Unpacking B2G data sharing mechanism under the EU data act

Ludovica Paseri, Stefaan G. Verhulst*

ABSTRACT: The paper proposes an analysis of the business-to-government (B2G) data sharing mechanism envisaged by the Regulation EU 2023/2854, the so-called Data Act. The Regulation, in force since 11 January 2024, will be applicable from 12 September 2025, requiring the actors involved to put in place a compliance process. The focus of the paper is to present an assessment of the mechanism foreseen by the EU legislators, with the intention of highlighting two bottlenecks, represented by: (i) the flexibility of the definition of "exceptional need", "public emergency" and "public interest"; (ii) the cumbersome procedure for data holders. The paper discusses the role that could be played by in-house data stewardship structures as a particularly beneficial contact point for complying with B2G data sharing requirements.

KEYWORDS: Data sharing; Data Act; B2G; public emergency; EU Law; politics of data; data stewardship

SUMMARY: 1. Introduction – 2. B2G data sharing mechanism – 3. Assessing EU Data Act B2G data sharing mechanism – 3.1 Exceptional need: Public emergency and public interest – 3.2 Request assessment and procedure – 4. A need for data stewardship framework? – 5. Conclusions.

1. Introduction

On 11 January 2024, the EU Regulation 2023/2854, the so-called Data Act,[1] came into force, designed to enhance competition, innovation and fairness within the European Union's Digital Single Market. The goal of the EU institutions that led to the approval of the Data Act was to promote greater data sharing, strengthening the European data economy to make it more globally competitive, complementing the Data Governance Act, another pillar of the European data strategy. In this regard, the EU Commission Communication 66 of 2020, titled "A European strategy for data",[2] explicitly mentioned the Data Act in relation to the need to "provide incentives for horizontal

* *Ludovica Paseri: Postdoctoral researcher, Law Department, University of Turin. Mail: ludovica.paseri@unito.it; Stefaan G. Verhulst: The Data Tank, Mail: stefaan.verhulst@datatank.org.* *Ludovica Paseri authored Section 1; Section 3; Section 4; Stefaan G. Verhulst authored Section 2; Section 4; Section 5. Stefaan Verhulst would like to acknowledge the input received from Anna Colom, Marta Poblet and Paulina Behluli, all at The Data Tank, at earlier stages of the above paper. Contribution subject to double-blind peer review.*

[1] 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), ELI: http://data.europa.eu/eli/reg/2023/2854/oj.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy for data*, COM/2020/66 final, ELI: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066.

data sharing across sectors",[3] with specific reference to the need to "[F]oster business-to-government data sharing for the public interest".[4] Thierry Breton, European Commissioner for the Internal Market at the time of the presentation of the proposal of the Regulation in February 2022,[5] stated that "[S]o far, only a small part of industrial data is used and the potential for growth and innovation is enormous. The Data Act will ensure that industrial data is shared, stored and processed in full respect of European rules",[6] also making explicit reference to the Data Act's potential to strengthen European sovereignty in the digital domain. The Data Act thus becomes a pillar of the so-called "politics of data",[7] a formula that identifies the set of legislative provisions concerning data at European level developed from COM/2020/66 onwards, "considering the novelty of current human data-driven societies in accordance with a basic tenet of Aristotle's 'politics,' or 'practical sciences'".[8] Underlying the legal text is the urge to address the barriers to data sharing that hinder "an optimal allocation of data for the benefit of society",[9] represented by:

> "a lack of incentives for data holders to enter voluntarily into data sharing agreements, uncertainty about rights and obligations in relation to data, the costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, bottlenecks impeding data access, a lack of common data sharing practices and the abuse of contractual imbalances with regard to data access and use".[10]

In order to overcome these obstacles, the Regulation sets out three mechanisms for sharing data by companies to consumers (business-to-consumer, B2C), to other private actors (business-to-business, B2B) and to public entities (business-to-governments, B2G). The aim of this paper is to focus on the third type of data sharing mechanism, the one regulated in chapter V of the Data act, titled "Making data available to public sector bodies, the Commission, the European Central Bank and Union bodies on the basis of an exceptional need", although it will soon be applicable. This specific form of data transfer is currently under researched in the legal domain,[11] yet holding significant relevance for legal and jurisprudential studies. In particular, the purpose of the analysis is to evaluate and examine the possible implications of this new data-sharing mechanism regulated in a hard-law instrument, which will be applicable in a few months, involving both the public and private sectors.

Pursuing this intention, the study begins, in Section 2, with a description of the B2G mechanism as regulated in Chapter V of the Data Act, highlighting the context, conditions and procedural rules. Then,

[3] COM/2020/66 final, 13.

[4] *Ibid*.

[5] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, ELI: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0068.

[6] EU press release, *Data Act: Commission proposes measures for a fair and innovative data economy*, 23 February 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

[7] U. PAGALLO, *The politics of data in EU law: Will it succeed?*, in *Digital Society*, 1.3, 2022, 1-20.

[8] U. PAGALLO, *The politics of data in EU law*, cit., 2.

[9] Data Act, recital 2.

[10] *Ibid*.

[11] Consider, regarding critical analyses of the Data Act, not specifically addressed to B2G, but with a broader scope: W. KERBER, *EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation?*, in *Journal of Antitrust Enforcement*, 2024, 1-7.

Section 3 presents an assessment of this form of data sharing between businesses and public bodies, from which two main bottlenecks emerge. The first problematic aspect is about the definition of the concepts of exceptional need and public emergency, which are fundamental conditions underlying the data access requests (Section 3.1). The second bottleneck identified revolves around the procedure envisaged to fulfil data-sharing requests, which is burdensome both in terms of effort and timing (Section 3.2). This second aspect also concerns the control over the shared data and the responsibilities that burden both companies and public actors. The way the mechanism is currently structured reveals an intricate distribution of competences, as well as heavy demands on the actors involved. Against this background, Section 4 discusses the role that could be played by in-house data stewardship structures intended as a particularly fruitful contact point for complying with B2G data sharing requirements, in particular in the light of the elaborate mechanism imagined by the institutions. The configuration proposed here of data stewardship or data stewards, defined as "organizational leaders or teams empowered to create public value by re-using their organization's data (and data expertise)",[12] draws on two fundamental documents: the final report of the High-level expert group on business-to-government data sharing, released in 2020;[13] and the Commission assessment that accompanied the Data Act Regulation Proposal.[14]

The data stewardship architecture explored in this paper, as a benchmark in the compliance of companies with the Data act, on the one hand fulfils the need, emphasised by the High-level expert group,[15] for substantial and coordinated long-term funding and investment at all levels, both public and private, to ensure the future sustainability and innovation of official statistics in the information era. On the other hand, it exercises a function that goes beyond the regulatory framework of the Data Act, to acquire broader relevance in the context of EU politics of data, e.g. with reference to the Data Governance Act.

2. B2G data sharing mechanism

Chapter 5 of the Data Act (Artt. 14-22) outlines a framework for the responsible and controlled sharing of personal and non-personal data in situations of exceptional need, defining the scope and conditions of this data-sharing mechanism. Two main actors are involved: (i) data holders and (ii) public sector entities and Union institutions, agencies or bodies.

[12] S. G. VERHULST, *Wanted: Data stewards. (Re-)defining the roles and responsibilities of data stewards for an age of data collaboration*, The GovLab report, 2020, 4.

[13] A. GAGO-FERNANDEZ *et al.*, *Towards a European strategy on business-to-government data sharing for the public interest*, Publications Office of the European Union, Luxembourg, 2020, 1-116.

[14] Commission staff working document impact assessment report, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), SWD/2022/34 final, ELI: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0034.

[15] A. GAGO-FERNANDEZ *et al.*, *Towards a European strategy on business-to-government data sharing for the public interest*, cit., 28.

Data holders are defined in Article 14 Data Act, as "legal persons, other than public sectors bodies, which hold those data" and "shall make them available upon a duly reasoned request".[16] This effectively expands the previous business-to-government (B2G) framework of data sharing,[17] as the category of data holder may also include non-profit legal entities. Therefore, the Data Act's scope extends to private entities that were not covered by previous data requirements. Nevertheless, Article 15(2) Data Act specifically removes microenterprises and small enterprises from the obligations to share non-personal data as stipulated in the Chapter in the case of no public emergencies, limiting the regulatory burdens and costs associated with complying with data requests. Since it is usually large enterprises and platforms that hold most data and are also able to bear the costs associated with the data sharing process, this exclusion aims at addressing power asymmetries.[18]

Articles 14 and 15 Data Act further define the type of data that fall under the rules requiring to make data available based on exceptional need. Data includes "the relevant metadata necessary to interpret and use those data". Whereas no exclusions are specified in the case of requesting data for responding to a public emergency under Article 15(1)(a) Data Act, "personal data" is excluded from data that can be requested for other public service needs (Article 15(1)(b) Data Act). By stipulating the exclusion of personal data except in the case of responding to a public emergency, the Data Act ensures compliance with other EU regulations on data protection and individuals' privacy rights, such as the European Union's General Data Protection Regulation (GDPR).[19]

There are two scenarios in which B2G data sharing requests are envisaged: emergency and non-emergency situations. EU lawmakers defined distinct procedures for data sharing in each type of situation. Emergency situations are defined as instances "where the data requested is necessary to respond to public emergency".[20]

A non-emergency situation arises, only in relation to non-personal data, when a double condition occurs:

> "(i) a public sector body, the Commission, the European Central Bank or a Union body is acting on the basis of Union or national law and has identified specific data, the lack of which prevents it from fulfilling

[16] A definition of data holder is also given in Article 2(13) Data Act, defined as "a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service".

[17] Consider Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a common European data space*, COM/2018/232 final, 11-14, ELI: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0232:FIN.

[18] By excluding microenterprises and small enterprises from the obligations, the Data Act acknowledges the distinct challenges and limitations faced by smaller businesses in the digital landscape and safeguards microenterprises and small enterprises from undue regulatory burdens that could impede their growth and sustainability. On power (and information) asymmetries, see M. DURANTE, *Computational power: the impact of ICT on law, society and knowledge*, New York-London, 2021, 127-146.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[20] Article 15(1)(a) Data Act.

ISSN 2284-4503

> a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency; and
> (ii) the public sector body, the Commission, the European Central Bank or the Union body has exhausted all other means at its disposal to obtain such data, including purchase of non-personal data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data."[21]

Concerning the scenario of an emergency situation, Article 17 Data Act details the procedure to request data. In such requests, a public sector body or Union institution, agency, or body must comply with specific criteria, although it is not specified who deems these criteria to be fulfilled upon completion of the request. The process includes the requirement to clearly specifying the needed datasets, demonstrating the exceptional need for the data, explaining the purpose of the request[22] and justifying the choice of the data holder. In addition, the request must provide certain information related to data processing that appears to be in line with the legal provisions of the GDPR. The request must specify when the data are expected to be erased; indicate any other public sector and the third parties with which the data requested is expected to be shared with; and describe any technical and organisational measures necessary and proportionate to implement data protection principles.[23]

The request should be written, ensuring clarity and specificity.[24] It must respect the legitimate aims of the data holder, especially regarding the protection of trade secrets and it should be ensured that the requesting body makes its best effort to prevent the fulfilment of the request from leading to the liability of the data controller for infringement of Union or Member State law.

Furthermore, the request should be transmitted to the national competent authority or to the data coordinator that will closely cooperate with the Commission,[25] who will make the request publicly available online. The data coordinator is a competent authority, designate as coordinator in case a Member State identifies more than one competent authority for the Data Act.[26]

In addition, also the procedure for compliance with requests for data is regulated. When a data holder receives a request from a public sector body or Union institution, agency, or body under exceptional circumstances, the data holder must timely make the data available, considering the necessary technical, organisational, and legal measures (Article 18 Data Act). The data holder may decline or seek modifications to the request within specific timeframes, such as five working days for public

[21] Article 15(1)(b) Data Act.

[22] It is also mandatory to explain "the intended use of the data requested, including, where applicable, by a third party […], the duration of that use, and, where relevant, how the processing of personal data is to address the exceptional need", Article 17(1)(c) Data Act.

[23] This is needed just in case the data access request involves personal data, according to the definition of Article 4(1) GDPR, as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[24] Article 17(2)(a) Data Act.

[25] Chapter IX Data Act.

[26] Article 37(2) Data Act. The data coordinator is identified in order "to facilitate cooperation between the competent authorities and to assist entities within the scope of this Regulation on all matters related to its application and enforcement".

emergencies and thirty working days in other cases of exceptional need.[27] Grounds for refusal include: (i) the unavailability of data; (ii) insufficient security measures; (iii) a similar previous request not notified for data erasure;[28] (iv) non-compliance with conditions laid down in Article 17(1) and (2) Data Act regarding the security measures and purpose of request.

Additionally, if compliance with the request requires the disclosure of personal data, the data holder needs to "properly anonymise"[29] the personal data before making it available. In case of disputes, whether initiated by the public sector body or the data holder, Article 18(5) Data Act set out that the matter needs to be brought to the competent authority of the Member State where the data holder is established, in consideration of the right to submit a dispute to a civil or administrative court, following Union or national law.

It is then detailed the case of involvement of research organisations or statistical bodies in the context of exceptional needs (Article 21 Data Act). Public sector bodies or Union institutions, agencies, or bodies can share the data received with individuals or organisations for scientific research or analytics related to the data's requested purpose, "in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested; or with national statistical institutes and Eurostat for the production of official statistics".[30] The recipients of data pursuant Article 21 Data Act must then operate on a not-for-profit basis or within a recognized public-interest mission, excluding entities with *significant* commercial influence. What constitutes "significant" commercial influence is, however, not defined. When a public sector body or Union institution has the intention to transfer data to a third party carrying out scientific research or analytics necessary to fulfil the purpose for which the data is requested, the data holder must be notified, detailing the recipient's identity, contact details, purpose, and duration of data usage. The data holder has the right to object to this data transfer within five working days, escalating objections to the data coordinator if rejected by the public sector body, Union institution, agency, or body. Considering this complex mechanism, next section addresses two main bottlenecks identified, which risk undermining the implementation of the legislation.

3. Assessing EU Data Act B2G data sharing mechanism

Public sector bodies requiring data to be available to individuals and citizens is certainly not a novelty introduced by the Data Act.[31] Consider the case law that led the German Federal Constitutional Court

[27] Article 18(2) Data Act.

[28] If a data holder decides to decline the request or seek modification, Art. 18(4) Data Act states that the identity of the public sector body or Union institution that previously submitted a similar request must be indicated.

[29] The anonymisation is needed "unless the compliance with the request to make data available to a public sector body, the Commission, the European Central Bank or a Union body requires the disclosure of personal data. In such cases, the data holder shall pseudonymise the data", pursuant to Art. 18(4) Data Act.

[30] Article 21(1)(a)(b) Data Act.

[31] On this aspect recital 66 Data Act specifies that "[T]his Regulation […] is without prejudice to Union legal acts providing for mandatory information requests by public entities to private entities".

to the first formulation of the Principle of Informational Self-Determination in 1983,[32] the basis of the current European Data Protection legislation.[33] Even then, the issue was to understand what personal data the public sector held on citizens and what purposes they were processing it for.
However, the novelty here lies in the fact that the European legislator envisages a form of access to data, personal and non-personal, by including a further actor: the private actors who have the availability of such data, i.e. data holders. The novelty of the mechanism and its forthcoming application make it necessary to develop some thoughts on the more complex aspects of the mechanism. These aspects, investigated below, are represented by the definitional challenges related to the concept of "exceptional need", "public emergency" and "public interest", and by the cumbersome procedure, in terms of effort, time and control over data, which requires an organisational apparatus within the data holder's structure capable of being responsive to the requests.

3.1. Exceptional need: Public emergency and public interest

The B2G data sharing mechanism established in Chapter V of the Data Act revolves around the concept of exceptional need, which is evoked even from the heading of the chapter. The exceptional must be "limited in time e scope"[34] and it arises in two circumstances: public emergency and public interest.
The first case in which B2G data sharing is permitted is when the data are "necessary to respond to a public emergency" and the public actor requesting it "is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions".[35] In such a case, the request may involve both personal and non-personal data.
The second case in which a B2G data sharing is allowed for an exceptional need is when (i) the public actor requesting the data operates on the basis of the public interest, which has been established in advance by law (either of the Member State or of the Union) and (ii) the requestor "has exhausted all other means at its disposal to obtain such data". The latter case only concerns non-personal data. Consider that regarding the condition (i) (i.e., that public authority needs to operate for the public interest as established by law), the EU lawmakers provided two examples, such as "the production of official statistics or the mitigation of or recovery from a public emergency".[36] While the production of official statistics is less problematic, what is more challenging is the identification of what is meant by mitigation or recovery from a public emergency, concepts that are not clarified by the legislation, as also recently admitted by the European Commission.[37]

[32] J. EICHENHOFER, C. GUSY, *Courts, privacy and data protection in Germany: Informational self-determination in the digital environment*, in M. BRKAN, E. PSYCHOGIOPOULOU (eds.), *Courts, Privacy and Data Protection in the Digital Environment*, Cheltenham-Northampton, 2017, 103.
[33] D. HALLINAN, *Data Protection as a Normative Problem*, in M. DURANTE, U. PAGALLO (eds.), *De Gruyter Handbook on Law and Digital Technologies*, Berlin, 2025, forthcoming, 483-502.
[34] Article 15(1) Data Act.
[35] Recital 63 and Article 15(1)(a) Data Act.
[36] Article 15(1)(b)(i) Data Act.
[37] European Commission, *Frequently Asked Questions Data Act*, version 1.2, 2025, 26. In addition, it is underlined once again the central role of the national level: "The factors to be considered when identifying an activity as 'mitigation or recovery from a public emergency' are likely to be laid down in national law, because mitigation or recovery from a public emergency must be designated as a 'specific task carried out in the public interest, that has been explicitly provided for by law' in order to be relevant for Chapter V requests".

The defining problem of sharing for exceptional needs relates precisely to the two circumstances in which public emergency or public interest arise.

The Data Act provides a definition of public emergency, such as:

> "an exceptional situation, limited in time, such as a public health emergency, an emergency resulting from natural disasters, a human-induced major disaster, including a major cybersecurity incident, negatively affecting the population of the Union or the whole or part of a Member State, with a risk of serious and lasting repercussions for living conditions or economic stability, financial stability, or the substantial and immediate degradation of economic assets in the Union or the relevant Member State and which is determined or officially declared in accordance with the relevant procedures under Union or national law".[38]

Significantly, in addition, recital 64 Data Act, specifies that "[T]he existence of a public emergency should be determined or declared in accordance with Union or national law and based on the relevant procedures, including those of the relevant international organisations". The definition is very broad, identifying rather flexible conditions for the definition of public emergency. In addition, a considerable leeway remains with the Member States. This could result in a very different implementation and application of the B2G data sharing mechanism in the different Member States, hampering the objective of EU harmonisation of the matter.

The second case, which does not involve personal data, is strictly related to the so-called public interest, a very flexible concept, often evoked within the EU politics of data and poorly defined.[39] The concept of public interest permeates the entire architecture of the B2G data sharing mechanism of Chapter V of the Data Act. It is recalled in Article 14 Data Act, which states that the objective of these data requests is "to carry out its statutory duties in the public interest", as well as in recital 5 Data Act where it is emphasised that in this context the data "are necessary for the performance of a specific task carried out in the public interest".

The public interest is a concept that has generated debates in multiple data-related regulatory provisions.[40] Consider, for instance, the debate about the role of public interest, as a legal basis under Art.

[38] Article 2(29) Data Act.

[39] On the notions of public interest, see E.R. BOOT, *Public interest*, in *Oxford research encyclopedia of politics*, 2022.

[40] See, for instance, the role of public interest in the data altruism mechanism established in Chapter IV of the Data Governance Act: L. PASERI, *The ethical and legal challenges of data altruism for the scientific research sector*, in M. ARIAS-OLIVA, J. PELEGRIN-BORONDO, K. MURATA, M. SOUTO ROMERO (eds.), *The leading role of smart ethics in the digital world*, Logroño, 197. On the concept of public interest in the EU politics of data, see: L. PASERI, *Il governo dei dati. Pubblico interesse, altruismo, partecipazione*, Torino, 2025, 32-78.

6(1)(e) GDPR, in the context of personal data processed for research purposes.[41] In general, in relation to non-personal data, a broad interpretation also emerges according to the EU Court of Justice.[42]
This broad and often ambiguous interpretation that results from the combination of the three concepts of exceptional need, public emergency and public interest raises concerns about the potential for inconsistent application across Member States, leading to legal uncertainty for both data holders and public authorities. This is likewise implied in the control over the requested data, a matter that is explored in the next section.

3.2. Request assessment and procedure

Data holders who receive a request from a public authority are required to respond to the request, following the provisions of Article 18 Data Act, as described in Section 2. The data holder must in any case provide a response "without undue delay, taking into account necessary technical, organisational and legal measures" and there are three possible outcomes: (i) sharing the requested data; (ii) demanding modification of the request; (iii) rejecting the request.
Preliminarily, in order to formulate a response, the data holder is required to put in place a procedure that analyses the request received. It must, in the first instance, assess the formal elements of the request: whether it comes from a public body that has the legitimacy to make the request; and whether it is accompanied by all the elements required by Article 17 Data Act.[43] After that, the data holder needs to evaluate whether the public authority's justification for the choice of the specific data holder is "sufficient and clear".[44] This assessment is entirely left to the private actor, who is autonomously called upon to define the suitability of the level of clarity. In addition, the data holder is

[41] In that context, after many years, there are Member States without any specific legislation for the processing of personal data for scientific research purposes in the public interest, and in general the doctrinal debate has led to the assertion that "under the GDPR public interest can be described as an object worth safeguarding for the needs or interests of the Member States or the EU for the purposes of which a number of specific measures could be taken, including the rights of a data subject could be constrained", S. SLOKENBERGA, *Setting the foundations: Individual rights, public interest, scientific research and biobanking*, in S. SLOKENBERGA, O. TZORTZATOU, J. REICHEL (eds.) *GDPR and biobanking: Individual rights, public interest and research regulation across Europe*, Cham, 2021, 23.
[42] E.g., CJUE, Case C-809/23, *Sumitomo Chemical Agro Europe SAS v. Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES), Compagnie européenne de réalisations antiparasitaires SAS France (CERA),* ECLI:EU:C:2025:195, in relation to environmental data it is stated that: "[T]he public interest in accessing information on emissions into the environment is specifically to know not only what is, or foreseeably will be, released into the environment, but also to understand the way in which the environment could be affected by the emissions in question (judgment of 23 November 2016, Bayer CropScience and Stichting De Bijenstichting, C-442/14, EU:C:2016:890, paragraph 86)", 92.
[43] In particular, in relation to the type of data or dataset specifically requested by the public authority, it is specified that "here the sui generis database rights under Directive 96/9/EC of the European Parliament and of the Council (29) apply in relation to the requested datasets, data holders should exercise their rights in such a way that does not prevent the public sector body, the Commission, the European Central Bank or Union body from obtaining the data, or from sharing it, in accordance with this Regulation" (recital 71 Data Act).
[44] European Commission, *Frequently Asked Questions Data Act*, cit., 26.

required to comment on the proportionality of the exceptional need, as recently specified by the European Commission, by carrying out an assessment regarding "data scope and granularity".[45]

The procedure becomes even more complex if personal data are involved, because the data holder must examine whether the technical and organisational measures that the public authority pledges it will implement (pursuant to Article 17(1)(g) Data Act) are sufficient to safeguard the protection of "data protection principles".[46]

The data holder may refuse to fulfil the public actor's demand if the request does not comply with the requirement pursuant Article 17 Data Act; or if the data holder does not have the data; or in case the data holder has already received a similar request before.[47] In this case, therefore, it is implicitly necessary for the data holder to have a structure in place internally to ensure that requests received are logged or traced over time (for instance, through internal registry).

It should be noted that if the request succeeds the assessment, the data holder must share the data "without undue delay",[48] not further specified. If the data holder deems necessary to demand a modification of the request or refuse to share the data, the response shall be given "no later than five working days after the receipt of a request for the data necessary to respond to a public emergency and without undue delay and, in any event, no later than 30 working days after the receipt of such a request in other cases of an exceptional need".[49]

A further aspect warrants attention. After the preliminary verification of the request, if the decision is made to share the data, the data holder is expected to take "into account necessary technical, organisational and legal measures".[50] On this point, recital 72 Data Act states that "the making available of the data and their subsequent use should be accompanied by safeguards for the rights and interests of individuals concerned by those data", a burden that falls on the public authority, but that also seems to be on the data holder who evaluates the request and then executes it.

However, consider that it is not specified what the required measures (i.e. technical, organisational and legal) consist of. It is fair to admit that it will be up to the data holder to identify which measures to take, considering that "control over data […] is a crucial issue of power and geopolitics in current data-driven societies".[51]

Moreover, where the request involves personal data, the data holder is called upon to anonymise them or, if this is not possible, to put in place pseudonymisation techniques, which are necessarily costly operations that require a prompt organisation with the high level of expertise in order to fulfil the

[45] European Commission, *Frequently Asked Questions Data Act*, cit., 27. On "granular knowledge" in the "current legislation in digital matters", see H. CH. HOFMANN, *New Regulatory Approaches under the EU's Legislation on Digitalisation: Introduction to the Special Edition of the EJRR "Charting the Landscape of Automation of Regulatory Decision-Making"* in *European Journal of Risk Regulation*, 2025, 1-10.

[46] Article 17(1)(g) Data Act.

[47] Despite the fact that "[T]he burden on data holders should be minimised by obliging requesting entities to respect the once-only principle, which prevents the same data from being requested more than once by more than one public sector body or the Commission, the European Central Bank or Union bodies" (recital 69 Data Act), however, the duty to keep track of any requests lies with the data holder.

[48] Article 18(1) Data Act.

[49] Article 18(2) Data Act.

[50] Article 18(1) Data Act.

[51] U. PAGALLO, *The politics of data in EU law*, cit., 3.

ISSN 2284-4503

requests. Such a procedure, both in its preliminary phase and in the case of acceptance of the request and sharing of data, due to the number of steps and verifications, as well as the tight timeframe, is rather burdensome. Complexity may jeopardise the entire structure of the mechanism or risk compromising the protection of the rights involved, in particular the fundamental rights of the individuals concerned.

It is important to clarify that this is not meant to argue that this form of data sharing mechanism is unnecessary, especially when observed from the perspective of "imbalances created by data monopolies".[52] Rather, here it is claimed the need to develop structures within the organisation of the data holder to respond effectively to such requests, in order to catalyse a beneficial exchange of data, and avoid frustrating the underlying objectives of the legislation. A study carried out in 2022, on the prospect of mandatory B2G sharing, revealed "statistically significant results of business opposition to regulatory action and to mandating B2G data sharing, particularly among telecom and finance sectors",[53] shedding light on "the conflictual nature of information sharing and scrutinize the tensions and even 'failures' in business-government collaborations".[54] Given this scenario, it is therefore necessary to look at mechanisms from streamlining compliance, as discussed in the following section.

4. Need for data stewardship framework?

In the Commission staff working document impact assessment report which accompanied the proposal for the Data Act regulation of 2022,[55] the critical aspects related to the European data economy were identified and, subsequently, possible approaches to be pursued were mapped out. The most pressing issue was identified as the insufficient availability of data for business, on the one hand, and for social purposes, on the other.[56] Starting from this need, three different policy strategies were analysed and compared.

The first option envisaged the development of non-binding measures encouraging wider access and processing of data. This strategy would be based on self-regulation, merely suggesting practices for the promotion of data sharing.

The second strategy envisaged limited legislative measures aimed at enhancing legal certainty as to how data could be used and by whom, without, however, going so far as to adopt the approach of the

[52] B. DA ROSA LAZAROTTO, *The Implications of the Proposed Data Act to B2G Data Sharing in Smart Cities*, in *SSRN*, 2022,7. On risks related to the emergence of data monopolies and power imbalances, see also: N. HELBERGER, M. SAX, J. STRYCHARZ, H. W. MICKLITZ, *Choice architectures in the digital economy: Towards a new understanding of digital vulnerability*, in *Journal of Consumer Policy*, 2022, 1-26; M. BORGHI, B. WHITE, *Data extractivism and public access to algorithms*, in M. BORGHI, R. BROWNSWORD (eds.) *Law, Regulation and Governance in the Information Society: Informational Rights and Informational Wrongs*, New York, 2023, 105-125.

[53] I. SUSHA, J. SCHIELE, K. FRENKEN, *Business-to-government data sharing for public interests in the European union: results of a public consultation*, in M. JANSSEN *et al*. (eds.), *International Conference on Electronic Government*, Cham, 2022, 529. The study is based on the analysis of the open dataset of responses to the European Commission's public consultation.

[54] *Ibid*.

[55] EU Commission, Commission staff working document impact assessment report, cit.

[56] "[…] the overall problem tackled by this initiative is the insufficient availability of data for use and reuse in the European economy or for societal purposes", SWD/2022/34 final, 7. L. PASERI, *Il governo dei dati. Pubblico interesse, altruismo, partecipazione*, cit., 1-27.

Open Data Directive[57] oriented towards maximising forms of sharing, which embraced openness by default.

The third policy option proposed instead legislative measures designed to maximise the opportunities for parties to request access to data and a regime for B2G that would emulate the G2B approach under the Open Data Directive.

The choice for the Data Act Regulation fell on the second policy strategy, representing a middle way between the first, based on self-regulation, and the third, an expression of the top-down model, oriented towards the configuration of strong sharing obligations. The second policy strategy was in some ways similar to the third, with a more beneficial economic impact for the European economy.[58] Although both aimed to foster data availability, the third option proposed an approach striving for greater openness, increasing mandatory forms of sharing and significantly limiting data owners' control over access, compensation and safeguards. However, a central aspect of the third policy option was the introduction of the function of data steward, for both the public[59] and business sectors.[60] This policy option was directly impacted by the report of the High-level expert group on business-to-government data sharing, mentioned above,[61] also referred to in the European Data Strategy.[62] The High-level expert group recommendations included the establishment of national governance structures, the creation of a recognized data steward function, organising B2G collaborations in testing environments and public-private partnerships, and exploring an EU regulatory framework for B2G data sharing. The report highlighted the need for mechanisms ensuring accountability, transparency, and compliance with ethical principles in B2G data-sharing collaborations. It suggested transparency on collaborations, public awareness of benefits, and public involvement in choosing challenges. The creation of user-friendly data-donation mechanisms, ethical guidelines, and investments in training for a data-literate public sector were also recommended, identifying trust as a crucial factor.

Although the establishment of data stewardship frameworks is not an obligation under the Data Act, it is fair to admit that it can be a beneficial enabler for data-holder organisations both to take full advantage of the data in the availability of the company and to address the technical, legal and ethical challenges associated with data management. The introduction of a data steward function part of the data holder organisation would necessarily entail a cost, but it would also save considerable time making it easy to identify the competent data unit within each organisation. The data steward may be a single point of contact, within the individual organisations involved, mirroring that of the data coordinator, on the institutional side, introduced in Article 37 Data Act. Specifically, Article 37(2) Data Act

[57] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), ELI: http://data.europa.eu/eli/dir/2019/1024/oj.

[58] SWD/2022/34 final, 40-41.

[59] "Public sector as well as medium and large companies would be required to designate a function ('data steward') responsible for handling public sector bodies' requests transparently and consistently", SWD/2022/34 final, 164.

[60] "Data stewards would benefit in particular businesses that receive many requests for data", SWD/2022/34 final, 50.

[61] A. GAGO-FERNANDEZ *et al.*, *Towards a European strategy on business-to-government data sharing for the public interest*, cit., 90.

[62] "Foster business-to-government data sharing for the public interest also in the light of the recommendations included in the report of the Expert Group on Business-to-Government Data Sharing)" COM/2020/66 final, 13.

stipulates that, where more than one competent authority is designated at national level for the Regulation, the Member State is also required to identify a data coordinator, i.e. an entity pursuing a dual function, of cooperation and assistance. The first function, i.e., cooperation, concerns the relationship between the various authorities appointed at national level and is intended to coordinate their work.[63] The function of the data coordinator is akin to the data steward function, since both facilitate data sharing for a common good. However, data coordinators are related to each Member State whereas data stewards would be the corresponding function *within* a data holder organisation. The Data Act does not specify a requirement of having a designated function from the data holder side to fulfil the obligations although such a function would help harmonize the procedure across industries.

While the Data Act does not mandate the establishment of data stewardship frameworks, it is reasonable to acknowledge that such frameworks can serve as valuable enablers for data-holder organizations. They not only help maximize the utilization of available data but also assist in navigating the technical, legal, and ethical challenges of data management. The assumption underlying the establishment of a framework for data stewardship is that "[R]esponsible data handling requires building out a professionalized human infrastructure".[64]

Several definitions of data stewardship[65] and data stewards[66] have been proposed. Consider data stewardship as "individuals or teams within data-holding organizations who are empowered to proactively initiative, facilitate, and coordinate data collaboratives toward the public interest". The entry into force and forthcoming implementation of the Data Act highlights the growing potential of data stewardship structures as a key tool also for ensuring compliance with a regulatory framework whose complexity is increasing. In this regard, consider that developing internal structures that ensure responsible data management can also become an asset in relation to compliance with other regulatory frameworks. Consider, for instance, the data altruism mechanism as set out in the Data Governance Act. The first European entity registered as a Data Altruism Organisation, namely the Spanish DATALOG, in describing its experience claims that "[I]t is imperative for all data intermediary organisations to include similar positions in their governance structures to have adequate authority for data-driven decision-

[63] The coordination function is further specified in Article 37(5) Data Act where it is established that "[W]here designated, the data coordinator shall facilitate the cooperation referred to in points (f), (g) and (h) of the first subparagraph and shall assist the competent authorities upon their request", namely: (i) cooperation with the competent authorities of other Member States and, where appropriate, with the Commission or EDIB to ensure the consistent and efficient application of the Regulation (Art. 37(1)(f) Data act); (ii) cooperation with the relevant competent authorities entrusted with the implementation of other Union or national legal acts (Art. 37(1)(g) Data act); (iii) cooperation with the relevant competent authorities to ensure that Articles 23 to 31 and Articles 34 and 35 are applied consistently with other Union law and self-regulatory measures applicable to data processing service providers (Art. 37(1)(h) Data act).

[64] S. G. VERHULST, *Reimagining data responsibility: 10 new approaches toward a culture of trust in re-using data to address critical public needs*, in *Data & Policy*, 3, 2021, 6.

[65] S. G, VERHULST, *Data Stewardship Decoded: Mapping Its Diverse Manifestations and Emerging Relevance at a time of AI*, in *SSRN*, 1-10.

[66] The topic is highly debated in the field of science, concerning the management of research data, see, M. D. WILKINSON et al., *The FAIR Guiding Principles for scientific data management and stewardship*, in *Scientific data* 3, 1, 2016, 1-9.; L. PASERI, *Open science and data protection: engaging scientific and legal contexts*, in *J. Open Access L.* 11, 2023, 1-18.

making and ongoing development of new value propositions that enhance and align with their goals"[67] and have in fact equipped the organisation with a data steward whom they consider "a central figure"[68] in the framework. Time will be required to better understand, with empirical analysis, what the impact of the data stewardship framework may be within the organisation of the data holder, but the potential is remarkable considering the high stakes.[69]

5. Conclusions

The B2G data sharing mechanism introduced by the Data Act represents a significant step toward enhancing data access for public bodies in situations of exceptional need, in the EU. This paper offers a preliminary exploration aimed at highlighting key challenges that may hinder its practical implementation. First, the broad and flexible definitions of "exceptional need", "public emergency" and "public interest" may generate legal uncertainty, risking leading to divergent interpretation across Member states. This potential fragmentation risks undermining the harmonisation objectives of the Regulation[70] and complicates compliance processes of data holders.

Second, the procedural burdens placed on data holders, particularly in cases where they must demonstrate the exhaustion of alternative means before complying with a request, introduce operational complexities. These obligations could deter private entities from engaging in data sharing or lead to delays in responding to legitimate public interest needs.

In light of these challenges, the analysis assesses the opportunity to envisage a layer of governance within the organisations of data holders, described in terms of data stewardship, that deals with ethical and legal issues related to data. This paper does not aim to define the role of the data steward in legal terms, e.g., specifying responsibilities and duties,[71] or in economical one, i.e., proposing an empirical or economic cost-benefit analysis of its establishment. Rather, the purpose is to explore possible

[67] V. ESTIVILL-CASTRO, M. PORTELA CHARNEJOVSKY, G. MACCANI, *Addressing Challenges and Opportunities in Data Sharing for the Common Good: The Case of Europe's First Data Altruism Organisation*, in *2024 IEEE Smart Cities Futures Summit (SCFC)*, 2024, 48.

[68] *Ibid*. In M. PONTI, *et al.*, *Unlocking Green Deal data – Innovative approaches for data governance and sharing in Europe*, Publications Office of the European Union, Luxembourg, 63, it has been claimed that "the development of data stewardship capabilities would be relevant in a data altruism model in order to better identify opportunities for data reuse and for conditions of general interest. Data stewards might be a needed support raising awareness, as well to navigate the complexities of data altruism for environmental data and for steering responsible data sharing and data reuse within data altruism initiatives".

[69] J. J. ZYGMUNTOWSKI, L. ZOBOLI, P. NEMITZ, *Embedding European values in data governance: A case for public data commons*, in *Internet Policy Review*, 10, 3, 2021, 1-29.

[70] The purpose of harmonization is made explicit in recital 4 Data Act: "In order to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data, it is necessary to lay down a harmonised framework specifying who is entitled to use product data or related service data, under which conditions and on what basis. Accordingly, Member States should not adopt or maintain additional national requirements regarding matters falling within the scope of this Regulation, unless explicitly provided for herein, since this would affect its direct and uniform application. Moreover, action at Union level should be without prejudice to obligations and commitments in the international trade agreements concluded by the Union".

[71] On these aspects, see S. VERHULST, *Wanted: Data Stewards — Drafting the Job Specs for A Re-imagined Data Stewardship Role*, in *Medium*, 2023; and S. G. VERHULST, *Wanted: Data stewards. (Re-)defining the roles and responsibilities of data stewards for an age of data collaboration*, cit., 8-15.

approaches on potential forms of compliance support. To achieve this goal, the paper argues that the role of in-house data stewardship function or structure may represent a fruitful mechanism from streamlining compliance. By serving as a dedicated structure between data holders and public authorities, these structures could facilitate more efficient data access for re-use while ensuring adherence to regulatory provisions. In light of this preliminary exploration, it will be worthwhile to develop some research strands in the future. In particular, the interplay between the Data Act and the GDPR (especially regarding the application of Article 18(4) Data Act), as well as the study of alternatives to the B2G mechanism under Article 15 Data Act, need to be further investigated in order to assist the implementation of the Data Act. Moving forward, further regulatory guidance and best practices will be essential to balancing the need for data accessibility with legal clarity and operational feasibility.