

# Data Governance Act as an Instrument for Strengthening the European Union's Digital Sovereignty


Agnieszka Piskorz-Ryń

PhD habil., Associate Professor, Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw; correspondence address: ul. Kazimierza Wóycickiego 1/3, 01–938 Warszawa, Poland; e-mail: a.piskorz.ryn@uksw.edu.pl

 <https://orcid.org/0000-0001-9788-0988>

Marlena Sakowska-Baryła

PhD habil., Associate Professor, Faculty of Law and Administration, University of Lodz, ul. Kopcińskiego 8/12, 90–232 Łódź, Poland; e-mail: marlena.sakowska.baryla2@wpia.uni.lodz.pl

 <https://orcid.org/0000-0002-3982-976X>

## Keywords:

digital sovereignty,  
open data,  
data management,  
data brokering,  
protected data

**Abstract:** The Data Governance Act (DGA) aims to support the development of European data spaces in key sectors of the economy, reduce dependence on non-EU suppliers, and strengthen the data-driven economy. In this way, it will strengthen the EU's digital sovereignty. Achieving these objectives depends on consistent implementation of legislation, the elimination of interpretation gaps, and ensuring a balance between the free flow of data and the protection of public and private interests.

## 1. Introduction

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, hereinafter referred to as the DGA (Data Governance Act),<sup>1</sup> is one of the pillars of the European data strategy.<sup>2</sup> The EU has announced

<sup>1</sup> 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 (OJ L152, 3 June 2022).

<sup>2</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European

two major legislative initiatives to achieve its ambitions for a European data economy of the future: the Data Act<sup>3</sup> and the DGA. The latter regulates three areas of concern that have data and its availability as a common ground. The regulation covers the reuse of protected data, data altruism, and data intermediation services. Unlike other recently adopted regulations targeting large technology companies, the DGA introduces new forms of data governance to reduce the problem of data concentration in the hands of large technology companies.<sup>4</sup> This regulation is a key component of the strategy to strengthen the EU's digital sovereignty, combining legal, technological, and economic dimensions. By establishing trusted mechanisms for data sharing, regulating intermediaries, and promoting the idea of data altruism, this regulation can contribute to increasing the EU's competitiveness in the global market while maintaining a high standard of protection of fundamental rights. The Act is a part of the larger regulatory framework pursued by the EU for digitalization, data economy, artificial intelligence, and other important policy goals often approached under the label of digital sovereignty.<sup>5</sup> The DGA aims to improve the sharing and reuse of data while protecting the privacy and data-protection rights of EU citizens.<sup>6</sup> This regulation aims to shape a system of trust for people, services, and industry to share their data, in stark contrast to the extraction practices of digital media platforms. The goal of the DGA is to ensure digital solidarity and data sharing.<sup>7</sup> It also sets out organizational or technical solutions that promote data altruism. The regulation allows for the voluntary sharing of data and

---

strategy for data, COM(2020) 66 final (OJ L345, 31 December 2020), accessed May 15, 2025, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066>.

<sup>3</sup> 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) (OJ L, 2023/2854, 22 December 2023).

<sup>4</sup> Marta Maroni, "The Idea of Data and European Constitutional Imaginaries: an Immanent Critique of the Data Governance Act," *Rivista Internazionale di Filosofia del Diritto* 5 (2024): 285–315.

<sup>5</sup> Jukka Ruohonen and Sini Mickelsson, "Reflections on the Data Governance Act," *Digital Society* 2 (2023): 1–10, <https://doi.org/10.1007/s44206-023-00041-7>.

<sup>6</sup> Francesco Vogezang, "Four Questions for the European Strategy for Data," Open Future, April 12, 2022, accessed May 15, 2025, <https://openfuture.eu/blog/four-questions-for-the-european-strategy-for-data/>.

<sup>7</sup> Maroni, "The Idea of Data and European Constitutional Imaginaries," 285–315; Paweł Hajduk and Victor Obinna Chukwuma, "Digital Solidarity Through Spatial Data – An EU and

enables the creation of large data repositories for machine learning and data analysis. The EU has high hopes for it.

The purpose of this article is to assess the DGA as a regulatory instrument for building the EU's digital sovereignty. This article attempts to explain whether the DGA is one of the ways to strengthen this sovereignty. The assessment of the DGA is undertaken with regard to the reuse of protected data. This article poses the research question of whether the DGA is a tool for improving the EU's digital sovereignty. This is a topical issue given the ongoing debate on digital sovereignty and the nature of current relations, particularly between the US and Europe.

The article consists of four parts: the first contains an introduction, the second discusses the term digital sovereignty in the context of EU action, the third analyzes the DGA in the context of the approach to so-called protected data, and the fourth presents findings regarding the institutional infrastructure.

## 2. Digital Sovereignty

Today, in any mature information society, we no longer live online or offline but onlife, that is, we increasingly live in that special space, or infosphere, that is seamlessly analogue and digital, offline and online.<sup>8</sup> This reality poses new challenges for countries and, above all, for the EU. With the importance of information and communication technologies in every area of life, they have become environmental forces that shape and transform our reality. Therefore, we need to address the new challenges posed by these technologies and the information society.<sup>9</sup> Digital technologies can also bypass and invalidate the old models of institutionalized sovereignty.<sup>10</sup> If we recognize that technology shapes sovereignty, it means that we can influence the

---

African Perspective,” *GIS Odyssey Journal* 4, no. 2 (2024): 101–16, <https://doi.org/10.57599/gisoj.2024.4.2.101>.

<sup>8</sup> Luciano Floridi, “Soft Ethics, the Governance of the Digital and the General Data Protection Regulation,” *Philosophical Transactions of the Royal Society A* 376, no. 2133 (2018): 20180081, <http://doi.org/10.1098/rsta.2018.0081>.

<sup>9</sup> Luciano Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford: Oxford University Press, 2014).

<sup>10</sup> Paul Timmers, “Sovereignty in the Digital Age,” in *Introduction to Digital Humanism*, eds. Hannes Werthner et al. (Cham: Springer, 2024), 571–92, [https://doi.org/10.1007/978-3-031-45304-5\\_36](https://doi.org/10.1007/978-3-031-45304-5_36).

shaping of that technology.<sup>11</sup> We can demand that digital technology be designed to protect our values, human rights, and human dignity.<sup>12</sup> Hence, the idea of digital sovereignty has a “defensive” aspect.

To this end, EU institutions have long referred to the concept of digital sovereignty as an organizing principle.<sup>13</sup> This issue has become part of the EU’s public policy based on digital humanism.<sup>14</sup> The concept of EU digital sovereignty is linked to ensuring Europe’s strategic autonomy<sup>15</sup> and to political support aimed at enhancing it within the digital sphere. This requires the Union to update and adapt a number of existing legal, regulatory, and financial instruments, as well as to more actively promote European values and principles in areas such as data protection, cybersecurity, and ethically designed artificial intelligence (AI).<sup>16</sup>

The term digital sovereignty is contrasted with the concept of corporate digital sovereignty.<sup>17</sup> It is not unambiguous, and its meaning depends on the context.<sup>18</sup> The terms digital sovereignty and technological sovereignty

<sup>11</sup> Paul Timmers, “The Technological Construction of Sovereignty,” in *Perspectives on Digital Humanism*, eds. Hannes Werthner et al. (Cham: Springer, 2022), 213–18, [https://doi.org/10.1007/978-3-030-86144-5\\_28](https://doi.org/10.1007/978-3-030-86144-5_28).

<sup>12</sup> “Vienna Manifesto on Digital Humanism,” TU Wien, May 2019, accessed May 15, 2025, <https://caiml.org/dighum/dighum-manifesto/>.

<sup>13</sup> EU institutional actors have referred to the concept of digital sovereignty for several years. Viviane Reding, “Digital Sovereignty: Europe at a Crossroads,” EIB Institute, 2016, accessed May 15, 2025, <https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf>.

<sup>14</sup> Timmers, “Sovereignty in the Digital Age,” 571–92.

<sup>15</sup> Frances G. Burwell and Kenneth Propp, “The European Union and the Search for Digital Sovereignty: Building ‘Fortress Europe’ or Preparing for a New World?,” Atlantic Council Future Europe Initiative, June 2020, accessed May 15, 2025, <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>; Timmers, “Sovereignty in the Digital Age,” 571–92.

<sup>16</sup> Tambiana Madiaga, “Digital Sovereignty for Europe,” European Parliamentary Research Service, July 2020, accessed May 15, 2025, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

<sup>17</sup> Luciano Floridi, “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU,” *Philosophy & Technology* 33 (2020): 369–78, <https://doi.org/10.1007/s13347-020-00423-6>.

<sup>18</sup> Ausma Bernot, Diarmuid Cooney-O’Donoghue, and Monique Mann, “Governing Chinese Technologies: TikTok, Foreign Interference, and Technological Sovereignty,” *Internet Policy Review* 13, no. 1 (2024), <https://doi.org/10.14763/2024.1.1741>; Huw Roberts et al.,

are used. They are most often treated as synonyms.<sup>19</sup> The term digital sovereignty is political and postulative in nature.<sup>20</sup> The need to clearly define this concept for the purposes of the EU is also emphasized.<sup>21</sup> This is not an easy task in itself, as the difficulties in defining it concern its constituent elements, primarily the concept of sovereignty.<sup>22</sup>

Digital sovereignty is Europe's ability to act independently in the digital world.<sup>23</sup> Digital sovereignty is the authority to set rules that regulate and govern action and, hence, the (digital) governance process involves the exercise of the capacities afforded, a priori, by sovereignty. Sovereignty captures the capacity of an actor to act (it is something that is held), whereas governance concerns the interactions of sovereign actors and the nature of the act itself (it is something that is done).<sup>24</sup> Digital sovereignty is – especially in Europe – now often used as a shorthand for an ordered, value-driven, regulated and therefore reasonable and secure digital sphere. It is presumed to resolve the multifaceted problems of individual rights and freedoms, collective and infrastructural security, political and legal enforceability, and fair economic.<sup>25</sup> Looking at the many definitions formulated by various

---

“Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies,” *Internet Policy Review* 10, no. 3 (2021), <https://doi.org/10.14763/2021.3.1575>; differently André Barrinha and George Christou, “Speaking Sovereignty: The EU in the Cyber Domain,” *European Security* 31, no. 3 (2022): 356–76, <https://doi.org/10.1080/09662839.2022.2102895>.

<sup>19</sup> Roberts et al., “Safeguarding European Values with Digital Sovereignty”; differently Burwell and Propp, “The European Union and the Search for Digital Sovereignty.”

<sup>20</sup> Julia Pohle and Thorsten Thiel, “Digital Sovereignty,” *Internet Policy Review* 9, no. 4 (2020), <https://doi.org/10.14763/2020.4.1532>; Roberts et al., “Safeguarding European Values with Digital Sovereignty”; Dennis Broeders, Fabio Cristiano, and Monica Kaminska, “In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions,” *Journal of Common Market Studies* 61, no. 5 (2023): 1261–80, <https://doi.org/10.1111/jcms.13462>.

<sup>21</sup> Roberts et al., “Safeguarding European Values with Digital Sovereignty.”

<sup>22</sup> Rocco Bellanova, Helena Carrapico, and Denis Duez, “Digital/Sovereignty and European Security Integration: An Introduction,” *European Security* 31, no. 3 (2022): 337–55, <https://doi.org/10.1080/09662839.2022.2101887>.

<sup>23</sup> Madiega, “Digital Sovereignty for Europe.”

<sup>24</sup> Roberts et al., “Safeguarding European Values with Digital Sovereignty.”

<sup>25</sup> Annegret Bendiek and Jürgen Neyer, “Europas digitale Souveränität. Bedingungen und Herausforderungen Internationaler politischer Handlungsfähigkeit,” in *Demokratiethorie im Zeitalter der Frühdigitalisierung*, eds. Michael Oswald and Isabelle Borucki (Wiesbaden: Springer, 2020), 103–25.

authors, it is possible to identify their common features. The core of digital sovereignty stipulates the need for control over the digital on the physical layer (resources, infrastructure, devices), the code layer (standards, rules, design), and the information layer (content, data). Control implies the ability to influence and restrict the manufacturing (including the mining and processing of necessary raw materials), design, use, and outputs of digital technologies.<sup>26</sup>

The issue of ensuring digital sovereignty through EU action can be considered on several levels. One of these is data control, which is presented as an integral part of the EU's digital sovereignty.<sup>27</sup> The European data strategy serves this purpose. The EU's goal is, on the one hand, to ensure privacy and the protection of personal data while maximizing the benefits for the economy and society. This approach aligns with the underlying principles of the DGA. The aim of the regulation should be to further develop a borderless digital internal market and a data-driven society and economy that are human-centered, trustworthy, and secure (recital 3). The data governance regulation will ensure access to more data for the EU economy and society and provide for more control for citizens and companies over the data they generate.<sup>28</sup> The DGA is therefore linked in EU documents to digital sovereignty.<sup>29</sup> The term "data sovereignty" is often used instead of "digital sovereignty."<sup>30</sup>

To sum up this part of the discussion, it must be said that defining digital sovereignty is not an easy task. There is no recognized definition of this concept developed by the EU. Nor is there such a definition formulated in

---

<sup>26</sup> Gerda Falkner et al., "Digital Sovereignty – Rhetoric and Reality," *Journal of European Public Policy* 31, no. 8 (2024): 2099–120, <https://doi.org/10.1080/13501763.2024.2358984>.

<sup>27</sup> Roberts et al., "Safeguarding European Values with Digital Sovereignty."

<sup>28</sup> European Commission, Regulation on data governance – Questions and Answers, November 25, 2020, accessed February 15, 2025, [https://ec.europa.eu/commission/presscorner/detail/en/QANDA\\_20\\_2103](https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2103).

<sup>29</sup> Ibid.; "The Once Only Principle System: A Breakthrough for the EU's Digital Single Market," European Commission, November 5, 2020, accessed February 15, 2025, [https://ec.europa.eu/info/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-nov-05\\_en](https://ec.europa.eu/info/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-nov-05_en).

<sup>30</sup> Patrik Hummel et al., "Data Sovereignty: A Review," *Big Data & Society* 8, no. 1 (2021): 1–17, <https://doi.org/10.1177/2053951720982012>; Anupam Chander and Haochen Sun, "Sovereignty 2.0," Georgetown Law Faculty Publications and Other Works, 2404, University of Hong Kong Faculty of Law Research Paper No. 2021/041, <http://dx.doi.org/10.2139/ssrn.3904949>.

the literature. Nevertheless, this cannot be considered an obstacle to achieving the objective of this article. The context related to data is important in this regard. In this sense, the term is not only postulative. It should be seen as an objective of EU public policy. It concerns the EU's control over data at the information level.<sup>31</sup> It should also be linked to the regulation of access to data with respect for the axiological foundations and fundamental values of the European Union. Digital sovereignty in relation to data, understood in this way, forms the basis for the analysis that follows.

### 3. Reuse of Protected Data

The DGA regulates the rules for the reuse of specific categories of data. In this regard, it supplements Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019, on open data and the re-use of public sector.<sup>32</sup> It regulates the scope of matters excluded from the scope of the Directive (Article 1(2)). The DGA applies to protected data. Pursuant to Article 3(1) of the DGA, these are data protected by trade secrets, including commercial, professional, and business secrets; the confidentiality of statistical information; the protection of intellectual property rights of third parties; or the protection of personal data, unless such data is covered by Directive 2019/1024. The DGA is a coordination instrument that sets out rules for the handling of data to which the Open Data Directive does not apply. In this way, it ensures that new categories of data (protected data) may be reused where possible while respecting its protected nature and the rights of third parties. The DGA regulation is therefore complementary to Directive 2019/1024. The DGA fills the gap left by that directive, which only concerns the re-use of public documents and does not refer to protected data.<sup>33</sup> The regulation of data reuse at the EU level thus creates a coherent system. Only minor issues can be raised, as both acts have a partially different scope in terms of subject matter and entities covered. Due to the list of exemptions from the scope of the DGA contained in Article 3(2) of that regulation, a data space is created to which neither Directive 2019/1024 nor

---

<sup>31</sup> Falkner et al., "Digital Sovereignty," 2099–120.

<sup>32</sup> OJ L172, 26 June 2019, p. 56.

<sup>33</sup> Agnieszka Piskorz-Ryń, "European Data Governance Act – Essential Problems for Reuse of Public Sector Information," *Prawo i Więź* 53, no. 4 (2024): 322–33, <https://doi.org/10.36128/PRIW.VI53.1148>.

the DGA apply. There is therefore a gray area that is not regulated by either of these acts. In addition, problems may arise with the implementation of the Open Data Directive in national law and, as a consequence, affect the application of the DGA. This is the case in the Republic of Poland.<sup>34</sup>

Data to which the DGA applies is particularly protected against disclosure. Technical and legal procedural requirements must be met, primarily to ensure respect for the rights of others in relation to such data, or to limit the negative impact on fundamental rights, the principle of non-discrimination, and data protection (recital 6). Meeting such requirements is usually time-consuming and requires specialist knowledge. For this reason, such data were underused before the entry into force of the DGA. Few Member States had established structures, processes, or legislation to facilitate this type of data reuse. However, such measures were not taken across the Union. Brink and Ungern-Sternberg point out that one of the objectives of the Data Governance Regulation is to promote the reuse of certain categories of protected data held by public authorities, in the sense of technical and factual control over the data.<sup>35</sup> In this context, the DGA should be seen as a further step towards obtaining new categories of data for reuse. Opening up this resource would not have been possible without the proactive attitude of the EU and the completion of the regulatory landscape in this area.

Unlike the Open Data Directive, the DGA focuses on the protection of legally protected data. This act does not grant a public right to reuse protected data. Nor does it provide a basis for an obligation on obligated

---

<sup>34</sup> Agnieszka Piskorz-Ryń, “Spotkanie legislatorów prawa administracyjnego” [“Meeting of Legislators of Administrative Law”], in *Prawo administracyjne jako miejsce spotkań: Księga jubileuszowa dedykowana Profesorowi Jerzemu Supernatowi* [Administrative Law as a Meeting Place: An Anniversary Book Dedicated to Professor Jerzy Supernat], eds. Barbara Kowalczyk et al. (Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2024), accessed February 15, 2025, [https://bibliotekacyfrowa.pl/Content/149252/PDF/Prawo\\_administracyjne\\_jako%20miejsce\\_spotkan\\_ksiega\\_jubileuszowa\\_dedykowana\\_Profesorowi\\_Jerzemu\\_Supernatowi.pdf](https://bibliotekacyfrowa.pl/Content/149252/PDF/Prawo_administracyjne_jako%20miejsce_spotkan_ksiega_jubileuszowa_dedykowana_Profesorowi_Jerzemu_Supernatowi.pdf).

<sup>35</sup> Stefan Brink and Antje von Ungern-Sternberg, “DGA,” Beck’scher Online-Kommentar Datenschutzrecht, May 2023, accessed December 8, 2025, [https://beck-online.beck.de/dokument?vpath=bibdata%2fkomm%2fbeckokdatens\\_44%2fcont%2fbeckokdatens.inhaltsverzeichnis.htm](https://beck-online.beck.de/dokument?vpath=bibdata%2fkomm%2fbeckokdatens_44%2fcont%2fbeckokdatens.inhaltsverzeichnis.htm).



entities to allow the reuse of data. Nor does it provide a legal basis for exempting protected data from confidentiality obligations under Union or national law. The DGA does not interfere with this matter and does not amend existing provisions. It does not provide a legal basis for claiming the reuse of protected data. This solution is analogous to that adopted in the original text of Directive 2003/98/EC.<sup>36</sup> The DGA is “neutral” in terms of data rights, i.e., it does not affect the substantive legal provisions on access to data and their further use.<sup>37</sup> Each Member State, outside the scope of matters regulated by EU law, remains free to decide whether protected data are made available for reuse, including the purposes and scope of such access (recital 11). The DGA is therefore based on ensuring control over protected data. This act does not limit that control. From the point of view of digital sovereignty, the scope of control depends on the Union insofar as it exercises shared competences. Where the “occupied field” principle does not apply, responsibility lies with the Member States.

Nevertheless, this act can clearly be classified as regulatory action aimed at ensuring control over data by the Union or its Member States. This protection is intended to uphold important European values and fundamental rights. These include the protection of privacy and personal data, the protection of intellectual property, and the guarantee of economic freedom, including competition in the internal market.<sup>38</sup> Only statistical confidentiality cannot be linked to a specific EU fundamental right. It serves the performance of Community tasks,<sup>39</sup> while national statistics serve the tasks of the Member States. It allows for the collection of reliable, objective, and systematically provided information for EU bodies, national authorities,

---

<sup>36</sup> Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L345, 31 December 2003), 90–9.

<sup>37</sup> Brink and Ungern-Sternberg, “DGA.”

<sup>38</sup> Charter of Fundamental Rights of the European Union (OJ C303, 14 December 2007), p. 1, as amended, Articles 7, 8, 16, and 17(2).

<sup>39</sup> Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No. 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No. 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (Text with relevance for the EEA and for Switzerland) (OJ L87, 31 March 2009), 164–73, Article 1.

and the public. Public statistics therefore serve the public interest and activities aimed at achieving the common good. In this respect, they are instrumental in enabling the good administration of public affairs and the realization of other fundamental values and rights.

However, this is not enough. No regulation was needed to protect the rights and values identified. The scope of protection was already provided by EU and national data protection laws. They also set limits on data collection. However, the DGA has a special role as a set of rules on the reuse of protected data. It provides control over such data in a unique way. It regulates an area that was previously subject only to proactive measures and depended on the goodwill of Member States. The DGA standardizes procedures relating to protected data in order to reconcile the protected nature of the data and the rights of third parties. This means that the DGA establishes a regulatory framework for assessing:

- (1) whether protected data can be transferred for reuse with the consent of the data subjects or the permission of the data holders, or
- (2) whether protected data may be transferred for reuse after modification or processing in such a way that it no longer has a protected character, or
- (3) whether protected data may be transferred for reuse in a manner that respects intellectual property rights.

Under the DGA, the context of personal data protection is also important, as personal data also fall within the category of protected data. Article 3(1)(d) of the DGA provides that Chapter II of the Regulation, concerning the reuse of certain categories of protected data held by public sector entities, applies to data protected for reasons of personal data protection to the extent that it goes beyond the application of Directive 2019/1024. Recital 10 of the DGA indicates that this refers to personal data excluded or restricted from access for reasons of privacy and integrity of the natural person, in accordance with data protection rules. However, the DGA does not clearly distinguish between the scope of reuse under Directive 2019/1024 and the scope resulting from the DGA, which makes it difficult to determine which data “go beyond” the scope of the Directive. It seems that the intention of the EU legislator was to cover only personal data whose reuse is explicitly excluded under Directive 2019/1024, its implementing provisions, or EU and national sectoral legislation. It is therefore

not a question of all data subject to privacy restrictions, but of data for which the law expressly excludes the open data mechanism. However, it remains difficult to determine precisely which categories of personal data meet this criterion. Recital 6 of the DGA indicates the desire to make data collected by the public sector available in the public interest, even if it is personal data, while complying with the technical and legal requirements of the GDPR, Directive 2002/58/EC, and Directive (EU) 2016/680. Directive 2019/1024, in Article 1(2)(h), excludes from its scope documents, or parts thereof, containing personal data whose reuse would be incompatible with data protection rules. At the same time, it is without prejudice to the GDPR, and recitals 52–53 specify that the reuse of personal data is only permitted in accordance with the principle of purpose limitation and after a data protection impact assessment has been carried out, if necessary. Similar principles are contained in recital 154 of the GDPR and Article 86 of the GDPR, according to which the disclosure of personal data from official documents may only take place within the limits of EU or national law, in order to reconcile public access with the right to data protection. In the relationship between the DGA and the GDPR, it is clear that the DGA does not create additional grounds for the processing of personal data. In the relationship between the GDPR and Directive 2019/1024, the principle of non-infringement of data protection standards applies. However, the relationship between the DGA and Directive 2019/1024 with regard to Article 3(1)(d) is unclear and requires interpretation. The most likely interpretation is that this refers to data to which Directive 2019/1024 does not apply at all by virtue of an explicit statutory exemption.

“Non-protected data” is data whose reuse is permitted by Directive 2019/1024 and the provisions implementing it into national law. Its scope is determined taking into account the principles and conditions for the processing of personal data set out in Articles 5–6 of the GDPR (for ordinary data) and Article 9(2) of the GDPR (for special categories of data). As a result, the application of Article 3(1)(d) of the DGA requires a case-by-case analysis of potentially conflicting and complementary provisions of the GDPR, Directive 2019/1024, and national provisions, including sector-specific regulations. The lack of clear criteria in the DGA means that the practical identification of personal data covered by this regulation is subject to significant interpretative risk.

#### 4. Institutional Infrastructure

The DGA is a step towards democratizing data and opening it up, including protected data categories. Thanks to this regulation, the pool of data available for economic, scientific, and social purposes is to be expanded while respecting protected data and the interests of the data subjects or entities to whom the data relate, as well as public and private interests. The provisions of the DGA formalize the retention of control over data within the meaning of Article 3(1) in the process of its reuse. The significance of the DGA should not be seen solely as establishing a framework for the reuse of protected data. However, the content of the DGA regulations referred to above raises some reservations and justifies reflection on whether this regulation is indeed an effective tool for strengthening the EU's digital sovereignty. The answer to this question is affirmative, although it should be noted that ensuring digital sovereignty under the DGA requires appropriate institutional preparation and the development of additional legal instruments in the form of procedural mechanisms.

Due to the specific nature and complexity of the measures that the obligated entity must adopt to reuse data for the purpose of exercising control over data and ensuring the protection of rights and freedoms fundamental to the EU, it is very important to establish an infrastructure that facilitates reuse in Member States. The first element of this infrastructure is the appropriate entities. Each Member State must designate at least one competent entity. They should have the necessary legal, financial, technical, and human resources to perform the tasks assigned to them, including the necessary technical knowledge to comply with the relevant provisions of Union or national law on systems for accessing protected data. It is the responsibility of the Member State to provide these entities with the necessary resources. The task of the competent entities is to assist public sector entities. This assistance is intended to support them in their capacity as obligated entities and as potential users of data, as well as the data subjects. This assistance is to be provided at the request of such an entity. It may consist of proactive measures and include guidance and technical support on how best to structure and store data so that they are easily accessible (Article 7(4)(b)). Proper structuring of data will facilitate its provision upon request. In addition, it may include providing technical support by making

available a secure processing environment for access for the purpose of re-use of data (Article 7(4)(a)).

Another task of the competent entities is to provide technical support for pseudonymization and data processing in a manner that effectively protects the privacy, confidentiality, integrity, and availability of the information contained in the data for which reuse has been authorized, including techniques such as anonymization, generalization, masking, and randomization of personal data or other state-of-the-art privacy-preserving techniques, and the removal of confidential commercial information, including trade secrets or content protected by intellectual property rights (Article 7(4)(c)). It may also include providing assistance, where appropriate, to public sector entities in supporting re-users in requesting consent from data subjects for the reuse of data and from data holders for permission, in accordance with their specific decisions, including regarding the jurisdiction in which the data processing is to take place, and – where practicable – assisting public sector bodies in establishing technical mechanisms to enable the transmission of requests from reusers for consent or permission (Article 7(4)(e)). The competent entities may also substitute public sector bodies in examining requests for protected data (Article 7(2)). The actions of the competent entities show that control over protected data in the process of transferring it for reuse also includes the creation of an institutional framework to ensure control at the technical level. This includes ensuring a secure processing environment and serves to guarantee that data are processed in a manner that effectively protects the privacy, confidentiality, integrity, and availability of the information contained in the data for which reuse has been authorized.

## 5. Conclusion

The term digital sovereignty is a postulate. However, apart from the problems associated with its definition, it should be treated as an objective of EU public policy on data. It is difficult to determine in the long term whether it will continue to be a subject of scientific interest. At the moment, it certainly combines the important challenges facing the EU. It is therefore a concept that allows these challenges to be organized. This is also the case in the area described. In this respect, the DGA should be considered a regulatory

instrument for digital sovereignty. It guarantees control over data at both the legal and technical-organizational levels. It also serves to realize the values and protect the fundamental rights of the EU. The DGA is an important instrument for implementing EU policy on digital sovereignty, in particular by establishing a framework for the reuse of certain categories of data held by the public sector. Article 3(1)(d) provides that data protected for reasons of personal data protection are covered by the scope of the regulation, insofar as they go beyond the application of Directive 2019/1024. However, the lack of clear criteria for distinguishing between the scope of application of the two legal acts gives rise to interpretative doubts. As a result, the practical application of the DGA as a tool for strengthening the EU's digital sovereignty requires a thorough analysis of potentially conflicting and complementary legal norms on a case-by-case basis. The lack of clarity regarding the criteria for classifying data means that the implementation of the regulation's objective may encounter interpretative barriers, which justifies the need to clarify the relationship between the DGA and Directive 2019/1024 in future legislative measures.

## References

- Barrinha, André, and George Christou. "Speaking Sovereignty: The EU in the Cyber Domain." *European Security* 31, no. 3 (2022): 356–76. <https://doi.org/10.1080/09662839.2022.2102895>.
- Bellanova, Rocco, Helena Carrapico, and Denis Duez. "Digital/Sovereignty and European Security Integration: An Introduction." *European Security* 31, no. 3 (2022): 337–55. <https://doi.org/10.1080/09662839.2022.2101887>.
- Bendiek, Annegret, and Jürgen Neyer. "Europas digitale Souveränität. Bedingungen und Herausforderungen Internationaler politischer Handlungsfähigkeit." In *Demokratietheorie im Zeitalter der Frühdigitalisierung*, edited by Michael Oswald and Isabelle Borucki, 103–25. Wiesbaden: Springer, 2020.
- Bernot, Ausma, Diarmuid Cooney-O'Donoghue, and Monique Mann. "Governing Chinese Technologies: TikTok, Foreign Interference, and Technological Sovereignty." *Internet Policy Review* 13, no. 1 (2024). <https://doi.org/10.14763/2024.1.1741>.
- Brink, Stefan, and Antje von Ungern-Sternberg. "DGA." Beck'scher Online-Kommentar Datenschutzrecht, May 2023. Accessed December 8, 2025. [https://beck-online.beck.de/dokument?vpath=bibdata%2fkomm%2fbeckokdatens\\_44%2fcant%2fbeckokdatens.inhaltsverzeichnis.htm](https://beck-online.beck.de/dokument?vpath=bibdata%2fkomm%2fbeckokdatens_44%2fcant%2fbeckokdatens.inhaltsverzeichnis.htm).

- Broeders, Dennis, Fabio Cristiano, and Monica Kaminska. "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions." *Journal of Common Market Studies* 61, no. 5 (2023): 1261–80. <https://doi.org/10.1111/jcms.13462>.
- Burwell, Frances G., and Kenneth Propp. "The European Union and the Search for Digital Sovereignty: Building 'Fortress Europe' or Preparing for a New World?." Atlantic Council Future Europe Initiative, June 2020. Accessed May 15, 2025. <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>.
- Chander, Anupam, and Haochen Sun. "Sovereignty 2.0." Georgetown Law Faculty Publications and Other Works, 2404, University of Hong Kong Faculty of Law Research Paper No. 2021/041. <http://dx.doi.org/10.2139/ssrn.3904949>.
- European Commission. "The Once Only Principle System: A Breakthrough for the EU's Digital Single Market," November 5, 2020. Accessed February 15, 2025. [https://ec.europa.eu/info/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-nov-05\\_en](https://ec.europa.eu/info/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-nov-05_en).
- Falkner, Gerda, Sebastian Heidebrecht, Anke Obendiek, and Timo Seidl. "Digital Sovereignty – Rhetoric and Reality." *Journal of European Public Policy* 31, no. 8 (2024): 2099–120. <https://doi.org/10.1080/13501763.2024.2358984>.
- Floridi, Luciano. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & Technology* 33 (2020): 369–78. <https://doi.org/10.1007/s13347-020-00423-6>.
- Floridi, Luciano. "Soft Ethics, the Governance of the Digital and the General Data Protection Regulation." *Philosophical Transactions of the Royal Society A* 376, no. 2133 (2018): 20180081. <http://doi.org/10.1098/rsta.2018.0081>.
- Floridi, Luciano. *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality*. Oxford: Oxford University Press, 2014.
- Hajduk, Paweł, and Victor Obinna Chukwuma. "Digital Solidarity Through Spatial Data – An EU and African Perspective." *GIS Odyssey Journal* 4, no. 2 (2024): 101–16. <https://doi.org/10.57599/gisoj.2024.4.2.101>.
- Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. "Data Sovereignty: A Review." *Big Data & Society* 8, no. 1 (2021): 1–17. <https://doi.org/10.1177/2053951720982012>.
- Madięga, Tambiama. "Digital Sovereignty for Europe." European Parliamentary Research Service, July 2020. Accessed May 15, 2025. [https://www.europarl.europa.eu/regdata/etudes/brie/2020/651992/eprs\\_bri\(2020\)651992\\_en.pdf](https://www.europarl.europa.eu/regdata/etudes/brie/2020/651992/eprs_bri(2020)651992_en.pdf).
- Maroni, Marta. "The Idea of Data and European Constitutional Imaginaries: an Immanent Critique of the Data Governance Act." *Rivista Internazionale di Filosofia del Diritto* 5 (2024): 285–315.

- Piskorz-Ryń, Agnieszka. “European Data Governance Act – Essential Problems for Reuse of Public Sector Information.” *Prawo i Więź* 53, no. 4 (2024): 322–33. <https://doi.org/10.36128/PRIW.VI53.1148>.
- Piskorz-Ryń, Agnieszka. “Spotkanie legislatorów prawa administracyjnego” [“Meeting of Legislators of Administrative Law”]. In *Prawo administracyjne jako miejsce spotkań: Księga jubileuszowa dedykowana Profesorowi Jerzemu Supernatowi* [Administrative Law as a Meeting Place: An Anniversary Book Dedicated to Professor Jerzy Supernat], edited by Barbara Kowalczyk, Karolina Kulińska-Jachowska, Łukasz Prus, Magdalena Tabernacka, and Iwona Sierpowska, 255–61. Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2024. Accessed February 15, 2025. [https://bibliotekacyfrowa.pl/Content/149252/PDF/Prawo\\_administracyjne\\_jako%20miejsce\\_spotkan\\_ksiega\\_jubileuszowa\\_dedykowana\\_Profesorowi\\_Jerzemu\\_Supernatowi.pdf](https://bibliotekacyfrowa.pl/Content/149252/PDF/Prawo_administracyjne_jako%20miejsce_spotkan_ksiega_jubileuszowa_dedykowana_Profesorowi_Jerzemu_Supernatowi.pdf).
- Pohle, Julia, and Thorsten Thiel. “Digital Sovereignty.” *Internet Policy Review* 9, no. 4 (2020). <https://doi.org/10.14763/2020.4.1532>.
- Reding, Viviane. “Digital Sovereignty: Europe at a Crossroads.” EIB Institute, 2016. Accessed May 15, 2025. <https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf>.
- Roberts, Huw, Josh Cowsls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi. “Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies.” *Internet Policy Review* 10, no. 3 (2021). <https://doi.org/10.14763/2021.3.1575>.
- Ruohonen, Jukka, and Sini Mickelsson. “Reflections on the Data Governance Act.” *Digital Society* 2 (2023): 1–10. <https://doi.org/10.1007/s44206-023-00041-7>.
- Timmers, Paul. “Sovereignty in the Digital Age.” In *Introduction to Digital Humanism*, edited by Hannes Werthner, Carlo Ghezzi, Jeff Kramer, Julian Nida-Rümelin, Bashar Nuseibeh, Erich Prem, and Allison Stanger, 571–92. Cham: Springer, 2024. [https://doi.org/10.1007/978-3-031-45304-5\\_36](https://doi.org/10.1007/978-3-031-45304-5_36).
- Timmers, Paul. “The Technological Construction of Sovereignty.” In *Perspectives on Digital Humanism*, edited by Hannes Werthner, Erich Prem, Edward A. Lee, and Carlo Ghezzi, 213–18. Cham: Springer, 2022. [https://doi.org/10.1007/978-3-030-86144-5\\_28](https://doi.org/10.1007/978-3-030-86144-5_28).
- TU Wien. “Vienna Manifesto on Digital Humanism,” May 2019. Accessed May 15, 2025. <https://caiml.org/dighum/dighum-manifesto/>.
- Vogelezang, Francesco. “Four Questions for the European Strategy for Data.” Open Future, April 12, 2022. Accessed May 15, 2025. <https://openfuture.eu/blog/four-questions-for-the-european-strategy-for-data/>.