Between the Data Act and the GDPR: Attributing Responsibility for Data Sharing

by

Antoni Napieralski*

CONTENTS

Abstract

The normative links between the GDPR and the Data Act increase the complexity of attributing responsibility for data sharing under the Data Act. Due to overlaps in the material scope of the GDPR and the Data Act, exercising access rights stipulated by the DA leads to consequences in attributing controllership under the GDPR. Users who are not data subjects, together with third parties receiving the requested data, are likely to become joint controllers. Judicial interpretation of the concept of joint controllership effectively lowered the threshold of becoming

* Antoni Napieralski, Dr, Assistant Professor at the Department of European Economic Law, Faculty of Management, University of Warsaw, Research Fellow at the University of Vienna; e-mail: a.napieralski@uw.edu.pl; ORCID: https://orcid.org/0000-0002-0576-0733.

Suggested Citation: Antoni Napieralski, 'Between the Data Act and the GDPR: Attributing Responsibility for Data Sharing' (2024) 17 YARS pp. 127–145.

Article received 6 January 2024, accepted 6 June 2024.

Yearbook of Antitrust and Regulatory Studies, Vol. 17, No. 29, pp. 127–145 • ISSN 1689-9024
https://doi.org/10.7172/1689-9024.YARS.2024.17.29.4

a joint controller. In pursuit of the effective protection of the data subject, joint controllership becomes an unintended consequence of mechanisms introduced by the Data Act.

Resumé

Les liens normatifs entre le GDPR et la Data Act augmentent la complexité de l'attribution de la responsabilité du partage des données en vertu de la Data Act. En raison des chevauchements du champ d'application matériel du GDPR et de la loi sur les données, l'exercice des droits d'accès stipulés par la DA entraîne des conséquences dans l'attribution de la responsabilité du contrôle en vertu du GDPR. Les utilisateurs qui ne sont pas des personnes concernées, ainsi que les tiers qui reçoivent les données demandées, sont susceptibles de devenir des responsables conjoints du traitement. L'interprétation judiciaire du concept de contrôle conjoint a effectivement abaissé le seuil à partir duquel il est possible de devenir un responsable conjoint du traitement. Dans l'optique d'une protection efficace de la personne concernée, le contrôle conjoint devient une conséquence involontaire des mécanismes introduits par la loi sur les données.

Key words: data sharing; GDPR; Data Act; controller; user; data holder.

JEL: K20, K23, K29

I. Introduction

This article analyses the normative links between the attribution of responsibility for accommodating access rights under the Data Act (hereinafter: DA)[1], and the attribution of controllership under the General Data Protection Regulation (hereinafter: GDPR).[2] While the existence of these links is not controversial, it has consequences as to the scope of potential liability for third-party data sharing.

The existence of the normative links between the DA and the GDPR is a consequence of overlaps in their material scope. While the GDPR applies to

[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) [2023] OJ L 2023/2854.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119.

any processing of personal data[3], the scope of the DA encompasses personal, as well as non-personal data generated by users of connected products and related services.[4] The overlap can be identified with regard to readily available data, which simultaneously qualify as personal data.[5]

As this article argues, the overlaps in attributing responsibility for data sharing under the DA have twofold implications. First, the data sharing mechanisms in the DA contribute to creating a complex landscape of controllership. Specifically, it is likely that accommodating access right under Article 5 DA will lead to establishing a joint controllership between a user and the receiving third party. Second, data holders, which simultaneously qualify as controllers, will be exposed to potential data protection liability in the course of accommodating DA access rights.

Accordingly, this article is structured as follows. First, the article provides an overview of the current understanding of the key legal roles defined in the GDPR (controller, joint controller, data subject) and in the DA (data holder, user). It builds upon the historical development of the GDPR definitions, in order to emphasise the differences in the underlying principles shaping the roles introduced in the GDPR and in the DA. Second, the above definitions are applied to data sharing scenarios foreseen in the DA. Specifically, the third-party data sharing mechanism in Article 5 DA is scrutinised. In conclusion, the final section analyses the implications of the overlaps between the GDPR and the DA with regard to the attribution of responsibility for data sharing.

II. Actors in the GDPR and in the DA

The following section analyses the legal roles defined in the GDPR and the DA. The assignment of roles is central to the operationalization of the data sharing regime stipulated by the DA. The roles defined under the GDPR and the DA are non-exclusive in their parallel application.[6] A single entity can simultaneously qualify as (for example) a controller and a user.[7] However, the non-exclusive character of the roles unveils an underlying tension. The

[3] With exceptions introduced in Art. 2 GDPR.

[4] Art. 1 DA.

[5] Art. 2(17) DA: '"readily available data" means product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation'.

[6] See Björn Steinrötter, 'Verhältnis von Data Act und DS-GVO. Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung' (2023) 4 Gewerblicher Rechtsschutz und Urheberrecht 216, 219–220.

[7] See Recital 34 DA.

GDPR's concept of a controller is phase-oriented and does not preclude one dataset from having multiple controllers, each in respect of a different data processing operation. The roles defined by the DA are dataset-oriented, i.e. a certain role (e.g. data holder, user) is assigned to a dataset. This distinction is analysed in detail in the following sub-sections.

1. The GDPR

The attribution of roles under the GDPR is rooted in real-world practices of persons and entities involved. Becoming a controller or a data subject is non-negotiable, as it is rather a legal consequence of one's status (for a data subject) and actions (for a controller or a processor).[8] The GDPR roles are an autonomous concept of EU law.[9]

The role of a 'data subject' is defined as an identified, or identifiable natural person.[10] The data subject is therefore defined by a reference to a link between a natural person and personal data. Whether the link can be established, depends on meeting the threshold of identifiability. However, regardless of the circumstances and the context in which data may be placed, data originating from any given individual may relate only to that individual. Data cannot be attributed to a different data subject depending merely on the context. Regardless of the actions undertaken, the link between data and a data subject remains (with a notable exception of anonymization).

The notion of a data subject can be traced back to the world's first data protection legislation from the German state of Hessen in 1970.[11] The 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter: OECD Guidelines) marked the direction for subsequent legislation.[12] The data subject was defined as 'an identified or identifiable individual'.[13] The definition of the data subject introduced in the OECD Guidelines has been directly re-used in the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing

[8] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.1' (2021), 12 <https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf> accessed 27 December 2023.

[9] Regina Becker and others, 'Applying GDPR Roles and Responsibilities to Scientific Data Sharing' (2022) 12 International Data Privacy Law 207, 208; Alexandra Giannopoulou, 'Allocating Control in Decentralised Identity Management' (2022) European Review of Digital Administration & Law 75, 82; European Data Protection Board (n 8) para 13.

[10] Art. 4 (1) GDPR.

[11] Hessisches Datenschutzgesetz 1970 (GVBl II 300-10).

[12] Art. 1 (b) OECD Guidelines: 'an identified or identifiable individual (data subject)'.

[13] Ibid.

of Personal Data (hereinafter: Convention 108).[14] The EU Directive 95/46/EC (hereinafter: Data Protection Directive), and later the GDPR, have accepted the above definition, with some alterations.[15] The Data Protection Directive and the GDPR have modified the subject of the definition, replacing the 'individual' with a 'natural person'.[16] Nevertheless, the core element of the definition, i.e. the threshold of identifiability as the decisive criterion, remained unchanged. The following table presents the aforementioned definitions of the data subject.

Figure 1. Data subject's definitions

	OECD Guidelines	**Convention 108**	**Data Protection Directive**	**GDPR**
Data subject	an identified or identifiable individual	an identified or identifiable individual	an identified or identifiable natural person	an identified or identifiable natural person

In terms of attributing responsibility under the GDPR, 'controllership' is the central concept. The responsibility of a processor is a derivative of the responsibility of a controller. The limits of the responsibility of a processor are drawn by the instructions from the controller.[17] Should the processor engage in processing beyond the scope of its controller's instructions, it would qualify as an independent controller.[18] Therefore, the role of a processor is not considered further in this article.[19]

The role of a 'controller', beginning with the OECD Guidelines, has been defined functionally.[20] According to these definitions, a controller is a person or entity with actual influence over the purposes and modalities of processing personal data. The following table illustrates the evolution of the notion of a controller.

[14] Council of Europe, 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (28 January 1981).

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

[16] Art. 2 (a) Convention 108: 'an identified or identifiable individual ("data subject")'; art. 2 (a) of the Data Protection Directive: 'an identified or identifiable natural person ("data subject")'.

[17] Art. 28(3) GDPR.

[18] Art. 28(10) GDPR; see Michèle Finck, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11 International Data Privacy Law 333, 334.

[19] See also Recital 22 DA: 'Processors as defined in Article 4, point (8), of Regulation (EU) 2016/679 are not considered to act as data holders'.

[20] Art. 1 (a) OECD Guidelines; art. 2 (d) of the Convention 108; art. 2 (d) Data Protection Directive; Yordanka Ivanova, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' (1 March 2020), 4 <https://papers.ssrn.com/abstract=3584207> accessed 29 July 2023; Giannopoulou (n 9) 82.

Figure 2. Controller's definitions

OECD Guidelines	'data controller' means a party who, according to domestic law, is competent to **decide about the contents and use of personal data** regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
Convention 108	'controller of the file' means the natural or legal person, public authority, agency or any other body who is competent according to the national law to **decide what should be the purpose of the automated data file**, **which categories of personal data should be stored** and **which operations should be applied to them**;
Data Protection Directive	'controller' shall mean the natural or legal person, public authority, agency or any other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
GDPR	'controller' means the natural or legal person, public authority, agency or other body which alone or jointly with others **determines the purposes and means of the processing** of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Pursuant to the GDPR, controllership can be attributed either through legal designation or through actual control over personal data processing.[21] The legal designation can be either explicit or implicit.[22] Explicit legal designation takes place when a provision explicitly appoints a specific entity as a controller.[23] Implicit legal designation is characteristic of provisions that impose an obligation to perform a specific task, in the course of which personal data must be processed.[24] In consequence, such a provision prescribes a specific purpose for the processing of personal data.[25] Implicit legal designation is often associated with the performance of a public task.[26] Controllership attribution through factual influence is characterised by a case-by-case analysis of factual circumstances of each processing activity[27].[28]

[21] Case C-231/22 *Belgian State (Données traitées par un journal officiel)* EU:C:2023:468, Opinion of AG Medina, para 50; European Data Protection Board (n 8), para 21.

[22] European Data Protection Board (n 8) paras 23–24; see also Becker and others (n 9) 9.

[23] European Data Protection Board (n 8) para 23.

[24] European Data Protection Board (n 8) para 24.

[25] Ibid.

[26] Ibid.

[27] Ibid., paras 25 ff.

[28] The underlying purpose of the DA, i.e. facilitating data sharing and incentivising data economy in the EU, cannot be treated as a purpose of processing within the meaning of the GDPR (Recital 4 DA). Under the GDPR, data sharing is a processing activity, not a purpose

The definition of a controller, in so far as it relates to the attribution through control over data processing, is (in principle) based on actions taken towards data: determining means and purposes of processing. The definition of a controller is thus a functional one.[29] The scope of actual control over data processing outweighs any contractual arrangements allocating responsibility for data processing.[30] Crucially, the definition of controllership rests upon the control over *processing* of data, not mere control over a given *dataset*.[31]

Controllership is attributed per each phase of processing (e.g. collection, storage, consultation, use, erasure).[32] The CJEU has established that processing personal data can be divided into individual phases of processing, each requiring a separate controller.[33] This means that one single piece of data originating from one data subject can have multiple controllers, depending on what processing activities will be carried out: with a different controller responsible for the collection of data, sharing of that data, and erasure of that data. This approach has been somewhat criticized as diverging too far from the letter of the GDPR.[34] As argued by Finck, complex networks of responsibility essentially lower the protection of data subjects.[35] However, the advantages of the phase-oriented approach have also been recognised.[36] The phase-oriented approach is useful in attributing liability in a multi-controller environment,

---

of processing (Art. 4(2) GDPR). As a consequence, any data sharing exercised through the Arts. 4–5 DA, will still require defining the purpose of processing within the meaning of the GDPR. As establishing purposes of processing lies within the scope of the responsibilities of the controller, it is likely that for DA-induced data sharing, the factual influence method, rather than its legal designation, will be appropriate in determining controllership. Therefore, the legal designation method is not considered further.

[29] Michèle Finck (n 18) 334; Yordanka Ivanova (n 20) 4; European Data Protection Board (n 8) para 12.

[30] See Case C-683/21 *Nacionalinis visuomenės sveikatos centras* EU:C:2023:949, para 45.

[31] Becker and others (n 9) 209.

[32] Case C-40/17 *Fashion ID* EU:C:2019:629, para 85; see also René Mahieu and Joris van Hoboken 'Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?' (European Law Blog, 30 September 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed 29 July 2023.

[33] Case C-40/17 *Fashion ID* (n 32) para 85; Case C-210/16 *Wirtschaftsakademie* EU:C:2018:388, para 43; see also Jörg Pohle, 'Die immer noch aktuellen Grundfragen des Datenschutzes' in Hansjürgen Garstka and W Coy (eds), *Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis* (Berlin: Helmholtz-Zentrum für Kulturtechnik, Humboldt-Universität zu Berlin 2014) 52; Wilhelm Steinmüller and Bernd Lutterbeck, 'Grundfragen Des Datenschutzes' (1971) Gutachten im Auftrag des Bundesministeriums des Innern 57–59 <https://dserver.bundestag.de/btd/06/038/0603826.pdf> accessed 16 August 2023.

[34] René Mahieu and Joris van Hoboken (n 32).

[35] Michèle Finck (n 18) 334.

[36] Regina Becker and others (n 9) 218.

especially, when multiple actors simultaneously process personal data for multiple purposes.

In its reasoning, the Court applies the principle of effective and complete protection of the data subject.[37] The principle of effective and complete protection of the data subject justifies a broad interpretation of the term controller.[38] Already in *Google Spain*, the CJEU ruled that in light of this principle, a search engine operator cannot be excluded from the scope of the term 'controller', merely on the grounds that processed personal data is hosted on third-party websites.[39] Further, the CJEU rejected the so-called 'knowledge' (i.e. knowledge that processed data is personal) and 'intention' (i.e. intention to process data as personal) components as elements of the definition of controllership.[40] This development ensured that the interpretation of controllership under the EU data protection law is free from subjective elements, which could serve as an excuse from accepting responsibility for processing personal data.

As recently stated by Advocate General Medina in *Belgian State*, every time personal data is processed, a controller must be identified at every stage of processing.[41] This interpretation precludes a situation where personal data is being processed in a vacuum, with no person or entity being accountable as a controller. The question of potential gaps in controllership attribution has been also raised in the context of COVID-19 contact tracing apps.[42] While the Lithuanian public health authority influenced some aspects of the design of the COVID-19 contact tracing app (e.g. the wording of the questions asked by the app to the users), it did not have access to personal data, was not operating the app, did not acquire the app, and did not disseminate it. This did not preclude the CJEU from considering that it could have been qualified as a controller.[43]

Rooted in the definition of controllership is the definition of 'joint controllership'.[44] It refers to the joint determination of means and purposes

---

[37] Case C-131/12 *Google Spain SL* EU:C:2014:317, para 34; Case C-40/17 *Fashion ID* (n 32) para 66; C-210/16 *Wirtschaftsakademie* (n 33) para 28; Case C-25/17 *Jehovan todistajat* EU:C:2018:551, para 66; Case C-683/21 *Nacionalinis visuomenės sveikatos centras* (n 30) para 29; Case C-807/21 *Deutsche Wohnen* EU:C:2023:950, para 40.

[38] Ibid.; see Regina Becker and others (n 9) 211ff.

[39] Case C-131/12 *Google Spain SL* (n 37) para 34.

[40] Orla Lynskey, 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78 The Modern Law Review 522, 524.

[41] Opinion of AG Medina (n 21) para 38.

[42] Case C-683/21 *Nacionalinis visuomenės sveikatos centras* (n 30).

[43] Case C-683/21 *Nacionalinis visuomenės sveikatos centras* (n 30), para 35.

[44] Art. 4(7) GDPR: '"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the

of processing between (at least) two actors.[45] The CJEU ruled that for an entity to qualify as a joint controller, it first needs to meet the requirements of becoming a controller.[46] Faced with questions concerning the attribution of controllership in a multi-agent data sharing environment, the CJEU opted for a relatively low threshold of becoming a joint controller – in order to ensure effective and complete protection of the data subject.[47] Drawing from the phase-oriented approach, the CJEU ruled that a joint controllership may be established when different entities are engaged in different phases of processing personal data.[48] As ruled by the CJEU, the degree of involvement between the joint controllers may vary: joint responsibility does not imply equal involvement to the same degree across all stages of processing.[49]

Crucially, as stated by the CJEU, access to personal data is not a requirement for becoming a joint controller.[50] In scenarios where at least two actors are engaged in processing personal data, one of them can become a controller without actually having access to personal data, just by exerting influence over the means and purposes of processing.[51] The CJEU stated further that there is a link between enjoying commercial benefits from data sharing and qualifying as a (joint) controller.[52] The criterion applied was not the actual access to data, but the capability to determine the purposes of processing.[53]

2. Data Act

The following section considers the two roles that are relevant to the data sharing process as envisaged by the DA, i.e. 'user' and 'data holder'. Arguably, these two roles are likely to overlap in their material scope with the roles defined in the GDPR. Further, this section provides an overview of the data sharing mechanisms stipulated by the DA.

---

processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

[45] Ibid.

[46] Case C-40/17 *Fashion ID* (n 32) para 74; C-683/21 Nacionalinis visuomenės sveikatos centras (n 30) para 41.

[47] Case C-40/17 *Fashion ID* (n 32) paras 70ff; Alexandra Giannopoulou (n 9) 82.

[48] Case C-40/17 *Fashion ID* (n 32) para 70.

[49] Case C-683/21 *Nacionalinis visuomenės sveikatos centras* (n 30) para 42.

[50] Case C-210/16 *Wirtschaftsakademie* (n 33) para 38; Case C-25/17 *Jehovan todistajat* (n 37) para 69.

[51] Case C-25/17 *Jehovan todistajat* (n 37) para 68.

[52] Case C-40/17 *Fashion ID* (n 32) para 80; Yordanka Ivanova (n 20) 5.

[53] Case C-40/17 *Fashion ID* (n 32) para 80.

The data sharing model introduced by the DA acknowledges the actual control over data exercised by the manufacturers of Internet of Things (IoT) devices.[54] In order to accommodate their role in data sharing scenarios, the notion of a 'data holder' is introduced.[55] A data holder is a natural or legal person with the ability to make available data generated by the use of an IoT device. This ability is derived either from a set of pre-existing rights and obligations attributed to the data holder[56], or from control over the technical design of the product[57].

The data sharing obligations under the DA foresee two avenues of data sharing. First, Article 4 DA stipulates a right of the user to directly access their co-generated data stored by the data holder.[58] A data holder is obliged to make the requested data available to the user 'without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time'.[59] This obligation includes in its scope readily available data[60], and the relevant metadata necessary to interpret the readily available data.

Article 5 DA introduces an alternative avenue of accessing data from the data holder.[61] A user has the right to (directly or through an intermediary) request the transmission of their co-generated data from the data holder to a third party. Similarly to the direct access right under Article 4 DA, the

---

[54] Rupprecht Podszun and Philipp Offergeld, 'The EU Data Act and the Access to Secondary Markets' (24 October 2022) 24 <https://papers.ssrn.com/abstract=4256882> accessed 7 August 2023.

[55] Art. 2(13) DA: '"data holder" means 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'.

[56] Art. 2(13) DA.

[57] Recital 20 DA.

[58] Art. 4 DA.

[59] Art. 4(1) DA.

[60] Art. 2(17) DA: '"readily available data" means product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation'.

[61] Art. 5(1) DA: 'Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9'.

requested data must meet specified quality standards[62], and include both readily available data as well as corresponding metadata.[63]

The 'user' is a central figure of the data sharing model envisaged by the DA. User's rights enshrined in Articles 4-5 DA are a necessary element of the data sharing mechanisms under the DA. Only exercising these rights enables data sharing, requesting the data holder to make data available either to the user or to a third party. The DA defines a user by reference to a commercial relationship (ownership or lease).[64] Owning, renting or leasing a product within the scope of the DA[65] automatically grants the status of a user. There is a direct link between becoming party to a contractual relationship and becoming a user within the meaning of the DA. The rights conferred upon the user can be equally enjoyed by a natural or a legal person. The DA foresees two types of users: those who are simultaneously users and data subjects, and other non-data-subject users.

With regard to the scope of the term user, the DA confirms the possibility of the existence of multiple simultaneous users of one product. This possibility is addressed in Recital 21 DA.[66] The suggested solution is a "one-user/one-account" rule, which is supposed to be implemented by the "manufacturer

---

[62] Art. 5(1) DA: 'without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time'.

[63] Art. 5(1) DA: 'available readily available data, as well as the relevant metadata necessary to interpret and use those data'.

[64] Art. 2(12) DA: '"user" means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services'.

[65] Art. 2(5) DA: '"connected product" means an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user'; art. 2(6) DA: '"related service" means a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product'.

[66] Recital 21 DA: 'Where several persons or entities are considered to be users, for example in the case of co-ownership or where an owner, renter or lessee shares rights of data access or use, the design of the connected product or related service, or the relevant interface, should enable each user to have access to the data they generate. Use of connected products that generate data typically requires a user account to be set up. Such an account allows the user to be identified by the data holder, which may be the manufacturer (...)'.

or designer".[67] However, the relationship between a user (having a legal title to the product) and a natural person (actually using the product) is unclear. This set up is likely to occur in a household, or within a group of people bound by informal ties. Under the DA, a person using an IoT device, with the permission of the owner but without a legal title, would be denied the access rights enshrined in Articles 4-5DA, despite their direct involvement in the co-generation of data. This deficiency of the user definition contained in the DA has been recognised by the scholarship.[68] Drexl et al. argue that a person involved in the process of co-generating data, by using the device, should be granted access rights.[69]

The distinction between users who are also data subjects and other non-data-subject users has significant consequences for establishing the lawfulness of data sharing under the GDPR. The DA foresees that the lawfulness (within the meaning of the GDPR) of DA-induced processing of personal data may be a potential field of conflict between the DA and the GDPR. This is addressed in Recital 7 DA, which stipulates that any processing of personal data resulting from the application of the DA requires a legal basis within the meaning of the GDPR.[70] Further, Recital 7 clarifies that the DA is not a legal basis within the meaning of the GDPR for the "collection or generation" of personal data by data holders.[71]

For users requesting access to personal data under the DA, the DA differentiates between two scenarios: (i) where the user submitting an access request is simultaneously a data subject (i.e. is requesting access to their own personal data), and (ii) where the user is not a data subject (i.e. is requesting access to someone else's personal data). In the first scenario, when a user is

[67] Recital 21 DA: '(…) Manufacturers or designers of a connected product that is typically used by several persons should put in place the necessary mechanisms to allow separate user accounts for individual persons, where relevant, or for the possibility of several persons using the same user account. (…)'.

[68] Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (25 May 2022) 25 <https://papers.ssrn.com/abstract=4136484> accessed 19 July 2023.

[69] Ibid.

[70] Recital 7 DA: 'Any processing of personal data pursuant to this Regulation should comply with Union data protection law, including the requirement of a valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC'.

[71] Recital 7 DA: 'This Regulation does not constitute a legal basis for the collection or generation of personal data by the data holder'.

simultaneously a data subject, it is convincing to argue that an access request within the meaning of the DA qualifies as 'consent' under the GDPR.[72]

The second scenario would be exemplified by a car rental company renting cars to individuals[73], or a healthcare provider making medical IoT devices available to the patients. Their ownership qualifies the car rental and the healthcare provider as a user under the DA. At the same time, the drivers of the rented cars and the patients of the healthcare provider would qualify as data subjects.[74] The second scenario is therefore characterised by a distinction between the legal title to an IoT device and the actual use of it.

In the second scenario, it is unclear whether the DA creates a legal basis within the meaning of the GDPR. In light of Recital 7 DA, this scenario can be further divided into situations when the accessed data will be shared with the user or with third parties.[75] Recital 7 DA explicitly excludes applying the DA as a GDPR legal basis when data is shared with third parties. However, it has been argued that when data is only accessed by the user, the data holder's duty to accommodate an access request constitutes a legal obligation within the meaning of Article 6(1)(c) GDPR.[76] An opposite view is based on a presumption of the rationality of the legislator: since the DA explicitly requires identifying a stand-alone GDPR legal basis for accommodating a user's access right, the DA cannot serve the same purpose.[77]

The latter view should be supported. Taking into account Articles 4(12) and 5(7) DA, considered in light of Recital 34 DA[78], it is justified to argue that the legislator does not consider the DA to be a legal basis within the meaning of Article 6(1) of the GDPR. Even the wording of Recital 34, which refers

---

[72] Steinrötter (n 6) 223; Louisa Specht-Riemenschneider, 'Der Entwurf des Data Act. Eine Analyse der vorgesehenen Datenzugangs- ansprüche im Verhältnis B2B, B2C und B2G' (2022) Beilage zu MMR 9/2022 809, 810.

[73] See Axel Metzger and Heike Schweitzer, 'Shaping Markets: A Critical Evaluation of the Draft Data Act' (18 September 2022) 28 <https://papers.ssrn.com/abstract=4222376> accessed 7 August 2023.

[74] However, it should be noted that a different interpretation is also possible. Namely, that the clients of the car rental, or the patients of the healthcare provider, qualify as users as well. In this set up, there would be two separate users of one product (e.g. car rental company that owns the car, and the client that rents the car).

[75] Specht-Riemenschneider (n 72) 810.

[76] Ibid. 811.

[77] Steinrötter (n 6) 223.

[78] Recital 34 DA: 'Accordingly, such a user who as controller intends to request personal data generated by the use of a connected product or related service is required to have a legal basis for processing the data as required by Article 6(1) of Regulation (EU) 2016/679, such as the consent of the data subject or the performance of a contract to which the data subject is a party'.

to potential examples of legal bases applicable in this case, does not refer to Article 6(1)(c) GDPR.

Essentially, the debate about the possibility of identifying a GDPR legal basis within the DA is a debate about the possibility of using the GDPR as a defence against DA access requests.[79] From the perspective of a data holder (controller), complying with requests to access datasets containing personal data will lead to considerable legal uncertainty. As rightly pointed out by Steinrötter, if a data holder misidentifies data as personal, and is unable to produce a GDPR legal basis, denying access would constitute an infringement of the DA.[80] At the same time, if a dataset containing personal data is treated as if it was non-personal, and thus shared without a GDPR legal basis, a GDPR infringement is unavoidable.[81]

It is likely that this uncertainty will incentivise data holders to apply an overly broad interpretation of personal data to their datasets, especially in light of the Recital 34 DA, which specifies that the GDPR shall apply to mixed datasets where personal and non-personal data are "inextricably linked".[82] However, it is unclear how far the fiction of data being personal should go: whether it covers all GDPR requirements, or just some of them (e.g. identifying a legal basis).

III. Applying the GDPR roles to Article 5 DA

The following section analyses the application of roles defined in the GDPR (i.e. data subject, controller, joint controller) to the roles defined in the DA (i.e. user, data holder, third party). The analysis refers to the exercise of the access right enshrined in Article 5 DA as it leads to the most complex scenario of responsibility attribution. Reconciling the notion of controllership under the GDPR with the data sharing mechanism in the DA creates a complex landscape of responsibility attribution. In some cases, the DA addresses this issue in its non-operative provisions.[83] The operative provisions of the DA refer to controllership attribution only implicitly, by reference to the obligation of identifying a legal basis under the GDPR before engaging in data sharing.[84]

---

[79] Steinrötter (n 6) 223.

[80] Steinrötter (n 6) 223.

[81] Ibid.

[82] Steinrötter (n 6) 219; see also Peter Georg Picht and Heiko Richter, 'EU Digital Regulation 2022: Data Desiderata' (2022) 71 GRUR International 395, 401.

[83] Recital 34 DA, Recital 35e DA.

[84] Art. 4(12), art. 5(7) DA.

Pursuant to Article 5 DA, data sharing includes at least three parties (user, data holder, third party receiving data). However, in an extreme scenario it may include up to five parties (data subject, non-data-subject user, intermediary requesting access on behalf of a user, data holder, third party receiving data).[85]

As outlined in the previous sections, the roles defined in the GDPR and in the DA are based on different principles. The roles in the GDPR are based on facts and are non-negotiable. The relationship between a person (or an entity) and personal data defines one's role. For a data subject, it is their link with a given piece of data – if it meets the threshold of identifiability. For the controller it is the power exercised over data and its processing modalities. In the latter case, what is being done to data, conditions one's legal status as a controller.

The roles defined in the DA are based on pre-existing legal and technical infrastructures, which determine one's status as a user or a data holder.[86] What is understood under legal infrastructures is a set of pre-existing rights and obligations, as referred to in the definitions of the user and data holder. Rights and obligations that exist beyond the scope of the DA, determine whether a person or an entity would become a user or data holder. In case of the latter, a technical infrastructure, understood as power over the technical design of the relevant product or related services, can also determine one's status as a data holder.

In line with the CJEU case law analysed in the previous sections, the following factors need to be taken into account when attributing controllership. Due to the phase-oriented character of controllership, its attribution requires separate consideration for each phase of the processing of personal data. Further, it is necessary to ensure that a controller is identified for each phase of data processing. The lack of access to processed data does not automatically preclude an entity from becoming a joint controller.

Going back to the example of a car rental company, the challenges associated with attributing responsibility for data sharing under Article 5 DA can be illustrated as follows. A user who is not a data subject (a car rental company), submits a request to share data of the driver (data subject's) with a third party (an after-market service provider). As this paper argues, in this scenario the user and the third party receiving the requested data become joint controllers. This is justified by the following arguments.

Drawing from Recital 34 DA, access to personal data may only be requested by a data subject or a controller. The DA foresees that a user, who is not a data subject, will become a controller (and possibly a new data holder) of the

[85] See also Axel Metzger and Heike Schweitzer (n 73).

[86] See Specht-Riemenschneider (n 72) 813.

data they will have requested from the data holder.[87] Similarly, once a third party within the meaning of Article 5 DA will receive the data requested by the user, they will also become controllers.

Since the DA does not determine the purpose of processing, in the course of data sharing under Articles 4-5 DA, such purpose remains to be decided by the involved actors. This means specifically, the user (as the party making the request, with an intention as to how the requested data will be used and for what purposes) and the receiving third party (as the party processing the data in agreement and coordination with the user). Especially under data sharing resulting from exercising the right enshrined in Article 5 DA, the lack of access by a user to the requested data, does not preclude a joint controllership from being formed.[88] The case law of the CJEU outlined above, further clarifies that a commercial benefit resulting from processing personal data is an argument in favour of establishing the existence of joint controllership.[89] This argument applies to the third party receiving requested data.

The following table illustrates the attribution of responsibility in the discussed scenario.

Figure 3. Attribution of responsibility – data sharing pursuant to Article 5 DA

	Data subject	**Joint controllers**		**Controller**
	User	User	Third party receiving the requested data	Data holder
Driver renting a car	x			
Car rental company		x		
After-market service provider			x	
Car manufacturer				x

At the same time, it is unlikely that, as a result of DA-induced data sharing, a joint controllership formed between the user and a third party, will include the original data holder. While it is clear that in principle data holders process personal data as controllers, the specific act of making data available to users and third parties is not an expression of their intention. To the contrary, drawing from its implicit objectives, the DA is supposed to overcome the reluctance

[87] Recital 34 DA.

[88] See Case C-210/16 *Wirtschaftsakademie* (n 33) para 38; Case C-25/17 *Jehovan todistajat* (n 37) paras. 68–69.

[89] See Case C-40/17 *Fashion ID* (n 32) para 80; Ivanova (n 20) 5.

of data holders to share their data.[90] Although the mere lack of intention to exercise influence over data processing does not automatically absolve data holders from being considered a controller[91], there are further arguments against considering original data holders to be joint controllers in DA-induced data sharing. The crucial element of determining controllership, which is missing, is the lack of influence over the purposes of data processing. The data holder, acting in response to an access request submitted by the user, does not exercise influence over the purposes of further processing the requested data.

IV. Conclusions

Due to the overlapping scope of the roles defined in the DA and the GDPR, processing personal data in the course of DA-induced data sharing creates a matrix of responsibilities dispersed between different entities. However, since the roles defined in the GDPR and in the DA are based on different underlying principles, the data sharing mechanisms under the DA lead to a conflation of roles across these two regulatory regimes.

The data sharing mechanisms stipulated in Articles 4–5 DA do not prescribe a purpose of processing within the meaning of the GDPR. Drawing from the definition of processing set out in the GDPR, data sharing is a processing activity (or phase) and, on its own, cannot serve as a purpose of data processing. As a result, it is unlikely that the provisions of the DA would qualify as a legal designation of GDPR's controllership.

Therefore, it is necessary to analyse possible controllership through the lenses of factual influence. This analysis, focusing on factual influence exercised by different actors over processing of personal data, leads to the following conclusions. First, it is justified to argue that data sharing under Article 5 DA will lead to the creation of joint controllership between the user requesting access and the third party receiving the requested data. Second, it is unlikely that the data holder making the requested data available to the third party will qualify as a joint controller as well. Due to the lack factual influence of the data holder on the determination of the purposes of processing, the attribution of joint controllership would have been unjustified. Being driven by the principle of complete and effective protection of the data subject, the CJEU's rulings create relatively low entry barriers to becoming a joint controller. As a result, the DA opens new possibilities for the formation of joint controllership.

[90] See Recital 4 DA.
[91] See Lynskey (n 40) 524.

Acknowledgments

I would like to thank the anonymous reviewers for valuable comments that improved the quality of this article.

Funding

This article received no funding

The cost of editing selected articles published in the Yearbook of Antitrust and Regulatory Studies in the 2022–2024 is covered by funding under the program "Development of scientific journals" of the Ministry of Education and Science under agreement No. RCN/SN/0324/2021/1. Task title: "Verification and correction of scientific articles and their abstracts". Funding value: 36 298,00 PLN; The task consists of professional editing of articles published in English.

Declaration of Conflict of interests

The author declared no potential conflicts of interest with respect to the research, authorship, and publication of this article. The author is also an employee of the Polish Office of Competition and Consumer Protection. Opinions expressed in this article are solely of the author and do not reflect the views of the Office of Competition and Consumer Protection.

Declaration about the scope of AI utilisation

The author did not use AI tools in the preparation of this article.

Literature

Becker, R., and others, 'Applying GDPR Roles and Responsibilities to Scientific Data Sharing' (2022) 12 International Data Privacy Law 207

Drexl, J., and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (25 May 2022) <https://papers.ssrn.com/abstract=4136484> accessed 19 July 2023

European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.1' (2021) <https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf> accessed 27 December 2023

Finck, M., 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11 International Data Privacy Law 333

Giannopoulou, A., 'Allocating Control in Decentralised Identity Management' (2022) European Review of Digital Administration & Law 75

Ivanova, Y., 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' (1 March 2020) <https://papers.ssrn.com/abstract=3584207> accessed 29 July 2023

Lynskey, O., 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78 The Modern Law Review 522

Mahieu, R., and van Hoboken, J, 'Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?' (European Law Blog, 30 September 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed 29 July 2023

Metzger A., and Schweitzer, H., 'Shaping Markets: A Critical Evaluation of the Draft Data Act' (18 September 2022) <https://papers.ssrn.com/abstract=4222376> accessed 7 August 2023

Picht P.G., and Richter, H., 'EU Digital Regulation 2022: Data Desiderata' (2022) 71 GRUR International 395

Pohle, J., 'Die immer noch aktuellen Grundfragen des Datenschutzes' in Hansjürgen Garstka and W Coy (eds), *Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis* (Berlin: Helmholtz-Zentrum für Kulturtechnik, Humboldt-Universität zu Berlin 2014)

Podszun, R., and Offergeld, P, 'The EU Data Act and the Access to Secondary Markets' (24 October 2022) <https://papers.ssrn.com/abstract=4256882> accessed 7 August 2023

Specht-Riemenschneider, L., 'Der Entwurf des Data Act. Eine Analyse der vorgesehenen Datenzugangs- ansprüche im Verhältnis B2B, B2C und B2G' (2022) Beilage zu MMR 9/2022 809

Steinmüller, W, and Lutterbeck, B., 'Grundfragen Des Datenschutzes' (1971) Gutachten im Auftrag des Bundesministeriums des Innern <https://dserver.bundestag.de/btd/06/038/0603826.pdf> accessed 16 August 2023

Steinrötter, B., 'Verhältnis von Data Act und DS-GVO. Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung' (2023) 4 Gewerblicher Rechtsschutz und Urheberrecht 216