Intermediating data rights exercises: the role of legal mandates

Giannopoulou, A.; Ausloos, J.; Delacroix, S.; Janssen, H.

DOI
10.1093/idpl/ipac017

Publication date
2022

Document Version
Final published version

Published in
International Data Privacy Law

Intermediating data rights exercises: the role of legal mandates

Alexandra Giannopoulou ,* Jef Ausloos ,**
Sylvie Delacroix ,*** and Heleen Janssen ****

Key Points

- Data subject rights constitute critical tools for empowerment in the digitized society. There is a growing trend of relying on third parties to facilitate or coordinate the collective exercises of data rights, on behalf of one or more data subjects.
- This contribution refers to these parties as 'Data Rights Intermediaries' (DRIs), ie where an 'intermediating' party facilitates or enables the collective exercise of data rights. The exercise of data rights by these DRIs on behalf of the data subjects can only be effectuated with the help of mandates.
- Data rights mandates are not expressly framed in the GDPR their delineation can be ambiguous. It is important to highlight that data rights are mandatable and this without affecting their inalienability in light of their fundamental rights' nature.
- This article argues that contract law and fiduciary duties both have longstanding traditions and robust norms in many jurisdictions, all of which can be explored towards shaping the appropriate environment to regulate data rights mandates in particular.
- The article concludes that the key in unlocking the full potential of data rights mandates can already be found in existing civil law constructs, whose diversity reveals the need for solidifying the responsibility and accountability of mandated DRIs. The continued adherence to fundamental contract law principles will have to be complemented by a robust framework of institutional safeguards. The need for such safeguards stems from the vulnerable position of data subjects, both vis-à-vis DRIs as well as data controllers.

Introduction

The vicious circle of rapid technological and economic developments, and exponential data production, brings about countless social, legal, and ethical concerns. Many of these concerns can be traced back to the significant information and power asymmetries that characterize today's political economy of data.[1] Transparency asymmetries result from the size and complexity of data infrastructures as well as engineered opaqueness by those who control the infrastructures.[2] Power asymmetries result from the ability to exploit these data infrastructures in light of strong (commercial/political) imperatives at the expense of individuals, communities, and/or society at large.

Data rights are emerging as an emancipatory legal tool to challenge these asymmetries, empowering people

* Alexandra Giannopoulou, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, The Netherlands. Email: a.giannopoulou@uva.nl
** Jef Ausloos, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, The Netherlands
*** Sylvie Delacroix, Birmingham Law School, University of Birmingham, Birmingham, United Kingdom
**** Heleen Janssen, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, The Netherlands
J.A., S.D., and H.J. contributed equally to the development of ideas, and to the writing of the article.
The work leading to this article was supported by a research grant from the Data Trusts Initiative, which is funded by the McGovern foundation. A.G. and H.J. have received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681. J.A. received funding from the Dutch Research Council (NWO), under grant agreement No VI.Veni.201R.096.

1 D Beer, 'The Social Power of Algorithms' (2017) 20 Information, Communication & Society 1; R Kitchin, 'Thinking Critically about and Researching Algorithms' (2017) 20 Information, Communication & Society 14.

2 P Tolmie and others, 'This Has to Be the Cats - Personal Data Legibility in Networked Sensing Systems' (Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work and Social Computing, San Francisco, 27 February 2016), 491; Beer (n 1) 1; Kitchin (n 1) 14; M Veale, R Binns and J Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) International Data Privacy Law 4.

to render visible data infrastructures and govern the use of their data. They feature in a growing number of legal frameworks, in Europe[3] and elsewhere.[4] Indeed, we can observe a proliferation of data rights in recent EU policymaking, either reinforcing or introducing new legal mechanisms to mitigate information/power asymmetries in the data economy. As (EU) policymakers are gradually catching up with the digital transformation of society, we also anticipate future legal frameworks will increasingly include data rights in specific contexts. For the time being, the most important legal source for data rights is chapter III of the General Data Protection Regulation (GDPR).[5] The 'rights of the data subject' in this Chapter are intent-agnostic and can be deployed in many different ways in order to safeguard countless interests, rights, or freedoms.[6]

While underused for many years, recent initiatives have demonstrated the value of data rights in a variety of contexts; from invoking the rights of access, portability and not to be subject to automated decision-making to obtain better working conditions,[7] to reverse engineering discriminatory credit scoring algorithms,[8] or enabling academic research using digital trace data.[9] As these examples illustrate, data rights should not be seen as (just) individualistic legal tools; they hold significant potential for tackling systemic data-driven injustices at a collective level.[10]

Despite the growing availability and awareness of data rights, important questions remain as to their functionality and effectiveness. Systemic transparency problems—resulting from the size and complexity of data infrastructures as well as engineered opaqueness by those who control those infrastructures[11]—thwart fair and lawful data processing, proper enforcement, and effective exercises of data rights. Additionally, rights holders often lack the (technical, legal, financial)capacity, time, or knowledge to effectively deploy their rights.

In light of the above, there is a growing trend of relying on a third party to facilitate or coordinate the (collective) exercises of data rights, on behalf of one or more data subjects. Within the context of this article, we term these intermediating parties 'data rights intermediaries' (DRI). We define data rights intermediation broadly, as situations where an 'intermediating' party facilitates or enables the (collective) exercise of data rights. Importantly, for our purposes here, DRIs should be clearly distinguished from data intermediaries. The concept of the data intermediary is used in a wide variety of contexts, generally to refer to organizations that capitalize on pooling data in one way or another.[12] DRIs do not

3 EU Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC 2008, OJ 2008 L 133/66, art 10; EU Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA, and 2009/968/JHA, OJ 2016 L133/53, arts 36–37; EU Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services' OJ 2019 L 186/57, arts 47–48.

4 See, notably, the California Consumer Privacy Act of 2018 [1798.100 – 1798.199.100] (Title 1.81.5 added by Stats 2018, ch 55, s 3) and numerous other frameworks across the globe. For an overview, see G Greenleaf, 'Global Tables of Data Privacy Laws and Bills' (7th Ed, January 2021)' (2021) 169 Privacy Laws & Business International Report 6 <https://papers.ssrn.com/abstract=3836261> accessed 18 March 2022.

5 EU 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) OJ 2016 L 119/1; for this article, we focus on the GDPR's data rights; that said, we see no a priori reasons why our analysis might not also apply to other data rights scattered across other frameworks.

6 J Ausloos, R Mahieu and M Veale, 'Getting Data Subject Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance (2020) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law; R Mahieu and J Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access' ArXiv, 2 July 2020 <https://osf.io/preprints/lawarxiv/b5dwm/> accessed 18 March 2022.

7 District Court of Amsterdam, Netherlands (11 March 2021) *Uber drivers v Uber*, ECLI:NL:RBAMS:2021:1020, paras 4.24–4.25; District Court of Amsterdam, Netherlands *Ola drivers v Ola Cabs* (11 March 2021) ECLI:NL:RBAMS:2021:1019, paras 4.4ff; Open Society Foundations, 'Q and A: Fighting for Worker's Right to Data' (23 May 2019) <https://www.opensocietyfoundations.org/voices/q-and-a-fighting-for-workers-right-to-data>; 'Uber Drivers Demand Their Data. The Ride Hailing Company Declined to Share Comprehensive Information. Now Drivers Are Taking Legal Action' (20 March 2019) <www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data>; J Toh, 'Empowering Workers Through Digital Rights' (Activist blog, *Digital Freedom Fund*, 30 April 2021) <https://digitalfreedomfund.org/empowering-workers-through-digital-rights/>; 'Shopper Transparency Calculator 2.0' (*Coworker*) <https://home.coworker.org/shiptcalc/> accessed 18 March 2022.

8 See notably OpenSCHUFA, 'The Campaign Is Over, the Problems Remain' (May 2019) <https://openschufa.de/>; J Angwin, S Mattu and J Larson, 'The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review' (*ProPublica*, 1 September 2015) <https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review> accessed 18 March 2022.

9 T Araujo and others, 'OSD2F: An Open-Source Data Donation Framework' (*SocArXiv*, 16 September 2021) <https://osf.io/preprints/socarxiv/xjk6t/> accessed 18 March 2022; J Ausloos, T Araujo and D Oberski, 'A Blueprint for Digital Trace Data Collection Through Data Donation' ICA May 2020. doi:10.48550/arXiv.2011.09851; J Ausloos and M Veale, 'Researching with Data Rights' (2020) Technology and Regulation 136.

10 R Mahieu and J Ausloos, 'Harnessing the Collective Potential of GDPR Access Rights: Towards an Ecology of Transparency' (2020) Internet Policy Review <https://policyreview.info/articles/news/harnessing-collective-potential-gdpr-access-rights-towards-ecology-transparency/1487> accessed 18 March 2022.

11 Tolmie and others (n 2) 491; Beer (n 2) 1; Kitchin (n 2) 14; Veale, Binns and Ausloos (n 2).

12 Note that the terminology is still *in flux*. The UK-based Open Data Institute (ODI) defined these organizations as 'data institutions', explaining them as 'organisations that steward data on behalf of others, often towards public, educational or charitable aims', see J Hardinges and J Tennison, *Data Institutions* (London Open Data Institute 2020) <https://

necessarily valorize any (personal) data, but simply assist in the (collective) exercise of data rights, whether it be the right to object, erasure, portability, or indeed access personal data.

Data rights intermediation in general can range from simply making templates available to the public for anyone to use,[13] to more organized initiatives like data trusts, which involve an active role of the intermediating parties in data governance. A central question in many of these initiatives is whether data subjects can effectively mandate the respective data rights to a third party. For the purposes of this article, we use the term 'mandate' to refer to situations where a data subject assigns to another party, the power to bring a legal action or exercise a right on the subject's behalf.

Under what conditions can data rights be lawfully exercised by someone other than the data subject, on behalf of one or more data subjects? As a key source of data rights, the GDPR, is essentially silent about whether intermediating parties can exercise data rights on behalf of the data subject. That is to say, the GDPR neither rejects nor explicitly condones data rights to be exercised by an intermediating party. Having said that, the GDPR does recognize the ability of data subjects to have specific types of organizations represent them, to obtain remedies for GDPR violations if such representation is recognized in Member State law.[14] The role of such representatives is also acknowledged in relation to data protection impact assessments, where controllers are encouraged to 'seek the views of data subjects *or their representatives [emphasis added]* on the intended processing.'[15] In this context, it is also worth mentioning that the Court of Justice of the European Union (CJEU) recently clarified that Article 80(2) of the GDPR does not preclude national legislation that allows a consumer protection association to bring legal proceedings in the absence of a mandate conferred on it for that purpose (and independently of the infringement of specific rights of a data subject), by alleging infringement of the prohibition of unfair commercial practices, consumer protection legislation or the prohibition of the use of invalid general terms and conditions.[16] Important as it is, the latter ruling still leaves open the question of whether—and under what conditions—the data subject rights granted by chapter III GDPR can be mandated to a DRI.

As will become more apparent throughout this article, there are many different understandings of the term 'mandate' both in normative descriptions and in case law. Because of the contrasted legal histories behind its uses in different jurisdictions, the concept of 'mandate' suffers from a significant degree of ambiguity. Yet its use in the GDPR, recent case law, and EU policy initiatives have made it a salient and increasingly important concept in a data protection context.[17] This article addresses the sources of this conceptual confusion to highlight the practical significance of mandates if data protection regimes are to take on board both the relational (hence collective) dimension of personal data *and* the fundamental (hence inalienable[18]) underpinnings of data rights.

Intermediating data rights under data protection law

Data rights

Data rights are legal instruments meant to empower (groups of) individuals to understand and control data processing operations. Currently, the clearest—and arguably most powerful—data rights can be found in the GDPR. More specifically, chapter III in the GDPR lists several data subject rights that can be used in a wide variety of situations: notably the rights of access (Article 15), to rectification (Article 16), to erasure (Article 17), to portability (Article 20), to object (Article 21), and not to be subject to automated decision-making (Article 22).[19]

While data rights have been integral to data protection laws since at least the 1970s, it is only in the last decade that they have gained more attention. Recent research has demonstrated the significant compliance and enforcement issues of data protection

theodi.org/article/what-do-we-mean-by-data-institutions/> accessed 18 March 2022. More recently, the EU's Data Governance Act (Regulation 2022/868 of 30 May 2022 on European data governance and amending Regulation 2018/1724 (Data Governance Act) OJ L152/1 of 3 June 2022 uses the term 'data intermediation'. See for an overview of term uses H Janssen and J Singh, 'Data Intermediary' (2020) 11(1) Internet Policy Review.

13 Eg Bits of Freedom, 'My Data Done Right' <https://www.mydatadoneright.eu/> accessed 18 March 2022.

14 Arts 80 in conjunction with77–79 GDPR.

15 Art 35(9) GDPR.

16 CJEU Case C-319/20, *Meta Platforms Ireland Limited, formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V* (2020) ECLI:EU:C:2022:322.

17 Arts 80 in conjunction with 77–79 and Recital 142 GDPR, and recently CJEU Case C-319/20, *Meta Platforms Ireland Limited, formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V* (28 April 2022) ECLI:EU:C:2022:322, paras 55, 56, and 84.

18 See subsubsections Data rights' rationale and Rights' alienation: abandonment and transfer.

19 See also art 9 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108 in conjunction with Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 2018, ETS 223.

rights,[20] but also highlighted their polyvalent potential.[21] In light of the ubiquity of digital technology in modern society, these rights will only become more important, not just on an individual, but even more so at a collective level.

Under the GDPR, the primary actor responsible for accommodating data rights is the data controller,[22] ie the actor determining the purpose and means of the respective data processing operations. Controllers must more generally comply with the data protection principles[23] and with a range of other obligations,[24] including the obligation to implement appropriate technical and organizational measures to ensure that their data processing complies with the GDPR.[25] Controllers are also required to consider data protection by design and by default principles, throughout the development and lifetime of their data processing obligations.[26]

Rationale of data rights

Natural persons should have control of their own personal data. One of the key motivations behind the GDPR is to (re-)empower data subjects.[27] The very first and main objective in the European Commission's official announcement for a data protection reform back in 2010, was to strengthen individuals' rights through 'enhancing control over one's data' and by 'improving the modalities for the actual exercise of the right.'[28] A year before, a public consultation had already highlighted that Europeans were demanding more control over their personal data,[29] with businesses raising concerns over potentially unreasonable and disproportionate exercises of data subject rights.[30] Eventually, the GDPR did expand the number and scope of available data rights significantly in its chapter III, also specifying a number of modalities aimed at facilitating their exercise.[31]

The GDPR's strong (though certainly not exclusive) emphasis on data subject *empowerment* does not come out of nowhere. Indeed, since its predecessor—the Data Protection Directive 95/46—the Charter of Fundamental Rights of the European Union ('Charter') was called into life. Notably, the Charter established the 'protection of personal data' as a stand-alone right in Article 8, next to the right to 'respect for private and family life' (Article 7).[32] No clear consensus exists on the exact rationale of this relatively new fundamental right, though it is generally associated with normative values such as autonomy, informational self-determination, integrity, and dignity.[33] Most commentators agree that the right to data protection does not (merely) have a passive 'protective' role, and incorporates a strong call for active control over one's personal data as well.[34]

Put briefly, for our purposes, a data subject's *control* over personal data can be considered at the core of the right to data protection in the Charter.[35] Importantly,

20 X Duncan L'Hoiry and C Norris, 'The Honest Data Protection Officer's Guide to Enable Citizens to Exercise Their Subject Access Rights: Lessons from a Ten-Country European Study' (2015) 5 International Data Privacy Law 190; C Norris and others, *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Sprinter International Publishing 2017); J Ausloos and P Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4; Veale, Binns and Ausloos (n 2); R Mahieu, H Asghari and M van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review 1.

21 S Delacroix and N Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance' (2019) 9 International Data Privacy Law 236; J Ausloos, D Oberski and T Araujo, 'A Blueprint for Digital Trace Data Collection Through Data Donation' (no date) <https://www.youtube.com/watch?v=6FEZaYUfC9Q> accessed 18 March 2022; Ausloos and Veale (n 9); Mahieu and Ausloos (n 6); N Vincent and others, 'Data Leverage: A Framework for Empowering the Public in Its Relationship with Technology Companies' (2021) arXiv:201209995 [cs].

22 Art 4(7) GDPR.

23 Art 5(1)(a)–(f) GDPR.

24 Art 5(2) GDPR.

25 Art 24 GDPR.

26 Art 25 GDPR.

27 Recital 7, GDPR.

28 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Comprehensive Approach on Personal Data Protection in the European Union' (4 November 2010) 5. COM/2010/0906 final <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF> accessed 18 March 2022.

29 DG Justice, 'Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data.' (4 November 2010) 2. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF>; Later confirmed in European Commission, 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (June 2011).

30 Justice (n 29) 9.

31 Art 12 GDPR.

32 G González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Law, Governance and Technology Series, Springer 2014).

33 See: P De Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Science 2009) 5; González Fuster (n 32); O Lynskey, *The Foundations of EU Data Protection Law* (Oxford Studies in European Law, OUP 2016) 210ff; H Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Law, Governance and Technology Series 31, Springer 2016); J Ausloos, *The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection* (OUP 2020).

34 European Group on Ethics in Science and New Technologies, 'Citizens Rights and New Technologies: A European Challenge. Report on the Charter on Fundamental Rights Related to Technological Innovation as Requested by President Prodi (Reproduced in: Draft Charter of Fundamental Rights of the European Union, CHARTE 4370/00)' (23 May 2000) 26; González Fuster (n 32) 194ff.

35 See similarly: European Group on Ethics in Science and New Technologies, *Ethics of Security and Surveillance Technologies* (Opinion 20 May 2014) 45; Lynskey (n 33) 11; D Clifford and J Ausloos, 'Data

such 'control' should not be interpreted narrowly, but implies the need for an overall architecture of control in function of data subjects' rights, freedoms, and interests. This includes both a positive dimension—ie the ability for data subjects to actively manage their personal data—and a negative dimension—ie safeguarding an environment where control over one's personal data is not subsumed by power asymmetries. This is most clearly (though not exclusively) given shape through the GDPR, a robust legal framework that constrains the free processing of data by way of strict conditions and a range of specific 'micro-rights', which enable data subjects to take active steps themselves (chapter III of the GDPR). The value of these rights in particular stems from the fact that the ubiquity and growing complexity of data-processing eco-systems, has made it impossible for legislators to anticipate all potential externalities, and for national supervisory authorities to appropriately tackle non-compliance.[36]

Ever since its landmark *Google Spain* Ruling, the CJEU has repeatedly emphasized the need for interpreting data protection law to ensure 'effective and complete protection' of data subjects' rights and freedoms.[37] Similarly, the CJEU also stressed the importance of guaranteeing 'efficient and timely protection' of data subjects' rights.[38] With these decisions, the CJEU underpinned the need to support data subject rights as easy-to-exercise tools. This is increasingly important to defend a variety of individual and collective rights, freedoms, and interests in a digitally intermediated society, from opportunities to protest, demonstrate, and unionize, to combatting discrimination, ensuring equal access to education, and enabling research.

Bearing this in mind, while also considering the systemic compliance and enforcement failure of data protection rules, the ability to have expert, independent intermediating parties assisting in the exercise of data rights, is appealing. Yet outsourcing the exercise of data rights might entail significant risks, such as where DRIs do not take appropriate measures to prevent identity fraud, misuse or abuse the mandated rights, or any challenges raised by the addressee of the data rights.

What data rights?

Chapter III of the GDPR is entirely devoted to the rights of data subjects, specifying in detail their respective modalities, conditions, and exceptions. Among these provisions, a distinction can be made between (a) *passive* provisions, aimed at enabling, facilitating, or further stipulating the conditions for the exercise of rights (ie Articles 12–14, 19), and (b) *active* provisions, explicitly granting rights for data subjects to proactively invoke (see Table 1). For our purposes here, we will focus primarily on the latter category.

When talking about data rights intermediation, two data rights have particularly drawn the attention of scholars, regulators, civil society, and industry: the right of access[39] and the right to data portability.[40] These rights are more versatile as they readily enable the repurposing of data, pooled together with others' data or not, for many different purposes. This contrasts with other data rights, which are more constrained: they enable editing/removing of specific data points (rights to rectification[41] and erasure[42]) or halting very specific processing operations (rights to restriction,[43] object,[44] and not be subject to automated decision-making[45]). Indeed, distinguishing between these different types of data rights is important when determining the conditions under which they can be mandated: Data rights focused on *transparency* (Articles 15, 20); on *personal data* itself (Articles 16, 17); and on *specific processing operations* (Articles 18, 21, 22). As such, the latter two categories can be particularly valuable to the respective individuals invoking them, but there appears to be less potential for these rights to directly benefit/affect a 'collective' exercise. This may also explain why, so far, most DRIs tend to focus on collectively exercising rights of access/portability on behalf of data subjects.

Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130; Ausloos (n 33) ch 2; S Rodotà, 'Data Protection as a Fundamental Right' in S Gutwirth and others (eds), *Reinventing Data Protection?* (First, Springer Netherlands 2009).

36 See Brave, 'Europe's Governments Are Failing the GDPR: Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities' (April 2020) <https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf> accessed 17 March 2022; J Ryan, 'Internal Problems Exposed at Irish Data Protection Commission' (February 2021) <https://www.iccl.ie/news/internal-problems-exposed-at-irish-data-protection-commission/>.

37 C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:2014:31; Case C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* [2017] ECLI:EU:C:2017:725; G González Fuster, 'Beyond the GDPR, above the GDPR' (2015) Internet Policy Review <http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385> accessed 17 March 2022; Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650; C136/17 *GC and Others v CNIL* [2019] ECLI:EU:C:2019:773; *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629.

38 Ibid (n 34).

39 Art 15 GDPR.

40 Art 20 GDPR.

41 Art 16 GDPR.

42 Art 17 GDPR.

43 Art 18 GDPR.

44 Art 21 GDPR.

45 Art 22 GDPR.

Table 1. Overview of data subject rights

Article	Title	Focus of the right
15	Right of access by the data subject	Rights focused on **transparency**
20	Right to data portability	
16	Right to rectification	Rights focused on **personal data** itself
17	Right to erasure ('right to be forgotten')	
18	Right to restriction of processing	
21	Right to object	Rights focused on specific **processing operations**
22	Automated individual decision-making, including profiling	

Table 1 - Active rights in Chapter III GDPR.

As mentioned before, the GDPR's data subject rights are intent-agnostic. Their primary value in a digitally intermediated society is that they enable reconfiguring data-driven power asymmetries. This reconfiguration can be asserted both individually and collectively. For example, individuals often request search engines to remove certain inadequate, irrelevant, or excessive results that show up on the basis of their name search.[46] There is also a growing number of examples where data rights are used collectively, notably by gig drivers to obtain more insight and agency over their work.[47] Apart from these two examples where data rights are invoked by individuals/collectives for their own benefit, there are also situations where these rights can be exercised for other purposes. One could think of an investigative journalist who would use her right of access to surface data malpractices; or coordinated erasure requests by environmental interest groups against polluting data intensive companies.

Intermediating collective exercises of data rights

Exercising data protection rights is meant to be easy and accessible to data subjects (Article 12 GDPR). Yet responses to individuals' requests hardly ever allow data subjects to acquire meaningful (legal) agency over their data. This can be explained both by problematic compliance by data controllers[48] as well as data subjects' limited (technical, legal, financial) capacities. It can take months and involve many back-and-forths with data controllers to overcome (bureaucratic) obstacles, making a successful data right's request a challenging experience.[49]

As mentioned before, the value and effectiveness of data rights often only surfaces when exercised collectively.[50] When exercised at scale, data rights can contribute significantly to exposing and challenging data-driven social injustices.[51] Journalists[52] and activists[53] have exercised the right of access to their data to uncover problematic data practices. Platform workers are capitalizing on the rights of access (Article 15) and not be subject to automated decision-making (Article 22) in order to vindicate fairer working conditions.[54] Campaigners in Germany have strategically used access rights in order to reveal discriminatory credit scoring algorithms.[55] These examples demonstrate that much of data rights' potential can only

46 See for instance <https://transparencyreport.google.com/eu-privacy/overview> accessed 17 March 2022.

47 Toh (n 7).

48 Ausloos and Dewitte (n 20); Privacy International, 'Our Complaints against Axciom, Criteo, Equifax. Experian, Oracle, Quantcast, Tapad' (Report, 8 November 2018) <https://www.privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad> accessed 18 March 2022.

49 Mahieu, Asghari and van Eeten (n 20).

50 It is worth noting that a collective action as the one described in the CJEU C-319/20 judgment is only one subcategory of the numerous possibilities in collectively exercising a (data) right. While collective action through a third party is frequently deployed in consumer or environmental law, this is much less the norm in data protection litigation.

51 Mahieu and Ausloos (n 6).

52 L Kelion, 'Ring Logs Every Doorbell Press and App Action' *BBC News* (4 March 2020 <https://www.bbc.com/news/technology-51709247>; L. Kelion, 'amazon: Why Amazon Knows So Much About You' *BBC News* (2020) <https://bbc.co.uk/news/extra/CLQYZENMBI/amazon-data> accessed 17 March 2022; examples borrowed from Mahieu and Ausloos (n 6) 31.

53 *Schrems v Facebook* (2014), see 'Europe-v-Facebook Complaints' (Europe-v-facebook.org) <http://europe-v-facebook.org/EN/Complaints/complaints.html> accessed 18 March 2022.

54 Privacy International, 'Case Study: The Gig Economy and Exploitation' (30 August 2017) <https://privacyinternational.org/case-study/751/case-study-gig-economy-and-exploitation>; District Court of Amsterdam (11 March 2021) *Uber drivers v Uber*, ECLI:NL:RBAMS:2021:1020, paras 4.24–4.25; District Court of Amsterdam, *Ola drivers v Ola Cabs* (11 March 2021) ECLI:NL:RBAMS:2021:1019, paras 4.4 ff <https://www.opensocietyfoundations.org/voices/q-and-a-fighting-for-workers-right-to-data>; <https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data> (accessed 21 April 2021); Toh (n 7).

55 'OpenSCHUFA – Shedding Light on Germany's Opaque Credit Scoring' (*AlgorithmWatch*, 22 May 2017) <https://algorithmwatch.org/en/open schufa-shedding-light-on-germanys-opaque-credit-scoring-2> accessed 17 March 2022.

materialize when transcending the mere focus on *individual/isolated* exercises. Yet organizing and valorizing data rights at scale can be complex.

In light of the above, DRIs are increasingly considered as a vehicle to support and strengthen individual and collective exercises of data rights. The latter need not be confined to transparency rights (Articles 15 and 20). DRIs can also assist in exercising rights focused on altering personal data (Articles 17–18), or challenging particular processing operations (Articles 18, 21–22).[56] While some DRIs can achieve their aims by coordinating the individual exercise of data rights in a way that does not rely on any formal rights mandate,[57] others strongly depend on—or at least presuppose the possibility of—data rights mandates. This reliance will depend, among other things, on the category of data rights involved, as well as the DRI's and data subject's specific goals.

Among those DRIs that do presuppose the possibility of data rights mandates, only some will aim to 'pull' and centrally store as much data as possible (thereby also becoming 'data intermediaries', on top of their DRI status). Other DRIs may be able to achieve their aims by leaving the data that is the object of data rights wherever it is (typically on the servers of various data controllers).[58] In some instances, the collective exercise of data rights may aim to 'port *en masse*' some data from one data controller to another, or merely provide access to facilitate research, In other instances, a DRI may leverage data rights to obtain better terms and conditions from service providers, monitor data sharing agreements or, in some cases, obtain a variety of insights.[59]

Finally, one important issue that may require a more formalized and recognized form of mandate for data rights relates to the identification of data subjects. Research has shown widely divergent practices on how controllers go about verifying the identity of data subjects exercising their rights.[60] This likely becomes even more complex when data rights are exercised through a DRI. However, controllers cannot use their duty to keep personal data secure (Articles 5(1)f and 32) as a blanket refusal to accommodate any mandated data rights exercise. Pursuant to Article 11(2), the data subject and mandated actor can provide the necessary evidence to demonstrate the veracity of the request. The burden of proof rests with the controller to establish why, based on all the evidence provided, it can still not identify the veracity of a (mandated) data subject right's exercise (Article12(2)). Furthermore, the security obligation and duty for controllers to assess the legitimacy and veracity of any mandated request will also need to be interpreted in light of the data right that is invoked. As an example, accommodating a right of access (especially if personal data would be sent to the mandated actor) entails more risks than accommodating other rights (such as the right to object or restrict processing).

Formalizing data rights intermediation—a private law perspective

The possibility to exercise data rights through a third party has already been at the centre of attention for policymakers, data protection authorities,[61] academics,[62] and civil society.[63] The GDPR remains silent on whether and how data rights can be mandated to any third party (cf above), and the Data Governance Act specifies that data rights 'are personal rights of the data subject and that data subjects cannot waive such rights',[64] further complicating our understanding of data rights mandatability.

Focusing on the legal concept of mandates as traditional yet polyvalent contractual tools within many jurisdictions, in this section, we approach the issue of mandating data rights from a private law perspective. We explain both why data rights are mandatable and the form and shape that this mandate will have. Rather than reinventing the wheel, we propose to look at existing private law constructs which have historically framed the context of application of mandates to different types of rights' exercise. The overall aim is to provide some much-needed terminological clarity and to

56 Cf Table 1.

57 Bits of Freedom (n 13) is a good example of this type of intermediation.

58 Delacroix and Lawrence (n 21).

59 A notable example includes mass access requests with Dexia bank in the Netherlands, used in litigation to expose malpractices. See Mahieu and Ausloos (n 6) 30.

60 C Norval and others, 'Reclaiming Data: Overcoming App Identification Barriers for Exercising Data Protection Rights' (2018) arXiv:180905369 [cs]; Veale, Binns and Ausloos (n 2); Ausloos and Dewitte (n 20); C Boniface and others, 'Security Analysis of Subject Access Request Procedures How to Authenticate Data Subjects Safely When They Request for Their Data' (*Annual Privacy Forum*, 13 June 2019) <https://hal.inria.fr/hal-02072302/document> accessed 18 March 2022.

61 CNIL, 'Délibération n° 2021-070 du 27 mai 2021 portant adoption d'une recommandation relative à l'exercice des droits par l'intermédiaire d'un mandataire' <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2021-070-recommandation-exercice-droits-_mandataire.pdf> accessed 18 March 2022.

62 Delacroix and Lawrence (n 21).

63 Ada Lovelace Institute, 'Exploring Legal Mechanisms for Data Stewardship' (Final Report, March 2021) <https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/> accessed 18 March 2022.

64 Data Governance Act (Regulation 2022/868 of 30 May 2022 on European data governance and amending Regulation 2018/1724 (Data Governance Act) OJ L 152/1 of 3 June 2022, Recital 31.

assess the appropriate framework within which mandates can fulfil their intended purpose in realizing data rights' full potential.

Putting mandates of data rights in context

Scene setting: exercise of rights in private law

Data rights sit within already well-established legal constructs and traditions that enable effective rights' enjoyment, such as applicable contract law frameworks for example. In order to ensure that data rights achieve their desired outcome, it is important to consider how these legal constructs and traditions apply to *data* rights' exercise.

There are several legal constructs putting in place the conditions through which rights can be exercised, depending on the (in)direct beneficiaries and the scope of protection. These constructs attempt to contextualize the rights' exercise and to create the appropriate environment within which rights can best achieve their purported legal raison d'être. As such, they provide the necessary scaffolding for applying abstract (data) rights to concrete situations. The diverse range of legal constructs also attests to the variable needs underlying all kinds of different rights and the contexts in which they might be relevant.

Safeguards put in place for the exercise of rights are generally built into the respective law stipulating them, generally in order to pre-empt or counter the power dynamics at play and protect individuals in more precarious positions. In essence, the logics underlying this framework-building can be traced back to the nature of the right, its rationale, the individual(s) benefitting from its exercise, and the risks which these individuals might be exposed when attempting to achieve their purpose(s). For instance, a right can be proclaimed inalienable due to its protective value being inherently linked to the beneficiary in question.[65] Data rights in particular are specifically designed as intent-agnostic tools aimed at empowering data subjects in any situation where the processing of personal data may affect any of their interests, rights, or freedoms. In light of the legislator's explicit aim to facilitate the exercise of these rights, that exercise cannot a priori be considered to be constrained to specific purposes or contexts only.

Mandates are used to enable a party other than the rights' beneficiary to exercise the rights in question according to the terms agreed upon with the original rightsholder. In this section, we present an overview of the types, limits, and extent of legal tools that enable third parties to exercise one's (data) rights using examples from representative jurisdictions. We will identify common *ratio legis* patterns, highlight parallels, and draw from examples that can inform the practicalities of mandating data rights. This attempt at systematizing the different formulations is a useful exercise because it unlocks—or even determines—the substantial and formal requirements in framing and enabling the mandatability of data rights. Additionally, placing rights mandates along different legal formulations that can be used by the rights' beneficiary to exercise their right is important in clarifying (and clearly demarcating) related concepts such as alienation of a right, clearly to be distinguished from mandating the exercise of a right. Indeed, in debates on data rights exercises by third parties, or governance models for so-called 'data intermediaries', we observe commentators conflating the alienation and mandating of (data) rights.[66] More specifically, the inalienability of data rights is often put forward as the main challenge and reason why these rights cannot be mandated to a third-party actor. Yet, as our ensuing analysis will show, inalienable rights can indeed be exercised through a mandate.

Table 2 presents a spectrum of different ways in which rights can be exercised, specifically considering third parties being delegated for their exercise. The one on the rightmost extremity is the straightforward exercise of (data) rights by rightsholders themselves and needs no further elaboration in the context of this article. As the line moves further leftwards, the rights exercise moves further away from the rightsholder, first through a mandate, then a rights transfer, and in most extreme cases rights abandonment. Before looking at rights mandates in particular ('Assigning data rights through mandates' section), this subsection will briefly elaborate on the latter two.

Alienation of rights: abandonment and transfer

A rights' mandate, ie a rights' exercise by *proxy* will first be distinguished from other contractual constructs of exercising a right, specifically the acts of alienation

65 This is particularly relevant in intellectual property law protections, where *a priori* moral rights are conceived to be inalienable.

66 See, for instance, E Bietti and others, 'Data Cooperatives in Europe: A Legal and Empirical Investigation' White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint (December 2021) <https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf>; F Vogelezang, 'A Closer Look at Data Intermediaries and the Risk of Platformization' (*Open Future Blog*, 1 March 2022) <https://openfuture.eu/blog/a-closer-look-at-data-intermediaries-and-the-risk-of-platformization/> accessed 18 March 2022.

Table 2. Overview of different forms of exercise of rights

Rights abandonment	Rights transfer	Rights mandate	Individual exercise
Complete **extinction** of a right	Extinction from the original rightsholder due to **movement** to the new beneficiary	Exercise a right **in the name of** the rightsholder	Exercise by the rightsholder **themselves**

The words in bold demarcate the distinctive elements of each category of exercise of rights.

including the abandonment of a right, and the contractual transfer of a right from one beneficiary to another.

Rights' abandonment refers to the situation where a right is extinguished not only from the personal sphere of the original rightsholder and beneficiary, but also from the public sphere in general. This is a unilateral act declaring that the right is exiting the personal protective sphere of the beneficiary. Rights can be abdicated, unless they are deemed inalienable by the applicable normative framework. The voluntary extinction of a right—abdicating it from the beneficiary's legal armoury—aims to relinquish the existence of a right as it is (by law) tied to the rightsholder themselves. This relinquishment of a right is in some cases qualified as eviction whereby the owner relinquishing a right is usually tied to a physical object the right seeks to protect. For instance, a property owner abandons their *dominium* over the object through an act that does not involve the transfer but the extinction of a right. Simply abstaining from exercising a right—even for a prolonged period of time—does not constitute an implicit abandonment of the right in question.

In principle, data rights are inalienable. They cannot be abandoned since they are foundational elements—and give shape to the underlying rationale—of Article 8 of the EU Charter of Fundamental Rights. According to the Charter, 'everyone' has a right to data protection, with no attached preconditions. The broad, protective scope of the GDPR, including positive rights enabling the effective protection of fundamental rights, combined with a broader tradition of non-waiverability in fundamental rights law,[67] all attest to the inability to abandon GDPR data rights by any contractual (or unilateral) means. The recent Data Governance Act confirms this, by clearly highlighting in Recital 31 that 'the rights under Regulation (EU) 2016/679 are personal rights of the data subject and that data subjects cannot waive such rights.'[68] This ban to waiving the right to data protection does not prevent contractual arrangements on how the different GDPR data rights can be exercised, but it puts a barrier to various power dynamics that lead to consenting to a waiver of exercise of these data rights altogether.

Rights' transfers are most common in (intellectual) property-like transactions. Transferred in part or in full, for a price or for free, for a specified amount of time or permanently, the conditions of the contractual arrangement are subject to the voluntary agreement between the parties and to the normative limitations of applicable law. The decisive factor—relevant for our purposes here—is whether the rights exit the personal sphere of the original rightsholder (who *a priori* no longer has agency over the right(s)) and enters that of the receiving party. Importantly, what qualifies something as a 'rights transfer' is the privileges that are created for the receiving entity. In contrast to the transfer of rights related to a physical object (where the dominium on the object accompanies the legal act of transfer of rights related to it), a data rights' transfer can lawfully occur only when it does not entail alienation. Data rights are attached to the individual data pertains to—the data subject, and are therefore *a priori* non-transferable.

Even though data rights cannot be alienated, they can be subject to contractual and legal tools usually reserved for transfers of rights. The most prominent example in this category is the application of trust law relationships[69] to data governance and data rights.[70] This means that the transfer of data rights to an

67 See M Finck, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2022) 11 International Data Protection Law Review 333; N Purtova, *Property Rights in Personal Data: A European Perspective* (BOXPress BV Oisterwijk 2011) 232.

68 Data Governance Act (Regulation 2022/868 of 30 May 2022 on European data governance and amending Regulation 2018/1724 (Data Governance Act) OJ L 152/1 of 3 June 2022.

69 In the UK common law system, the subject matter of a trust need not be only property, but any type of right, See B Mcfarlane and R Stevens, 'The Nature of Equitable Property' (2010) 4 The Journal of Equity <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1350473> accessed 18 March 2022.

70 The theoretical framework underlying data trusts has been put forward in Delacroix and Lawrence (n 21); For examples of data trusts currently under development, see <https://datatrusts.uk> accessed 18 March 2022.

intermediating party can be formulated through specific legal constructs that permit the data subject to not forego the data rights' protection, ie to enable the transfer without alienation in favour of a tripartite relationship with special constraints and loyalty obligations. There are notably trust-like legal relationships that are established in civil law systems such as the *Treuhand* in German law, but these bear little resemblance to their common law counterparts.[71]

It is important to highlight that these legal constructs cannot deprive the data subject of individually exercising their data right(s) in question. Even so, this non-exclusivity does not render useless the transfer of data rights, as illustrated by one example in the GDPR where this is expressly permitted even if restrictively interpreted. Article 8 GDPR temporarily transfers the right to (withdraw) consent for children below the age of 16 (13 in some Member States),[72] to the holder of parental responsibility.[73] Any exercise of these data rights needs to be interpreted in light of the child's interests.[74] The ICO also explains that holders of parental responsibility can exercise children's data rights when the child is unable to understand the processes involved in exercising their rights.[75] The legislator has (albeit implicitly) created space for the parallel exercise of data rights of children (ie the data subjects). This would be a legally prescribed transfer of a right without alienation, but only within the framework of the specified purpose. Attending to a child's interests is the singular goal for which parents or guardians are entitled—without the need for an express mandate—to exercise these data rights for their children. This is confirmed by the European Data Protection Board's (EDPB) recent guidelines on the exercise of the right of access. According to the guidelines, 'the best interests of the child should be the leading consideration in all decisions taken with respect to the exercise of the right of access in the context of children, in particular where the right of access is exercised on behalf of the child, for example by the holder of parental authority.'[76]

Outside of the strict GDPR framework and the special category of children's data rights, the same EDPB guidelines point out that exercising a right of access on behalf of a deceased person can be considered as yet another instance of exercise by *proxy* that can likely be regulated on a national law level. According to the EDPB, 'while the exercise of the right of access to personal data of deceased persons amounts to another example of access by a third party other than the data subject, Recital 27 specifies that the GDPR does not apply to the personal data of deceased persons. The matter is therefore dealt with by national law as Member States may provide for rules regarding the processing of personal data of deceased persons.'[77] Some Member States are already regulating the exercise of rights after death, giving the possibility to explicitly mandate an individual (or any entity) the exercise of data rights post-mortem.[78] It is important to highlight that while the special rules attached to *post mortem* data protection and the challenges related to these entities receiving (and processing) data of deceased people[79] all fall outside of the scope of this article, the right to exercise data rights on behalf of a deceased person is likely to derive its legitimacy either by law (eg Member States creating special rules on who inherits data rights' exercise privileges from deceased people) or through contractual agreements.

Assigning data rights through mandates

Mandates are generally described as contracts permitting the rights' exercise by a party other than the rightsholder. Acknowledging the pluriformity of this legal concept, this section briefly presents the scope of

71 See section 3.3, where we address fiduciary obligations.

72 I Milkaite and E Lievens, 'The Changing Patchwork of the Child's Age of Consent for Data Processing across the EU' (*Academic Blog*, no date) <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751> accessed 18 March 2022.

73 The provision specifically applies to situations where the processing of personal data relies on consent (art 6(1) GDPR) in relation to the offer of information society services directly to a child.

74 For instance, 'The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child', see Recital 38 GDPR. I Milkaite, 'A Children's Rights Perspective on Privacy and Data Protection in the Digital Age: A Critical and Forward-Looking Analysis of the EU General Data Protection Regulation and Its Implementation with Respect to Children and Youth' (Dissertation, Ghent University 2021).

75 For instance, according to the UK ICO, 'You should therefore only allow parents to exercise these rights on behalf of a child if the child authorises them to do so, when the child does not have sufficient understanding to exercise the rights him or herself, or when it is evident that this is in the best interests of the child' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-rights-do-children-have/> accessed 18 March 2022.

76 European Data Protection Board (EDPB), 'Guidelines 01/2022 on Data Subject Rights - Right of Access' (adopted on 18 January 2022, para 84.

77 Ibid para 81.

78 L Edwards and E Harbinja, 'Protecting Post-mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World' (2013) 32 Cardozo Arts & Entertainment Law Journal 83; G Malgieri, 'R.I.P.: Rest in Privacy or Rest in (Quasi-) Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions' in R Leenes and others (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2018) 300; M Van Eechoud and others, 'Data after Death – Legal Aspects of Digital Inheritances' (Report commissioned by the Dutch Ministry of the Interior and Kingdom Relations, April 2021) <https://www.sectorplandls.nl/wordpress/news/data-after-death-legal-aspects-of-digital-inheritances/> accessed 18 March 2022.

79 E Harbinja, 'Post-mortem Privacy 2.0: Theory, Law, and Technology' (2017) 13 International Review of Law, Computers & Technology 26.

authorizations and restrictions attached to mandates ('Exercise of rights: mandate' section), before exploring how these can be applied to GDPR data rights ('Regulating mandates of data rights' section).

Exercise of rights: mandate

The exercise of a right can be assigned to a party other than the original rights' beneficiary, which becomes authorized to exercise the right *on behalf of* the beneficiary in question. These contractual acts—the mandates—permit the concession of the exercise of a right within the limits set by the rightsholder, ie the data subject. In certain jurisdictions, mandates are regulated as special contracts with specific scope, objectives, formalities, and liability structures.[80] In others,[81] mandates are rather amorphous and dynamic, defined generally as the acts by which one person gives another the power to do something for the former and in their name.

Mandates are a distinct category of rights' exercise.[82] They appear either as special contracts subject to specific rules or as expressly designed contracts subject to the general contract law provisions. For example, the French private law formulation *mandats* describes a strict framework that applies to both procurations and mandates, as acts 'by which one person gives another power to do something for them and on their behalf'.[83] This set of rules mainly applies to property rights management, as is also revealed by the civil code chapter in which it can be found. Similarly, procuration (or power of attorney)—the legal construct for mandating rights to an attorney—is described in the Dutch civil code in a way to expressly note that these provisions apply accordingly outside the field of property law as far as the nature of the legal act or the legal relationship does not oppose to this procuration act.[84] Belgian civil law describes and regulates both general and special mandates. The special ones, such as the one described in Article 490 of the Belgian civil code concerning extrajudicial protection mandates, are still subject to the same formality rules as the general ones regulated by Articles 1984–2010 of the same civil code, but they also follow special restrictions and formalities especially when it comes to mandate revocability and revocation. Germany has created a similar regulatory framing for mandates, relying on general contractual provisions that create the legal obligations derived from these contractual agreements.

Mandates are polyvalent: the framework describing the rights' exercise can be dictated (more or less firmly) by law and/or by contract. Take, for instance, the mandate for representation in court (or power of attorney). This mandate permits the representation of a client's rights in court, a relationship largely defined by the contract signed between the two parties and by professional duties and ethics standards.[85] This type of relationship between the two parties is substantiated through legal statutory obligations that ensure the loyalty and fiduciary obligation and duty of care, among other liabilities. The relationship is not solely defined by the contract terms, but also by the legal assurances and deontological codes which address disciplinary actions in case of breaches.[86] In other words, mandate agreements in the context for representation in court, are firmly embedded within both a regulatory framework and deontological rules. In the case of the representation-in-court mandate for instance, the mandated party has to be a qualified lawyer. We see thus a legal restriction in the type of actor that is qualified to act as a mandated entity for this specific rights exercise.

Similarly, Article 80 GDPR designates a particular type of the third party that can be mandated by data subjects to exercise a number of remedial rights. As already discussed, this provision expressly clarifies that the right to a judicial remedy on behalf of data subjects can be mandated to a 'not-for-profit body, organisation or association' which has been 'properly constituted in accordance with member state or EU law'. In essence, Article 80 enables pre-specified entities to exercise a subset of procedural rights attached to the data subjects (ie Articles 77–79; Article 82).

One could argue that, since the GDPR includes specific instances of representation already (ie consent provision for children in Article 8 and remedial rights in Article 80), other forms of substitution in the exercise of GDPR rights are *a contrario* not allowed. Such argument would further be substantiated by an earlier public draft of the Data Governance Act, which specified in Recital 24 that 'the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data

80 For instance, the French 'mandat' is regulated as a special contract bearing specific formalities, obligations, and liabilities.

81 In Belgium, mandates are generally defined and regulated by arts 1984–2010 of the Belgian Civil Code.

82 See section 3.1.1.

83 See arts 1984–2010 of the French civil code.

84 Art 3:79 BW

85 For the fiduciary obligations in representation mandates, see RW Painter, 'Fiduciary Principles in Legal Representation' in EJ Criddle, PB Miller and RH Sitkoff (eds), *The Oxford Handbook of Fiduciary Law* (OUP 2019).

86 See, for instance, the regulation of power of attorney mandates in Germany A Ruhaak, 'Data Trusts in Germany and under the GDPR' (2020) <https://algorithmwatch.org/en/data-trusts/> accessed 18 March 2022.

cooperative.'[87] We find that this restrictive interpretation neglects the diversity of GDPR rights and the polyvalence of their exercise which can only be fulfilled with the necessary contractual freedom. We have already highlighted that the rationale for GDPR data rights focuses on empowering data subjects in order to ensure their effective and complete protection (cf 'Data rights' section). The exercise of these rights reflecting data subject empowerment can occur within complex power asymmetries which can more efficiently be countered with the mandated intermediation in the (collective) rights' exercise. The restriction of this freedom to exercise a right through a mandated actor would only operate as an obstacle rather than an enabler in the efficient protection of data subjects. That is also why we welcome the revised recital in the final text of the DGA, stating that 'the rights under Regulation (EU) 2016/679 are personal rights of the data subject and that data subjects cannot waive such rights', which is in line with our arguments in 'Putting mandates of data rights in context' section.

Regulating mandates of data rights

The GDPR describes numerous modalities meant to support data subjects in exercising their data rights, notably in Articles 12, 24–25. Naturally, the specific conditions for mandating data rights will be affected by the type of data right at stake; ie data rights focused on *transparency*,[88] on *personal data*,[89] or on *specific processing operations*.[90] This is because of the diverging goals and challenges of different (types of) data rights. In practice, mandates which enable an entity other than the data subject to exercise data rights within specific one-off situations are not uncommon. The mandating of delisting rights in the name of a data subject vis-à-vis a search engine[91] is but one example of these practices. Currently, there is noticeable interest from data protection authorities in exploring how these mandates can be used for the rights of access and portability.[92]

In France, for example, a rather specific provision was introduced into an executive order to address the mandating of data subject rights. This provision requires that such mandates explicitly specify whether the mandator can also receive the answer to the data rights exercise from the data controller directly.[93] In its recommendations, the French DPA (CNIL) refers to this provision, but only to explain how a mandate would function in the context of an exercise of the right of access or a right of portability request (ie highlighting the controllership framework of responsibilities). This focus on data access and data portability rights—despite the actual provision encompassing *all* data rights—could be due to their enabling function for other data rights as well as their prominence in current data governance-related policy debates. It could also be an express policy choice to focus regulatory attention on the mandatability of these rights in particular. Overall, even if most regulatory, policy, scholarly, and even technical attention appears to focus on the rights of access and portability, we think it is important to consider mandates concerning other data rights too. This would imply addressing their discrete particularities and how these might affect the context within which mandates can be used, their extent, and potential risks.

Fiduciary obligations

Whether general-purpose or specific, mandates by themselves are an insufficient tool to convey extra-contractual obligations, especially when none are prescribed by law. These obligations come in the form of deontological codes, loyalty obligations defining a duty of care, as well as fiduciary obligations. Fiduciary regimes have become a recurring concept in data governance discussions and are particularly relevant in the context of the mandatability of data rights. In this section, we briefly explore what can be learned from fiduciary regimes when it comes to concretely giving shape to data rights mandates.

A critique of 'information fiduciaries'

In order to unpack how fiduciary duties can feed into the formalization of data rights mandates, it is useful to

87 Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act) Brussels, 25 November 2020, COM(2020) 767 final, 2020/0340(COD).

88 Arts 15, 20 GDPR.

89 Arts 16, 17 GDPR.

90 Arts 18, 21, 22 GDPR.

91 Especially since the CJEU confirmed the existence of a right to be delisted from search engines in *Google Spain*, several companies have started offering 'reputation management' services, see B Medeiros, 'The Reputation-Management Industry and the Prospects for a "Right to Be Forgotten" in the US' (2017) 51 First Amendment Studies 14.

92 See, for instance, Commission nationale de l'informatique et des libertés (CNIL), 'Délibération n° 2021-070 du 27 mai 2021 portant adoption d'une recommandation relative à l'exercice des droits par l'intermédiaire d'un mandataire' (27 May 2021) <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2021-070-recommandation-exercice-droits-_mandataire.pdf> accessed 18 March 2022.

93 According to art 77 of the Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 'La demande peut être également présentée par une personne spécialement mandatée à cet effet par le demandeur, si celle-ci justifie de son identité et de l'identité du mandant, de son mandat ainsi que de la durée et de l'objet précis de celui-ci. Le mandat doit également préciser si le mandataire peut être rendu destinataire de la réponse du responsable du traitement ou du sous-traitant.'

take a critical look at the concept of so-called 'information fiduciaries'. The concept of 'information fiduciaries' gained prominence after US scholar Jack Balkin wrote about them specifically in relation to data collecting platforms. In short, Balkin suggested that economic and tax[94] incentives[95] ought to be offered to such platforms in exchange for their accepting 'fiduciary obligations'[96] (they would thereby become 'information fiduciaries'). This proposal is problematic on several counts, not least because it underestimates the extent to which fiduciary obligations are incompatible with any form of conflict of interest. We expand on this 'incompatibility with conflicts of interests' aspect below, since it also has a bearing in the context of the fiduciary responsibilities of DRIs in particular.

Balkin is right to point out that 'fiduciary' does not mean 'not for profit',[97] but rather an obligation of *undivided loyalty* towards patients/clients. Yet since Balkin's 'information fiduciaries'—ie data-collecting platforms—have a business interest in amassing data provided by data subjects (and a concomitant responsibility towards their shareholders), they would not be able to honour such an obligation of undivided loyalty. To honour their fiduciary obligations towards data subjects, such platforms would have to be free of any imperatives imposed by shareholders (whether these imperatives take the form of data monetization or otherwise). While Balkin acknowledges the potential for conflict of interest, he fails to draw the only logical conclusion: a fiduciary obligation towards data subjects is incompatible with data controllers' responsibility towards their shareholders.

While this critique is based on Balkin's framing of 'information fiduciaries' in the context of data-collecting platforms, we believe it to be of relevance for DRIs as well. As seen previously, a DRI need not collect any personal data. While its business model need not hinge on drawing value from personal data, a DRI may nevertheless be faced with no less significant conflicts of interest. For example, a DRI helping individuals to (collectively) exercise their rights to erasure[98] or object[99] may have perverse incentives, which stem from commercial interests in the companies targeted by those requests.

To honour a fiduciary obligation not only demands a robust absence of conflict of interest, it also requires an ability to relate to the complex and multi-faceted nature of the vulnerability inherent in the data subject/intermediary/data controller relationship. In this respect, the 'information fiduciary' proposed by Balkin[100] would be placed in a position that is comparable to that of a doctor[101] who gains a commission on particular drug prescriptions or a lawyer who uses a company to provide medical reports for his clients while owning shares in that company.[102]

Fiduciary duties informing data rights mandates

Fiduciary obligations are sometimes offered as an alternative panacea to the lack of trust-related legal structures in civil law countries.[103] What these proposals lack is sufficient clarity over the sort of fiduciary obligations that would need to be attached to any DRI when mandated to exercise specific data rights on behalf of the data subject.

As trusts tend to vary between different jurisdictions, so do fiduciary duties. Even if the trust is considered to be the most developed institutionalization of fiduciary obligations, there are numerous legal constructs in civil law jurisdictions that attempt to fulfil the same purposes as those of the trust.[104] However, so far there is no 'lowest common denominator' that could ground a purported harmonization of fiduciary obligations in civil law countries.

In most civil law jurisdictions, the application of a rights mandate comes with some type of fiduciary obligations. The most common one is a loyalty obligation when it comes to the performance of the contractual terms. For instance, the French civil code attaches a fiduciary loyalty obligation to all *contrats de mandat*. In Germany, the general obligation law principles apply for

94 JM Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 UC Davis Law Review 1183.

95 J Zittrain, 'Engineering an Election' (2013) 127 Harvard Law Review Forum 335, 339 also suggests immunity from certain kinds of lawsuits among the incentives that could be offered.

96 Balkin (n 94) 1229.

97 Indeed, in many jurisdictions healthcare providers and lawyers are deemed to have fiduciary obligations towards their patients or clients. This does not mean that they cannot be paid for their work.

98 Art 17 GDPR.

99 Art 21 GDPR.

100 Aside from sidestepping the conflict-of-interest issue mentioned above, Balkin's information fiduciary proposal only affords protection to those who are already in a contractual relationship with 'digital companies'. Balkin acknowledges this issue in JM Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation Essays' (2017) 51 UC Davis Law Review 1149.

101 Balkin's proposal has the merit of acknowledging some of the similarities between the vulnerability that characterizes the doctor/patient (or lawyer/client) relationship and that which underlies the data–subject/data–controller relationship, even if Balkin only focuses on the epistemic aspect of data–subjects' vulnerability: Balkin (n 94) 1216 and 1222.

102 *Solicitors Regulation Authority v. Dennison* [2012] EWCA Civ 421.

103 See, for instance, Aapti Institute, 'Enabling Data Sharing for Social Benefit through Data Trusts' An Interim Report for the 2021 GPAI Paris Summit <https://gpai.ai/projects/data-governance/data-trusts/enabling-data-sharing-for-social-benefit-data-trusts-interim-report.pdf> accessed 18 March 2022.

104 See, for instance, the *Treuhand* regime in Germany.

all mandates (*Auftrag*) whether gratuitous or commercial, and the mandated entity is expected to be subject to the fiduciary loyalty duty vis-a-vis the mandator.[105]

The fiduciary regime refers to a normative framework that applies heightened duties of care and loyalty obligations to relationships that are often marked by a situation of vulnerability, such that one of the parties has little choice but to trust the other. There are a variety of legal regimes that incorporate such heightened duties, such as the common law trust, the German *Treuhand*, the French *fiducie*, and, in some countries, professional responsibility regimes.

The *Treuhand* regime does include a duty of loyalty (whose nature depends on the exact type of trust, serving the interests of the principal or of the trustee) and a duty to not compete. Ultimately, the extent of these duties will be clarified through the contractual relationship that forms the *Treuhand*. This highlights the sometimes-problematic dependence on contracts in the establishment of certain fiduciary duties.

In the French legal system, the *fiducie* is a specific regime, where the party in charge of exercising a right shall act for a specific purpose for the benefit of one or more beneficiaries.[106] It is highly formalistic, applies only to a small subset of financial relations, and it precludes individuals who do not fall under the strict professional categories, ie corporate bodies in the banking, insurance, or finance sectors listed in the Monetary and Financial Code, and lawyers. This a priori regulation of what types of intermediaries can be placed as responsible entities in the *fiducie* is linked to the legislator's intent to subject only individuals with a strict professional duty of loyalty to this regime. The liability of the trustee in this *fiducie* regime is rather loosely determined in Article 2026 of the French civil code which states that the trustee is personally liable for any wrong committed whilst carrying out their obligations. The exact nature of this liability (contractual, extra-contractual/tort, or both) is undetermined.

Fiduciary obligations systematically appear in specific sectors. Take the financial sector for example. According to the Markets in Financial Instruments Directive ('MiFID II'),[107] when financial advisers provide investment services to their clients, they have a statutory obligation to act honestly, fairly, and professionally in accordance with the best interest of their clients. Commercial and financial relationships are emblematic among civil law frameworks establishing fiduciary relationships and duties. With the pressure to ensure a harmonized application of fiduciary obligations across European jurisdictions, emerges a need for uncovering fiduciary relationships as an autonomous concept among Member States. This becomes particularly salient when one considers the political economy of data.[108] From this brief overview, it especially becomes clear that in none of the abovementioned systems, the corresponding fiduciary obligations can easily extend to a more mature data governance.

As previously mentioned, the recent EDPB guidelines on data subject rights—and specifically, the right of access—consider the possibility that this right's exercise can be fulfilled through 'portals/channels provided by a third party'.[109] The EDPB concedes that there are third parties that can make access requests on behalf of data subjects,[110] as long as adequate accountability structures are in place. Along this line, the EDPB expressly refers to the 'national laws governing legal representation (eg powers of attorney), which may impose specific requirements for demonstrating authorization to make a request on behalf of the data subject, should be taken into account, since the GDPR does not regulate this issue.'[111]

The EDPB's reference to national legal representation frameworks is interesting, since the power imbalances inherent in the lay–professional relationship have long given rise to a recognition of the need for professional duties that go beyond a standard 'duty of care'. The courts' delineation of such enhanced duties varies from jurisdiction to jurisdiction, with some countries (like Canada) explicitly applying fiduciary standards.[112] In the UK, the comparatively low level of doctrinal interest for fiduciary duties and their potential as an independent ground for action in professional malpractice claims can be traced back to Lord Scarman's dictum in *Sidaway*.[113] Yet there is an increasing number of voices who consider it is time for the reinstatement of

105 For an overview of civil law fiduciary duties, see M Gelter and G Helleringer, 'Fiduciary Principles in European Civil Law Systems' in EJ Criddle, PB Miller and RH Sitkoff (eds), *The Oxford Handbook of Fiduciary Law* (OUP 2019).

106 Cf arts 2011–2030 French Civil Code.

107 EU Regulation 600/2014 of the Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 OJ (2014) L 173/84.

108 The articulation of a European-wide (data) fiduciary regime deserves further work. While this is a subject of particular interest and continues to take on new forms in the new complex data ecosystems, it is not where the contribution of the present article lies.

109 EDPB (n 76) paras 87–89.

110 Arguably, this can be extended to other data subject rights as well.

111 EDPB (n 76) para 80.

112 As far as medical practice is concerned, Canada does characterize the patient-doctor relationship as fiduciary.

113 *Sidaway v Bethlem RHG* [1985] 1 All ER 643. This dictum unequivocally dismissed the possibility of obtaining equitable relief on the basis of a breach of fiduciary duty by a doctor.

professional fiduciary duties, since such duties are better suited to the kind of vulnerability at stake.[114] The latter debate is of direct relevance to the delineation of adequate accountability mechanisms in the context of data rights mandates.

Whatever form it takes, (eg legal representative, NGO, a union), DRI mandates must be specific enough to address the needs and aspirations of the data subject, and do so in a way that acknowledges the relevant vulnerabilities. These vulnerabilities may involve asymmetries in technical or legal knowhow, but can also be tied to the right and/or data at stake.[115]

The enhanced duties and safeguards called for are not easily achieved through contracts alone, given the extent to which the latter are likely to fall prey to problematic power dynamics, whereby the mandated actor could unilaterally determine terms (in the absence of built-in protection for the presumed weaker party). To remedy this, a presumption of unequal bargaining power (present in sector-specific contracts such as labour and copyright) should be applied to the benefit of the data subject, especially in cases where mandate interpretation is uncertain. Such presumption would ideally go hand in hand with the delineation of fiduciary duties. This delineation may be prompted by national legislation, or evolve through case law, and needs to be accompanied by robust institutional oversight.

This institutional oversight dimension is key: without institutional mechanisms to give them 'teeth' (such as the overseeing court in the case of data trusts), fiduciary responsibilities risk becoming little more than make-believe. This would in turn transform a well-intentioned construct—DRIs—into a way of perpetuating the very power imbalances they were meant to address. In light of their mandate to monitor and enforce the application of the GDPR (Articles 51, 57), we believe data protection authorities are among the most evident actors to ensure data rights mandates are respected (and respectful). This will need to be complemented by a 'local' regulatory layer, not unlike the professional bodies regulating the way in which doctors, lawyers, and other professionals discharge their—often fiduciary—duties in light of the vulnerabilities at stake. Indeed, to the extent that mandatability constitutes a vital component for effectuating data rights, data protection authorities have an active duty to ensure they are properly complied with pursuant to Article 8(3) Charter.

Conclusions

As the need to develop a culture (and legal infrastructure) that stimulates the exercise of data rights is increasingly recognized, the value inherent to their collective exercise is becoming apparent. In this context, DRIs have emerged as entities charged with facilitating rights exercises, often with a focus on the right of access and the right to data portability. In this article, we explored the application of relevant legal frameworks for mandating data rights. These rights' mandates are not expressly framed in the GDPR and as evidenced by brief references in the Data Governance Act, their delineation can be ambiguous. Thus, it is important to first highlight that data rights are in fact mandatable and this without affecting their inalienable nature.

The goal of this article is 2-fold: first, we address the question of whether data rights are mandatable (ie whether they can be exercised by an intermediating entity); and secondly, we explore how existing private law constructs across different jurisdictions can be used to inform such mandates. We argue that private law can already provide the legal framework and necessary assurances to lawfully mandate a right's exercise. Contract law and fiduciary duties both have longstanding traditions and robust norms in many jurisdictions, all of which can be explored towards shaping the appropriate environment to regulate data rights mandates in particular.

The absence of trust-like relationships in civil law jurisdictions is not (and should not be) the determining factor shaping the regulation of data rights mandates. Indeed, while trust-like legal constructs can certainly help inform institutional safeguards for DRIs, we argue that the key in unlocking the full potential of data rights mandates can already be found in existing civil law constructs. Naturally, the diversity in how different legal systems regulate fiduciary obligations, coupled with that in contract law, reveals the need for solidifying the responsibility and accountability of mandated DRIs. The DGA already introduces the need to create trust through fiduciary duties for data intermediaries operating as data sharing service providers. In order to identify the

114 For an argument along this line in the context of education, see: BG Scharffs and JW Welch, 'An Analytic Framework for Understanding and Evaluating the Fiduciary Duties of Educators' (2005) number 2 Brigham Young University Education and Law Journal 159; RP Schuwerk, 'The Law Professor as Fiduciary: What Duties Do We Owe to Our Students' (2003) 45 South Texas Law Review 753. In the (Canadian) legal context, see A Woolley, 'The Lawyer as Fiduciary: Defining Private Law Duties in Public Law Relations' (2015) 65(4) University of Toronto Law Journal 285–334.

115 The contours of such a 'sense of self' vulnerability and its implications when it comes to the delineation of heightened duties of care is discussed in S Delacroix, 'Professional Responsibility: Conceptual Rescue and Plea for Reform' (2021) 42(1)Oxford Journal of Legal Studies gqab010 1–26 <https://doi.org/10.1093/ojls/gqab010>.

legal conditions and safeguards to be considered by DRIs, we first need to recognize that (data rights) mandates are contracts. The continued adherence to fundamental contract law principles will have to be complemented by a robust framework of institutional safeguards. The need for such safeguards stems from the vulnerable position of data subjects, both vis-à-vis DRIs as well as data controllers. This article explored and identified some key components to be considered in such a framework, so as to ensure data rights mandatability can become a powerful tool in the hands of data subjects.

https://doi.org/10.1093/idpl/ipac017
Advance Access Publication 17 October 2022