen_00383.pdf> accessed 1 October 2023.

[16] European Parliament, 'Digital Sovereignty for Europe', EPRS Ideas Paper, July 2020. See also Huw Roberts and others, 'Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies' (2021) 10 Internet Policy Rev 1. More generally, on the notion of 'digital sovereignty' see Farid Gueham, 'Digital Sovereignty. Steps Towards a New System of Internet Governance' (2017) <https://www.fondapol.org/app/uploads/2020/06/f-gueham-digital-sovereignty-3.pdf> accessed 1 October 2023; Svetlana Yakovleva, 'On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows' (2022) 49 Leg Issues Econ Integration 339.

scandals that have encouraged the EU legislature to step in.[17] Such an ambition, together with the trajectories of the EU digital sovereignty, have been traced in the 2020 Commission's strategic paper on the EU digital future,[18] and further improved in the so-called Union's 2030 Digital Compass, defining the priorities of the EU action in the digital ecosystem for the next decade, where it was stated that:

> That is the way for Europe to be digitally sovereign in an interconnected world by building and developing logical capabilities in a way that empowers people and business to seize the potential of the digital transformation.[19]

Turning to the EU data policy, the new supranational approach has been enshrined in the 2020 European Strategy for Data.[20] The vision expressed by the European Commission in that Strategy is clear:

> [it] stems from European values and fundamental rights and the conviction that the human being is and should remain at the centre. The Commission is convinced that businesses and the public sector in the EU can be empowered through the use of data to make better decisions. It is all the more compelling to seize the opportunity presented by data for social and economic good, as data—unlike most economic resources—can be replicated at nearly zero cost, and its use by one person or organisation does not prevent the simultaneous use by another person or organisation. That potential should be put to work to address the needs of individuals and thus create value for the economy and society. To release this potential, there is a need to ensure better access to data and its responsible usage.[21]

Based on the 'very identity of the European Union as a common legal order'[22]—that is, respect for human dignity, freedom, democracy, equality, the rule of law, and human rights, including the rights of persons belonging to minorities—the Commission calls for a better use of data in the EU economy.[23]

More precisely, the Commission has identified the main challenges[24] and the four pillars upon which the EU's relevant action should be based (Fig. 1). Pillar 1 concerns the regulatory framework to be introduced to ensure better access to, and more responsible use of data. Here, two major cross-sectoral initiatives are envisaged. The first has led to the adoption of the DGA and requires a legislative framework for the governance of the European data spaces. The second one, carried out with the proposal of the DA, should incentivise data availability for access

[17] Edoardo Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives', in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing 2021).

[18] European Commission, 'Shaping Europe's Digital Future', 2020.

[19] Commission, Communication on 2030 Digital Compass: the European way for the Digital Decade, COM (2021) 118 final, 9 March 2021.

[20] Commission, Communication on A European Strategy for Data, COM (2020) 66 final, 19 February 2020.

[21] ibid, para 3.

[22] Case C-157/21, *Republic of Poland v European Parliament and Council of the European Union* [2022] ECLI:EU:C:2022:98, para 145.

[23] The human-centred approach towards digital transformation and data governance has been further stressed in the 2022 European Declaration on Digital Rights and Principles for the Digital Decade, which was solemnly proclaimed by the European Parliament, the Council and the Commission (2023) OJ C23/1.

[24] They are identified as follows: (i) fragmentation of the regulatory framework at Member States level, which undermines the proper functioning of the internal market; (ii) availability of data for innovative re-use, including for the development of artificial intelligence systems; (iii) imbalances in the market power; (iv) data interoperability and quality; (v) data governance, implying the need to elaborate organizational approaches and structures to enable data-driven innovation; (vi) data infrastructure and interoperability; (vii) individuals empowerment; (viii) cybersecurity. Commission Communication, 'A European Strategy for Data', cit., para 4.

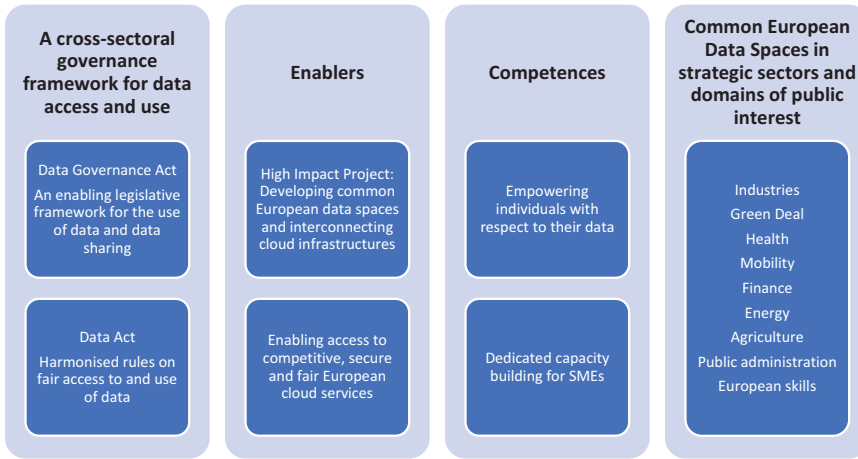

Figure 1. The four pillars of the EU Data strategy.

and re-use. Pillar 2 contains initiatives the Commission should implement to strengthen the EU's capabilities for hosting, processing, and using data. The Commission intends to fund the creation and functioning of common European data spaces and interconnecting cloud infrastructures to overcome the legal and technical barriers to data sharing across Europe. Pillar 3 looks at the empowerment of individuals: it foresees measures to enforce individuals' rights when it comes to the use of the data they generate. As for legal persons, and SMEs, in particular, the Strategy promotes the creation of better opportunities in the data economy, also thanks to capacity-building schemes and specific investment funds. Pillar 4 complements the other pillars by fostering the development of common European data spaces in strategic economic sectors and other domains of public interest.[25]

Notably, the Strategy clarifies that the approach to be adopted in defining the legal framework for data will consist of creating 'frameworks that shape the context, allowing lively, dynamic and vivid ecosystems to develop.'[26] Quite significantly, the Commission further elaborates on the features that should characterize the EU law-making in the field concerned:

> Because it is difficult to fully comprehend all elements of this transformation towards a data-agile economy, the Commission deliberately abstains from overly detailed, heavy-handed ex ante regulation, and will prefer an agile approach to governance that favours experimentation (such as regulatory sandboxes), iteration, and differentiation.[27]

This approach, echoing the recourse to regulatory sandboxes in the EU artificial intelligence proposal,[28] has advantages and disadvantages. Adopting general and flexible legal frameworks could ensure an easier and more effective data management, given the quick transformations and evolutions of the domain at stake, and the fact that the allocation of competencies between

[25] cf. Commission Staff Working Document, 'Common European Data Spaces', SWD (2022) 45 final, 23 February 2022. See also Edward Curry, Simon Scerri and Tuomo Tuikka, 'Data Spaces: Design, Deployment, and Future Directions' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds) *Data Spaces* (Springer 2022) <https://doi.org/10.1007/978-3-030-98636-0_1> accessed 1 October 2023. The first Common European Data Space to be established should be the European Health Data Space: see Commission, 'Proposal for a Regulation on the European Health Data Space' COM (2022) 197 final, 3 May 2022.

[26] Commission, Communication on A European Strategy for Data', cit., para 5.

[27] ibid.

[28] Sofia Ranchordas, 'Experimental lawmaking in the EU: Regulatory Sandboxes' University of Groningen Faculty of Law Research Paper 12/2021, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3963810> accessed 1 October 2023.

the Union and its Member States is not always clear enough (this issue that will also be discussed in the following sections). However, the downside of a more flexible approach to data governance is that it may be too flexible, so to speak, thus raising doubts as to its legitimacy and transparency and preventing the possibility of establishing permanent regulatory cooperation in the data economy. Furthermore, such an approach could lead to uncertainty of the law, potentially inhibiting innovation and growth in the data-driven economy, something that the EU Strategy would like to prevent. Finally, the experimentalism and differentiation promoted by the Commission may further exacerbate the fragmentation of the EU legal framework, making it more challenging to establish an effective and coherent regulatory European space for data. Let us now turn to the DGA.

The DGA

As anticipated, Regulation 2022/868 has contributed to shaping the first Pillar of the EU Data Strategy. By relying on Article 114 TFEU—the so-called 'Internal Market Clause',[29] which allows the Union to adopt binding instruments to ensure the proper functioning of the internal market—this piece of legislation seeks to introduce a general legal framework defining: (i) conditions and fees for re-use, within the Union, of specific categories of data held by public authorities; (ii) rules for the provision of data intermediation services; and (iii) rules for the voluntary registration of entities collecting and processing data for altruistic purposes. The DGA gives precedence to the specific discipline enshrined in the General Data Protection Regulation (GDPR)[30] and to EU competition law (Articles 1.3 and 1.4, respectively). It also safeguards the Member States' prerogatives in public security, defence, and national security (Articles 1.3 and 1.5, respectively).

Concerning data re-use,[31] the DGA establishes that related conditions shall be non-discriminatory, transparent, proportionate and objectively justified with regard to categories of data and the purposes of re-use and the nature of the data for which re-use is allowed (Article 5.2).[32] Re-use requires that relevant data be anonymized (in case of personal data) and modified, aggregated, or treated by any other method of disclosure control, in case of commercial confidential information (Article 5.3). Arrangements granting exclusive rights or restricting data availability for re-use by entities other than the parties to such agreements or other practices having equivalent effects are prohibited (Article 4.1).

The intermediation services regulated by the DGA consist of (i) intermediation services between data holders and potential data users; (ii) intermediation services between data subjects seeking to make their personal data available or natural persons seeking to make non-personal data available, and potential data users; and (iii) services of data cooperatives (Article 10). The DGA imposes specific notification duties upon the data intermediation services providers intending to provide similar services (Article 11) and specifies the conditions for providing data intermediation services (Article 12).

A specific discipline is then introduced for data altruism. This represents an important legal milestone, mainly in the medical field, concerning the donation of one's own medical data. In the past, it had been argued by some scholars that the impossibility of voluntarily sharing medical records for research purposes presented an 'ethically unjustifiable asymmetry in the

[29] See Manuel Kellerbauer, 'Article 114 TFEU' in Marcus Klamert, Jonathan Tomkin and Manuel Kellerbauer (eds), *The EU Treaties and the Charter of Fundamental Rights* (OUP 2019).

[30] 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, [2016] OJ L119/1.

[31] According to Article 2.1, re-use 'means the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks'.

[32] The same requirements apply to fees charged by public sector bodies for allowing re-use of data: DGA, Article 6.1.

biomedical research' for two main reasons: on the one hand, these data are extremely valuable for further scientific improvements, and on the other hand, such impossibility obstacles the free will of whom is interested in sharing their data for scientific purposes.[33] The DGA tries to fill the gap, by providing first a (somewhat) articulated definition of data altruism. According to the DGA, it includes:

> the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest.[34]

Data altruism is not subject to the conditions related to intermediation services (Article 15). It requires the adoption by Member States of national arrangements to facilitate the collection of data based on it. Registration requirements and procedures are then specified in order to qualify entities as data altruism organizations (Articles 17–24). Also significantly, the DGA foresees that the EU shall adopt a Rulebook containing additional information requirements, appropriate technical and security measures, communication roadmaps, and interoperability standards (Article 22).

Due to the significant implementation measures that Member States shall adopt to operationalize the DGA, this piece of legislation, which entered into force on 23 June 2022, applies from 24 September 2023 (Article 38).

This is not the place for an in-depth analysis of the DGA and its possible implications, but it is worth highlighting some emerging trends that have been replicated in the proposal of DA. First, the DGA seems to reduce significantly the flexible and differentiated approach promoted by the Commission in the EU Data strategy. Not only does it introduce a strict regulatory approach towards data governance, it also replicates a classical EU multilevel law-making strategy, thus requiring the establishment of national competent authorities to implement and monitor related measures. While consistent with the shared nature of the EU competence exercised by the supranational legislature, which is subject to the respect of the principle of subsidiarity (Article 5, para 3, TEU), it has been argued that such a trend may represent a possible disincentive to access a data-driven economy by SMEs.[35] Secondly, the several 'without prejudice clauses' occurring in the DGA—giving precedence to other sectoral supranational sets of rules and recognizing specific Member States' prerogatives—together with the vagueness of some concepts it contains—starting from the notion of 'data altruism', which mainly relies on the opaque notion of 'objectives of general interest'[36]—create a multi-layered regulatory framework that risks undermining the objectives pursued by the DGA, introducing further bureaucratic burden to data sharing. As anticipated, some of these problems are also present in the DA, to which we shall now turn.

[33] Jenny Krutzinna and Luciano Floridi, 'Ethical Medical Data Donation: A Pressing Issue' in Jenny Krutzinna and Luciano Floridi (eds), *The Ethics of Medical Data Donation,* (Springer 2019).

[34] DGA, Article 1.16.

[35] See Winfried Veil, 'Data Altruism: how the EU is screwing up a good idea', Discussion Paper # 1, Algorithm Watch, <https://algorithmwatch.org/en/eu-and-data-donations/>, accessed 1 October 2023.

[36] See Paul Keller and Francesco Vogelezang, 'The Data Governance Act: Five Opportunities for the Data Commons' (*Open Future Policy Brief # 0,* 23 June 2021) <https://openfuture.eu/publication/the-data-governance-act-five-opportunities-for-the-data-commons/> accessed 1 October 2023.

ZOOM-IN: THE EU DATA ACT IN A NUTSHELL

The proposal for an EU Data Act is also based on Article 114 TFEU. This is significant. Not only is the Internal Market Clause becoming a fundamental legal basis for shaping the digital sovereignty of the Union[37] but, as anticipated, it also represents a shared competence between the EU and its Member States. More precisely, Article 4.2 and 4.3 TFEU specify that, in the area of the single market and technological development, the EU can carry out specific activities without prejudice to Member States' freedom to act in the same area. This also explains why, like in the case of the DGA, the discipline introduced in the DA leaves room for different levels of Member States' action, provided that this margin of manoeuvre does not undermine the supranational objectives of the initiative.

The subject and scope of the DA are identified in Article 1.1. The proposed regulation lays down harmonized rules on (i) making data generated by a product or related service available to the user of that product or service, (ii) making data available by data holders to data recipients, and (iii) making data available by data holders to public sector bodies or Union institutions, agencies, or bodies in cases of exceptional needs. The DA has a Union-based scope: it applies to manufacturers of products and suppliers of related services placed on the EU market and the users of such products and services; to data holders making available data to data recipients in the Union; to data recipients in the Union; to Member States' public sector bodies and EU institutions and bodies; and to providers of data processing services offering such services to customers in the Union.

Significantly, the DA too contains several 'without prejudice' clauses. First, the primacy of the GDPR is reaffirmed (Article 1.4). Moreover, the proposal does not interfere with specific provisions introduced to foster cooperation in criminal matters via data usage (Article 1.4). EU law regulating intellectual property rights, as well as EU competition law, are not affected. Like the DGA, the DA confirms the respect of Member States' prerogatives concerning public security, defence, and national security and specifies that States' powers regarding activities concerning customs, tax administration, and the health and safety of citizens are protected too (Article 1.4). The most relevant aspects of the substantive discipline enshrined in the DA can be briefly summarized as follows.

Regarding business-to-consumer (B2C) and business-to-business (B2B) data sharing (Chapter II), the DA introduces an obligation to make data generated by the use of products or related services accessible. This means that products and services must be designed or provided so that data generated by their use 'are, by default, easily, securely and [...] directly accessible to user' (Article 3.1). The data holder must provide the user with relevant information concerning data. Data holders' obligations are further elaborated in Chapter III of the DA, where it is also specified that they may receive compensation for making data available (Article 9). Secondly, the DA defines the right of users to access and use data (Article 4): a right that

[37] Among the other proposals and pieces of legislation based on Article 114 TFEU one may cite the Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1; the Regulation (EU) 2019/881 of 17 April 2019 on information and communication technology cybersecurity certification (Cybersecurity Act) [2019] OJ L151/15; the 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 (NIS 2 Directive) [2022] OJ L333/80; the Commission's Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative act COM (2021) 206 final; the Commission's Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (EU Chips Act) COM (2022) 46 final; the Commission's Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) COM (2022) 454 final; the Commission's Proposal for a Regulation establishing a framework for ensuring a secure and sustainable supply of critical raw materials (Critical Raw Materials Act) COM (2023) 160 final. More generally, Article 114 TFEU has acquired a leading role in adopting EU tools to preserve its strategic autonomy: see Yulya Miadzvetskaya and Ramses A. Wessel, 'The Externalisation of EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox' (2022) 7 European Papers 413, 438 <https://www.europeanpapers.eu/en/e-journal/externalisation-eu-cybersecurity-regime-cyber-diplomacytoolbox> accessed 1 October 2023.

should ensure access to data without undue delay, free of charge, and, where applicable, continuously and in real-time. Thirdly, the DA gives shape to the right to share data with third parties, upon request by a user or by a party acting on behalf of a user (Article 5). Should this be the case, the data holder shall make available the data under the same conditions that are applicable to the right of the user. Recital 36 of the DA specifies that data cannot be made available to large providers designated as 'gatekeepers' under the Digital Markets Act. Finally, it has to be noted that the obligations flowing from Chapter II are not applicable to data generated by micro or small enterprises.

Chapter V (Articles 14-22) introduces a uniform framework for the use by public bodies and EU institutional actors of data held by private subjects under exceptional circumstances. In particular, two different scenarios are envisaged. In the first one, data are requested to prevent, respond to, or assist in, the recovery from a public emergency (Article 15.a and 15.b). Note that the definition of 'public emergency' enshrined in the proposal is rather broad. According to Article 2.10

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

In the second scenario, data may be needed provided that the lack of their availability prevents the relevant public body from fulfilling a specific task in the public interest that has been explicitly provided by law (Article 15.c). By way of example, IoT data can be extremely valuable for weather predictions and climate monitoring in order to prevent and respond to natural disasters (such as floods, drought, and forest fires). Indeed, data coming from cars or telephones can contain precious information on surface pressure, which is one of the most fundamental parameters in atmosphere monitoring the weather forecast. Consequentially, by relying on Article 15.c, it can be argued that for EU public bodies and institutes such as the National Meteorological Services and the European Centre for Medium-Range Weather Forecasts (ECMWF), the dynamic of obtaining such data from private providers would greatly improve not only forecasts but also the verification of forecast and climate monitoring. Small and micro enterprises are expressly exempted from making data available in both scenarios (Article 14.2). Importantly, the DA imposes upon the public bodies an obligation to share data with individuals or organizations operating for research purposes only, and on a not-for-profit basis (Article 21). Specific provisions are included to promote and enhance mutual assistance and cross-border cooperation among public bodies regarding data exchange (Article 22).

Chapter VI of the DA (Articles 23–26) contains provisions intended to facilitate switching between data processing services, while Chapter VII (Article 27) introduces safeguards to prevent possible unlawful third-party access to non-personal data held in the Union. Chapter VIII (Articles 28–30) envisages specific interoperability duties and data sharing mechanisms and services for the operators of data spaces and identifies the essential requirements regarding smart contracts for data sharing.

The time has come to evaluate the DA.

THE EU DATA ACT: A CRITICAL EVALUATION

As one may expect, the DA has positive and negative features. The mechanisms put in place to prohibit unfair contracts in relation to B2B data sharing and make it easier for SMEs to access

data are remarkable.[38] Also positive is the provision imposing upon the Commission an obligation to develop and recommend non-binding model contractual terms on data access and use containing balanced contractual rights and obligations.[39] And one may also appreciate that, in line with the assertive approach enshrined in the notion of EU digital sovereignty, the DA perfectly illustrates the normative power of the Union—also known as the Brussel effect[40]—by defining a scope of application which is likely to produce a vast extraterritorial reach. In fact, DA's provisions apply to manufacturers of products sold on the EU market and to providers of data processing services offered in the EU, regardless of whether they may be located in a Member State. This is even more significant if one considers that the DA complements Article 20 of the GDPR, extending the scope of data portability rights to data generated by IoT.

However, like the DGA, the DA contains solutions likely to create tensions and uncertainties, requiring further and better elaboration by the supranational legislature. In particular, five specific points deserve to be mentioned.

To begin with, in the B2C and B2B schemes, several concerns have been raised about the position held by manufacturers and users. Some scholars stressed that the manufacturers' role remains predominant in the DA. It is very indicative that the DA does not pay much attention to the initial contract between the manufacturer (or seller) of a product or the provider of a service and the user. Indeed, although the need for a contractual agreement with the user undoubtedly represents a milestone, Article 3(2) only lists some transparency information to be included in the contract. This is a relevant gap in the legal framework at stake, considering that the rights and duties flowing from the DA complement those contained in that contract. Furthermore, others have highlighted that in the B2B constellations, the central role played by users (businesses in this case) requires a justification.[41] For instance, in such a scheme, it has to be further clarified by the EU legislature whether the generation of data through the use of IoT devices gives rise to 'certain limited and non-exclusive access, use and sharing rights for the user'.[42]

The second point concerns the possibility for public sector bodies and EU institutional actors to have access to data in exceptional cases. Even though the DA contains a definition of 'public emergency' functional to trigger the related mechanism, such a definition is vague and significantly broad. Thus, it remains unclear how it interacts with similar notions that are enshrined in some EU primary law provisions, such as Articles 107 (mentioning state aid to make good the damage caused by natural disasters or exceptional occurrences), 122 (mentioning severe difficulties caused by natural disasters or exceptional occurrences), 168 (referring to the fight against major health scourges and the cooperation in early warning of and combating serious cross-border threats to health), 196 (providing for the EU's contribution to the Member States' cooperation for preventing and protecting against natural or man-made disasters), 222 TFEU (introducing solidarity duties when a Member State is a victim of a terrorist attack, a man-made disaster or a natural disaster). Also unclear is how access to data by public entities, as described in the proposal, could interact with Member States' prerogatives concerning the protection of

[38] The DA introduces a specific unfair test for the assessment of contractual terms: Article 13. Clément Perarnaud and Rosanna Fanni, 'The EU Data Act. Towards a New European Data Revolution?, CEPS Policy Insight' (2022). <https://www.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-05_The-EU-Data-Act.pdf> accessed 1 October 2023, argue that such an innovation is likely to be opposed by dominant actors.

[39] DA, Article 34.

[40] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2019). On the extraterritorial reach of EU data law, see Christopher Kuner, 'The Internet and the Global Reach of EU Law', in Marise Cremona and Joanne Scott (eds) *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2019) and Elanie Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade And Cybersecurity* (Hart 2022).

[41] Matthias Leistner and Antonie Lucie, 'Attention, Here Comes the EU Data Act! A Critical In-Depth Analysis of the Commission's 2022 Proposal' (2022) JIPITEC <https://www.jipitec.eu/issues/jipitec-13-3-2022/5564> accessed 1 October 2023.

[42] ibid, 347.

public health, national security, and national defence, which the DA preserves. No doubt, the recognition of Member States' prerogatives in the DA is formally consistent with EU primary law. In this context, Article 4.2 TEU and Article 346 TFEU recognize a national security and defence privilege to the Member States, allowing the exercise of state-exclusive competencies in the domain at stake. This said, one also has to stress that the Court of Justice of the European Union has made it clear that 'the mere fact that a national measure has been taken to protect national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law'.[43] In light of the concerns raised by the Court regarding the potential impact of Member States' prerogatives on the effectiveness of EU law, it would have been preferable to specify better the interaction of the former on the mechanism enshrined in the DA.

The third point worth stressing concerns the interaction of the DA with other EU law instruments and EU policies. Precisely as in the case of the DGA, such an interaction, which is essentially based on the functioning of 'without prejudice' clauses, contributes to the establishment of a highly fragmented legal framework, which risks reducing the potential effectiveness of the EU tool in question.

The fourth point relates to the significant role that the DA attributes to Member States—something that has already been discussed in this article with regard to the DGA. As mentioned above, such a role is (partially) inherent in the nature of the competence exercised to adopt the DA, which is shared between the Union and its Member States. However, this does not prevent the EU legislature from further elaborating the cooperation mechanisms that should inform the EU's and Member States' roles to promote more coherence and effectiveness of the relevant legal framework. Likewise, the fact that Member States may (still) enjoy retained powers in the whole domain covered by the proposal does not entirely explain why the Commission decided to identify such powers so extensively. Besides the 'classical' retained powers that Member States enjoy in maintaining public order, national security and defence, and public health, the proposal mentions other areas—such as the customs policy—where the position of Member States is less strong.[44]

The fifth and final point is related to the lack, in the DA, of a sound analysis of data as a public asset potentially able to provide the foundations to build an Open Data economy. Precisely as in the case of economies based on open source, this would include creating standardized Data Sharing Agreements and Data User Agreements to create and support data infrastructures and curation not only to make the data available but also long-term accessible and reusable.

At least some of these points have been considered in the legislative process that will lead to adopting the final version of the DA. In particular, the consolidated compromise text of the DA is worth mentioning.[45] First, more attention is paid to the content of the initial contract concluded between the manufacturer (or seller) of a product—or the provider of related services—and the user, as well as to the reasonable compensation for data holders for costs incurred in providing direct access to the data generated by the user's product. Moreover, the co-legislatures do not ignore the need to stress further the awareness of users and businesses on the responsible offer and access to data. This explains why specific references to data literacy are included in the

[43] Joined Cases C-511/18, 512/18 and 520/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791, para 99. On the interaction between the EU and its Member States in security matters, see Federico Casolari, 'Regional Perspective: Distribution of Powers and Cooperation Patterns under EU Law as Applicable to CBRN Protection', in Andreas de Gutty and others (eds), *International Law and Chemical, Biological, Radio-Nuclear (CBRN) Events. Towards an All-Hazard Approach* (Brill Nijhoff 2022), stressing the role that the principle of sincere cooperation—enshrined in Article 4.3 TEU—may exercise to prevent that Member States' prerogatives may undermine the fulfilment of EU objectives.

[44] As it is well-known, the EU enjoys an exclusive competence in the context of the customs union (Article 3 TFEU).

[45] See n 5.

compromise text, requiring the Union and Member States to promote tools and measures in this respect.[46]

On a different note, both institutions propose a narrower definition of 'public emergency',[47] and require a more detailed procedure for making data available for public entities and EU institutional actors. In addition to this, the compromise text seems to presuppose a relevant limitation of the EU subjects that are entitled to have access to relevant data in case of exceptional need: while the Commission's proposal referred to 'Union institution, agency or body', thus including all possible categories of supranational actors, the agreed text refers only to the European Commission, the European Central Bank and Union bodies. The other EU institutions listed in Article 13 TEU (ie, the European Parliament, the European Council, the Council of the European Union, the Court of Justice and the Court of Auditors) should, therefore, be excluded from the personal scope of data sharing.[48]

Also worth mentioning are the amendments adopted for data sharing for scientific research or analytics. In particular, it is stated that individuals or organizations receiving data may keep it for up to 6 months following the erasure of the data by the public entity concerned. This specification could be seen as a restriction to promote access to data for research purposes, which seems to be not wholly consistent with some amendments to the Commission's proposal that have been proposed by the Council and welcomed by the research community.[49] Significantly, Article 40.2a of the compromise text formally recognizes such exceptionalism: the provision expressly states that the DA 'is without prejudice to Union and national law providing for access to and authorizing the use of data for scientific research purposes' with the sole exception of its Chapter V on data availability based on exceptional need.[50]

Cooperative schemes have been further detailed with regard to the B2B and B2C sharing schemes, as well as the switching process and the mutual assistance between Member States and the Commission in the implementation of the Regulation. The changes proposed in the compromise text also specify the right to an effective judicial remedy for users, data holders, and data recipients. Last but not least, efforts have been made to clarify better the interplay between the DA and other horizontal (eg, the GDPR) and sectoral EU legislation.

While some of the proposed changes will undoubtedly contribute to strengthening the effectiveness of the DA, one cannot ignore that some significant features of the proposed regulatory scheme—such as the access to data for research purposes and the interaction with other strands of EU legislation—are likely to remain vague or unsolved also after the agreement reached by the Parliament and the Council. For instance, the compromise text does not intervene to specify more precisely to what extent Member States' prerogatives may impact the DA's functioning.

Beyond the specific shortcomings of the DA, there is a cross-cutting issue that deserves comment. By and large, the DA seems to replicate the same regulatory approach adopted by the DGA. Unlike the indications emerging from the EU Data Strategy, the DA adopts a strict regulatory approach towards data management that could determine competitive disadvantages to

[46] Doc. A 004595, cit.

[47] According to the new definition given by the European Parliament in its amendments, 'public emergency' means 'an exceptional situation, *limited in time such as public health emergencies, emergencies resulting from natural disasters, as well as human- induced major disasters, including major cybersecurity incidents,* negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, *financial stability,* or the substantial *and immediate* degradation of economic assets in the Union or the relevant Member State(s) *and which is determined and officially declared according to the relevant procedures under Union or national law*'. Emphasis added. Doc. A 004595, cit.

[48] Doc. A 004595, cit.

[49] See 'Joint calls to the EU Co-Legislators to Promote Fair Access to Data for Research Purposes Through the Data Act' (2023) <https://www.the-guild.eu/publications/statements/joint-calls-to-the-eu-co-legislators-to-promote-fair-access-to-data-for-research-purposes-through-the-data-act.pdf> accessed 1 October 2023.

[50] Doc. A 004595, cit.

the EU tech groups operating in the global market.[51] It is thus helpful to add a short reference to the regulatory environments elaborated by the other two major players in global data governance, that is, the USA and China.[52]

THE COMPETITIVE, REGULATORY LANDSCAPE

Historically, as claimed by Amie Stepanovich, executive director at the Silicon Flatirons Centre at Colorado Law, the US legal framework on data has been characterized by 'a bunch of disparate federal [and state] laws'[53] showing no stated position on digital sovereignty. This way of dealing with the privacy of data led to a fragmented scenario of a mix of laws meant to target specific types of data, such as the Health Insurance Portability and Accountability Act, the Family Educational Rights and Privacy Act and the Video Privacy Protection Act, etc. Currently, only three states in the USA have comprehensive data privacy laws: California, Virginia, and Colorado. This means that, currently, there is no national IoT cybersecurity regulatory framework, nor a comprehensive federal law regulating the collection and use of personal information. However, in 2019, the Members of the Senate and the House of Representatives introduced the IoT Cybersecurity Improvement Act, a bill seeking to set minimum security standards for connected devices used by the federal government. Against this scenario, it is easy to understand why it has been argued that citizens might easily get confused and that there is a strong need for a consistent approach. Having said this, the USA appears to be inspired by a harms-prevention-based philosophy rather than a right-based one, such as the EU way of dealing with data governance, which, among other things, greatly influenced the upcoming data laws of California, Colorado, Connecticut, Utah, and Virginia.[54]

The absence of a comprehensive IoT regulatory framework is also visible in the approach so far adopted by China. This does not mean, however, that China lacks normative positions on data governance. Interestingly, the country seems to be trying to reconcile an approach based on a strong reaffirmation of the state cyber sovereignty—requiring strict regulation and control of data security—with the need to make a more flexible approach regarding data sharing possible. A clear illustration of this is contained in Article 7 of the 2021 Data Security Law, which reads as follows:

> The state shall protect the data-related rights and interests of individuals and organizations, encourage the lawful, reasonable, and effective use of data, ensure free flow of data in an orderly manner and in accordance with the law, and promote the development of a digital economy with data as the key factor.[55]

This article argues that by taking what is positive from other countries' experiences and ways of dealing with data, and setting aside the downsides, the EU should be encouraged to lean towards a more structured 'multilevel approach', where Member State's sectoral peculiarity is preserved according to a clear cooperation framework, and mechanisms allowing for some flexibility are

[51] cf. Andy Bounds and Javier Espinoza, 'Tech Groups Call for Changes to EU Data-Sharing Proposals' (*The Financial Times* 2023) <https://www.ft.com/content/8ce1f3a9-1859-499f-972e-d4801b9d44d1> accessed 1 October 2023.

[52] See also Giusella Finocchiaro, Luigi Balestra and Marina Timoteo (eds), *Major Legal Trends in the Digital Economy. The Approach of the EU, the US, and China* (Il Mulino 2022).

[53] Thorin Klosowki, 'The State of Consumer Data Privacy Laws in the US (And Why It Matters)' (*Wirecutter*, 6 September 2021) <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/> accessed 1 October 2023.

[54] Fredric D. Bellamy, 'U.S. Data Privacy Laws to Enter New Era in 2023' (*Reuters*, 12 January 2023) <https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/> accessed 1 October 2023.

[55] Data Security Law of the People's Republic of China, adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress on June 10, 2021, available at <http://www.npc.gov.cn/> accessed 1 October 2023. See also Xuechen Chen and Xinchuchu Gao, 'Comparing the EU's and China's Approaches In Data Governance', in Elaine Fahey and Isabella Mancini (eds), *Understanding the EU as a Good Global Actor. Ambitions, Values and Metrics* (Edward Elgar Publishing 2020), emphasizing that such an approach should lead to make usable original data, yet anonymized.

recognized and regulated. Significantly, the proposed approach is perfectly in line with the EU vision and that had already been pointed out by the European Strategy for Data, which affirmed that the measures put in place by the latter strategy 'should nonetheless take into account the specificities of individual sectors and the Member States'.[56] Yet, as rightly stressed by some scholars, against the US 'light-touch regulation', the EU 'prides itself on having the toughest regulation.'[57] Although it is understandable that the EU is simply asking to play by its rule when it comes to its internal market, such proposed reshaping of the EU approach would preserve its essence, that is, the respect of the fundamental values upon which the Union is based. A significant role could be exercised in this respect by the principle of sincere cooperation, representing a veritable cornerstone of the interplay between the Union and its Member States, requiring a 'full mutual respect [...] in carrying out tasks flowing from the Treaties'.[58] Indeed, the proposed cooperation framework could specify the mutual loyalty obligations informing the EU's and Member States' action, thus making sure that the EU's fundamental values are, in any case, respected.

CONCLUDING REMARKS

In this article, we have contextualized and evaluated the EU Data Act against the background of the general framework elaborated by the EU for supranational digital sovereignty in data management. The EU's objective is ambitious: developing a data-driven economy while preserving the EU's structural identity—meaning its fundamental values—and the complex allocation of competencies and prerogatives between the Union and its Member States. Implementing and harmonizing all these goals is far from easy. As usual, only time will tell whether the EU will be successful in its endeavour. One may expect revisions, improvements, and even changes in the general approach, especially in a context where digital innovation is still progressing so quickly and radically. The recent development of Large Language Models provides a remarkable example. At the moment, it seems that the first legal tools adopted in the wake of the new EU Data Strategy—namely, the DGA and the DA—still present shortcomings and gaps, which render it more challenging to pursue the EU's objective. Partly, this is due to the structural nature of the EU legal order, which is based on multilevel governance, implying a cohabitation between the Union and its Member States. In this case, a significant role may be exercised by the principle of sincere cooperation, which imposes upon the Union and its Member States mutual duties functional to the fulfilment of supranational objectives.[59] Partly, this situation results from an inevitable fragmentation of the different policies covered by the EU umbrella. However, some of the shortcomings illustrated in the previous sections directly flow from the choices made by the supranational legislature and other EU institutions involved in the law-making process. While it is unlikely that the text of the DA will be subject to further changes before its formal adoption, a more cautious and sound approach to further implementing and interpreting the EU data regulatory approach is still desirable and possible.

POST SCRIPTUM

Following the compromise text agreed on 14 July 2023, the final text of the DA has been adopted on 13 December 2023. cf 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 (Data Act) (2023) OJ L. The DA entered into foce on 11 January 2024 and it shall apply from 12 September 2025.

[56] See above,'Setting the Scene' section.

[57] Theodore Christakis, 'European Digital Sovereignty Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy' (2020) <https://ssrn.com/abstract=3748098> accessed 1 October 2023.

[58] Marcus Klamert, *The Principle of Loyalty in EU Law* (OUP 2014).

[59] Federico Casolari, 'EU Loyalty and the Protection of Member States' National Interests' in Marton Varju (ed), *Between Compliance and Particularism. Member State Interests and European Union Law* (Springer 2019).