

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

Elettra Bietti
Harvard Law School

Ander Etxeberria
TAZEBAEZ – Travelling U | Mondragon University

Morshed Mannan
European University Institute

Janis Wong
University of St Andrews

Contents

Introduction	2
Objectives and Takeaways	3
Project Goals	3
Project Audience	3
Project Methodology	3
Main Takeaways from Interviews	4
Context: Data and Cooperatives in Europe	6
What is Data?	6
Data Co-operatives: Landscape and Typologies	8
Ideologies of the cooperative movement, goals and challenges	9
Data Governance: Law and Policy	11
Existing legal framework for (data) cooperatives	11
Legal proposals that are of relevance for data cooperatives	15
Discussion & Key Takeaways	20
Understanding data cooperatives	20
Key Takeaways and Next Steps	21
Conclusions	24

Introduction

In spite of significant developments in the European Union's digital and data policies in the last five years, not least the entry into force of the General Data Protection Regulation (GDPR) in 2018, there continue to be lingering concerns surrounding our increasingly datafied society. This includes the outsized control that multinational corporations have over citizens' data and the need to incentivize the creation of neutral data intermediaries and alternative business models that prioritize commoning and altruism. Some of the existing EU data co-operatives (e.g., polypoly SCE, Salus.coop) have been formed to meet part of these concerns. While these data co-operatives demonstrate promise in creating a more inclusive, equitable, and empowering form of data management, the adoption of co-operative or similar infrastructures is yet to be seen as a feasible model for governing data. The potential and success of these novel and radically different organizations, many of which operate within the EU, thus depends on the evolution of EU legal and policy frameworks, alongside the rise of the citizens' awareness and the adoption of data cooperative solutions.

As part of the New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society "Alternative Data Futures: Cooperative Principles, Data Trusts, and the Digital Economy" Research Sprint, our group conducted a legal and empirical investigation into data cooperatives in Europe (the "Project"). In particular, we draw attention to the possible impact, benefits, and limitations of two EU legislative proposals - the Data Governance Act (DGA) and the Digital Markets Act (DMA) - for the growing ecosystem of data co-operatives in Europe and potentially beyond.

To inform our work, we combine our learnings from the Research Sprint sessions, desk-based research, with findings from interviews with different data co-operatives to better understand the opportunities, challenges, and gaps between these organisations, governments, and policymakers in advancing our digital futures. Our paper is structured as follows. After an executive summary describing our goals, research scope, methodology, and main takeaways, in Part II we discuss data, identify the data co-operative landscape in Europe and illustrate the typologies of data co-operatives, focusing on the purpose and different models data co-operatives follow in Europe. In Part III, we then outline the legal developments relevant to the data co-operatives ecosystem and assess how these changes interact with co-operative and data organisation models. Finally, in Part IV, we summarize some of our takeaways and some future directions for policy and research, before concluding.

We hope our contribution can not only support data co-operatives navigate the legal constraints and access data-related opportunities, but also directly inform EU institutions that are currently deliberating over the DGA and DMA on how to build a sustainable and democratic digital economy.

I. Objectives and Takeaways

A. Project Goals

Our Project has three main objectives:

- Mapping the ecosystem of data cooperatives and small data governance realities in Europe.
- Understanding how EU law impacts on these realities and what changes might be needed to ease the work and development of their business models, e.g. how the General Data Protection Regulation (GDPR), Digital Markets Act (DMA), Digital Governance Act (DGA) and other initiatives are affecting or might affect data cooperatives going forward.
- Mapping these organisations' concerns and needs regarding law at EU and local levels, e.g. lack of legal and policy resources, absence of voice at EU level, absence of power to influence on EU legislation.

B. Project Audience

Our Project is primarily aimed at an EU policy audience as well as at an audience of cooperatives and cooperative members interested in understanding the data governance landscape and in promoting new synergies and possibilities in this space.

C. Project Methodology

In order to achieve the above explained goals, we first identified the main data cooperatives and actors working in this field across Europe. The cooperatives we identified included those that participated in the research sprint, cooperatives that are registered under the European Societas Cooperativa Europaea (SCE) cooperative legal form or cooperatives that describe themselves as data cooperatives more generally. Data cooperatives are structures that enable the creation of open data and personal data stores for mutual benefit, rebalancing what many may perceive as asymmetric relationship between data subjects and data processing entities.¹ Where possible, we attempted to identify the person that was directly involved with data management or navigating the law and policy implications within their data cooperative. This was done by discovering which persons were presenting on these topics based on our desk research. They were then contacted directly by email and/or social media. Francesc Lopez Segui (Salus Coop), Christian Buggedei and Laird Brown (Polypoly), and Ben W. (d.Org) agreed to be interviewed over a video call at a mutually convenient time. All participants named consented to having the interview recorded. We also communicated with organisations such as SAOS and Driver's Coop for general comments regarding our

¹ Please refer to, e.g., the General Data Protection Regulation for definitions of terms related to data protection, https://edps.europa.eu/data-protection/data-protection/glossary_en.

work but did not conduct interviews with them. The interviews lasted between 45 minutes to 60 minutes between October and December 2021. While the interviews were semi-structured, each interview addressed issues including:

1. Organisation's structure and purpose
 - a. How does the organisation work and what is the organisation's structure? In case of counting with more than one entity, how do they relate to each other?
 - b. What is the organisation's purpose?
 - c. At what scale does the cooperative operate, what are the challenges to setting up, and what are the future plans for the cooperative (process of scaling to other countries)?
2. Legal issues
 - a. What knowledge does the interviewee or the cooperative have of the GDPR, DGA, and DMA?
 - b. How do these and other EU laws affect the organisation?
 - c. Would any changes to these laws be welcome from the cooperative's perspective?
3. Relations between cooperatives and public institutions
 - a. Does the organisation work closely with public institutions or does it view them with skepticism?
 - b. What is the attitude of public institutions towards data cooperatives and the work that they are doing?
 - c. Could the relationship be described as successful?

After conducting the interviews, we wrote summaries and verbatim quotes. We also corresponded with interviewees regarding some follow-up questions and clarifications. In combination with the Research Sprint session and our knowledge in this area, these interviews provided an additional source of empirical research that helped us better understand any data-related and legal considerations regarding the data cooperative landscape.

D. Main Takeaways from Interviews

- The data cooperative space in Europe is rich, dynamic and diverse. It is a space the flourishing of which should be prioritized by digital and non-digital policy-makers in Europe and European Member States.
- Data cooperatives have a keen interest in collaborating with public institutions and should be understood in continuity with public purpose data governance activities carried out by public institutions.
- Data cooperative models tend to be under-resourced from a legal and/or policy perspective and would benefit from help and coordination as regards legal and EU policy matters.
- Some data cooperative models tend to rely on blockchain or multi-party computation so as to shield themselves from complex legal responsibilities.

- In keeping with the developments we've observed in practice, including the willingness of data cooperatives to work with the public sector, as well as the shortcomings we've identified in the DGA, we suggest that the cooperative movement be involved in consultative and expert bodies such as the proposed European Data Innovation Board.
- There is a lack of initiatives in Europe that foster collaborative group management of pools of data, which may be because of data protection limitations and costly compliance for small cooperative entities.

II. Context: Data and Cooperatives in Europe

A. What is Data?

The importance of data in the digital economy cannot be ignored. The mass collection of data, its storage, processing and use is a key pillar of platform companies' businesses and the way they make a profit.² As noted by Jathan Sadowski, data in the digital economy is used not only to profile and target people with content and ads, but also to optimize systems; manage, control and discipline processes; model probabilities; build new products and grow the value of existing assets.³ Platform companies like Google/Alphabet or Facebook/Meta make most of their profits from advertising, understood as the monetization of user data and user engagement. In 2020, about 97% of Facebook's global revenues were based on advertising,⁴ and about 80% of Alphabet's global revenues were based on advertising.⁵

Data is often referred to as a raw material (oil), a commodity (labor), an object (bits, bytes, property) or an extension of the self (something that embodies aspects of the personality). Yet none of these characterizations is fully accurate or sufficient to capture what data is and does in the digital economy.

The law primarily construes data as a modular unit of information. In Europe, law tends to construe data as a personal matter, to focus on units of information about persons and to disregard other types of information not traceable to persons as less important. Under the GDPR, "personal data" is defined as:

*Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (emphasis added)*⁶.

To put it concretely in the context of data cooperatives, an address associated with a membership number can be deemed personal data even when the member is not identified by name.⁷

The proposed EU DGA offers a more general definition, seeing data as "any digital representation of acts, facts or information and any compilation of such acts, facts or

² See, in particular, Jathan Sadowski, *When data is capital: Datafication, accumulation, extraction*, BIG DATA AND SOCIETY 5-6 (January-June 2019); SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* (2019); JULIE E. COHEN, *BETWEEN TRUTH AND POWER* (2019).

³ Sadowski, *supra*.

⁴ Facebook, Inc., Form 10-K (January 2021), <https://investor.fb.com/financials/default.aspx>.

⁵ Alphabet Inc., Form 10-K (February 2021), <https://abc.xyz/investor/>.

⁶ Gen. Data Protection Reg. 2016/679 of Apr. 27, 2016, Article 4(1).

⁷ Anthony Collins Solicitors, *GDPR Guidance for Co-operatives - Data Protection and the GDPR: what do you need to know?* Co-operatives UK, Manchester, 2018, p. 3, available online at: <https://www.uk.coop/sites/default/files/2020-10/gdpr-for-co-ops-resource.pdf>.

information, including in the form of sound, visual or audiovisual recording.”⁸ The same draft legislation defines metadata as “data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation, duration of activity, connections to other natural or legal persons established by the person who uses the service”.⁹ As discussed below, the DGA’s guarantees and provisions are all subject to the GDPR and to the EU fundamental and individual right to the protection of personal data. This means that any reuse of data for prosocial ends and any collaborative data governance schemes remain subject to data protection restrictions and individual guarantees.

Overall, therefore, the law in Europe focuses on and heavily regulates personal data. Regulators, academics, activists consequently tend to view data primarily as a “personal” matter with harmful consequences for the self. In reality, however, data is a much more complex social phenomenon with more systemic and collective effects. Digital platform economies perpetuate logics of accumulation where data becomes a form of capital.¹⁰ Regulating and envisioning data as primarily a personal matter with effects on the self necessarily leaves behind significant aspects of what data is, what it does in the existing digital platform ecosystem and what it could do in a different more collaborative digital environment.¹¹

Collaborative bottom-up data governance and cooperatives present themselves as opportunities to move beyond the existing neoliberal and individualistic focus on personal data, and to embrace more collaborative approaches to the production, use, monetization of and access to data. The cooperative movement indeed seems to cater to the needs of this new data-intensive economy. It offers a history, a philosophy and some practical tools for moving beyond a focus on individuals and toward a collective approach that is centered on groups and cooperation.

Yet, in practice, the direction data cooperativism is taking in this space, one confirmed by our interviews, remains in line with a neoliberal focus on personal data and the individual imperative for each person to govern ‘their’ data. The problems with existing data cooperativism attempts in Europe are thus at least two-fold.

First, EU law’s fixation on personal data, grounded in neoliberal assumptions about the primacy of individual liberty and choice in (digital) markets, makes alternative bottom-up management schemes including cooperative modalities of data management difficult to implement. Any attempt at managing data as a common resource often entails the processing of some personal data. This makes attempts at governing data collaboratively unduly costly and burdensome. As a result, the question of how to manage data more collaboratively in this context often appears intractable.

Second, cooperatives and small data governance realities in Europe tend to remain stuck in neoliberal paradigms of governance based on individual self-rule and choice. Most data

⁸ Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act) COM/2020/767 final, Article 2(1), available online at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020PC0767>.

⁹ *Id. supra*, Article 2(4).

¹⁰ Sadowski, above.

¹¹ See Salome Viljoen, *A Relational Theory of Data Governance*, 131 Yale Law Journal 573 (2021).

cooperatives, as discussed further below, defer the management of technology to technical solutions that allow individuals and only them to access what might be personal data. This makes managing data as a collective pool or commons the exception rather than the rule even in the cooperative space.

B. Data Co-operatives: Landscape and Typologies

Faced with the impossibility to govern and decide on the use and privacy of user data, data cooperatives have arisen as a tool to explore new data stewardship mechanisms. These enterprises aim to allow their members to have more control over their individual data and to use this data in the interest of their community or the commons.

During the Research Sprint, we identified two axes that helped us understand the existing landscape or typologies of data cooperatives in Europe. One of these axes is based on the motivation or purpose given to the data. In this sense, we identified and interviewed data cooperatives focused on the field of health (MIDATA, Salus), personal data (polypoly), transport in the gig economy (Drivers' Seat) and agriculture (SAOS). The second axis focuses on how data is gathered and used. In this sense, we identified some data cooperatives that do not want to access their members' data (Salus, polypoly) and others that work directly with this data (Drivers' Seat, SAOS). There are different reasons behind this, including legal issues, ideological conceptions of data, viability of business models, and data economy concerns at the time.

Below, we will briefly explain the interviewed data cooperatives, the field in which they work and the way they handle the data.

Salus is a data cooperative based in Catalonia that aims to facilitate secure sharing of health data enabling citizens to control their health records while incentivizing data sharing to accelerate health research innovation. Another data cooperative working with health data is MIDATA. This cooperative is based in Switzerland and works similarly to Salus, actively contributing to medical research and clinical studies by granting their members a selective access to their personal data.

Polypoly is a European cooperative that has developed a platform and technical infrastructure for a decentralised dataconomy. The personal data of the members of this cooperative is also saved in the users' devices.

Drivers' Seat is a cooperative owned by rideshare and delivery drivers. Their platform runs on shared data, freely contributed by thousands of gig drivers. They collect data from their app and website in order to sell it to cities and transportation agencies and at the same time help the members maximize their income.

We also spoke to SAOS, a data cooperative from Scotland working in the field of agriculture that pulls the data of the members in order to create a database that provides real-time tracing data of farm livestock through their supply chains, until the point when they enter the food chain.

C. Ideologies of the cooperative movement, goals and challenges

Each data cooperative exhibits a different perspective on how personal data should be handled. While some of them want their members to have total and individual control over their personal data, others generate a pool of members' data and use it for different purposes. Besides, there is also a debate about data commons, an open and collaborative approach that takes data as part of a "global commons" and makes access to it available to a range of independent stakeholders that use this data to generate a positive social impact.

These choices about pooling data ('the collective approach') or giving members greater control over their data on their individual devices ('the individualistic approach') are,¹² in part, shaped by how these cooperatives respond to market pressures. Even regulatory developments can be characterised as individualistic political (GDPR and DSA) or economic (DMA) as well as collective (DGA) forms of data sovereignty. However, despite the intention for these legal frameworks to rebalance power through regulation, they do not challenge the economic unfairness of data capitalism. Aggregate data in particular is an intangible social relational resource that is not only a mere sum of individual data footprints. If the encouragement to pool data is not supported by cooperative infrastructures that reflect this social relation, the requirement for creating data cooperatives is simply to continue mandating large companies to pool data without due consideration of the value of collective and aggregated data.

Ultimately, cooperatives have to maintain a viable enterprise, while continuing to serve its members. Some cooperatives seek to insulate themselves from the market by adopting a non-profit status: this allows the entity to enjoy certain forms of tax relief (depending on jurisdiction) and makes them eligible for grants, government funding, etc. However, this form of financing is likely to be, on its own, insufficient for the substantial costs involved in software development and marketing. Other cooperatives operate as commercial entities, which opens up possibilities for receiving financing from a greater array of market actors. This can include external investors being included as a distinct member category within the cooperative holding a distinct class of shares, as well as issuing cooperatives bonds, participation titles and non-voting certificates. There are also several instances in which agricultural cooperatives have 'gone public', by either forming a subsidiary that lists on a stock exchange or even listing its own (often preferred) shares on a stock exchange.¹³ For some, these "entrepreneurial cooperatives"¹⁴ continue to serve the purpose of redressing a

¹² Anita Gurumurthy, "Data Sovereignty: A View from the South", Presentation for the Research Sprint on Alternative Data Futures: Cooperative Principles, Data Trusts, and the Digital Economy, Berkman Klein Center and Platform Cooperativism Consortium, 24 October 2021.

¹³ Jos Bijman and Onno van Bekkum, "Cooperatives going public: motives, ownership, and performance", Paper presented at the International Conference on Economics and Management of Networks, EMNet 2005 – Budapest, 15 – 17 September, 2005, available online at: <https://cemi.com.au/sites/all/publications/Bijman-Bekkum-2005.pdf>.

¹⁴ Jerker Nilsson, "Cooperative Organisational Models as Reflections of the Business Environment", *Finnish Journal of Business Economics*, Vol. 48, No. 4, 1999, pp. 449-470, p. 451. Nilsson identifies four types of entrepreneurial cooperatives, all of which involve external non-member participation: (1) participation shares cooperative, (2) cooperative with a subsidiary, (3) proportional tradable shares cooperative, and (4) PLC cooperatives. *ibid*, p. 453.

poorly functioning market, while for others this drift from the traditional cooperative model by diluting members' ownership and control poses the risk of demutualization. Demutualization refers to the degenerative process by which a cooperative loses its democratic character and mutual purpose. While there is a rich vein of literature on this topic,¹⁵ for our purposes it suffices to say that they contribute to the erosion of the cooperative difference from corporate counterparts.

The fact that non-profit, entrepreneurial and other hybrid economic motives can co-exist speaks more broadly to the political ambivalence of cooperatives—including platform cooperatives.¹⁶ Scholars like Jossa have argued that labor-managed firms that are debt-financed, including a subset of worker and producer cooperatives, are in harmony with Marxist thought and can be vehicles for a transition to a socialist system as they involve a subversion of the typical capital relation by having labor hiring capital.¹⁷ On the other hand, there has been criticism that cooperatives, including platform cooperatives, are unable to extricate themselves from the logic of capitalist markets.¹⁸ An important limb of this argument is that a formalistic equality of votes—one member, one vote—is insufficient to foster cooperation. Ratner, for instance, contends that the conditions for solidarity and true cooperation are only created if the need to calculate exchange value is abolished in favor of a system of production and distribution that is based on need.¹⁹

It is unlikely that platform and data cooperatives, including those discussed in this paper, meet the exacting ideological standards set by these thinkers. Other than d.Org, the cooperatives we interviewed are not labor-managed. And even if a wider spectrum of cooperative types are countenanced as being part of an anti-/post-capitalist economy, most of these data cooperatives do not seek the elimination of exchange value. Personal data, including sensitive personal data, is very much seen as a commodity, and just as much as it merits protection and secrecy—in the interest of individual sovereignty—it is also seen as having exchange value that is worth monetizing. That said, members of some of the coops we interviewed seemed more interested in donating data to research than in benefiting from it economically, pointing to a hopeful altruistic ethos at the basis of many data cooperatives. Unlike their corporate competitors, any value and benefits derived from data as part of a data cooperative can be shared more widely.

¹⁵ See, for e.g., Ignacio Bretos, Anjel Errasti and Carmen Marcuello, “Is there life after degeneration? The organizational life cycle of cooperatives under a ‘grow-or-die’ dichotomy”, *Annals of Public and Cooperative Economics*, Vol. 91, No. 3, 2020, pp. 435-458; Chris Cornforth, “Patterns of Cooperative Management: Beyond the Degeneration Thesis”, *Economic and Industrial Democracy*, Vol. 16, No. 4, 1995, pp. 487-523.

¹⁶ Marisol Sandoval, “Entrepreneurial Activism? Platform Cooperativism Between Subversion and Co-optation”, *Critical Sociology*, Vol. 46, No. 6, 2020, pp. 801-817, p. 810; Carl Ratner, “Neoliberal Co-optation of Leading Co-op Organizations, and a Socialist Counter-Politics of Cooperation”, *Monthly Review*, Vol. 66, No. 9, 2015, available online: <https://monthlyreview.org/2015/02/01/neoliberal-co-optation-of-leading-co-op-organizations-and-a-socialist-counter-politics-of-cooperation/>.

¹⁷ Bruno Jossa, *Labour Managed Firms and Post-Capitalism*, Routledge, London and New York, 2017, pp. 45, 98; Bruno Jossa, “Marx, Marxism and the cooperative movement”, *Cambridge Journal of Economics*, Vol. 29, No. 1, 2005, pp. 3-18, p. 15.

¹⁸ Ratner, above; Sandoval, above, p. 808.

¹⁹ Carl Ratner, *Cooperation, Community, and Co-ops in a Global Era*, Springer, New York 2013, pp. 194-196; Ratner, above.

III. Data Governance: Law and Policy

A. Existing legal framework for (data) cooperatives

Privacy and personal data protection are both fundamental rights in the EU.²⁰ European data protection is based on the foundational principle that any processing of personal data, a term widely construed, is unlawful unless it can be justified in line with principles of fair and lawful processing: principles of lawfulness, fairness and transparency, the principle of purpose limitation, the principles of adequacy, relevance and data minimization, the fact that data must be accurate and kept up to date, that it must be retained for no longer than is necessary and securely stored.

In this section, we will discuss two legislative texts that are important for business organizations handling personal data, the GDPR and the ePrivacy Directive²¹. This EU legislation on data protection and privacy is relevant for a broad spectrum of data cooperatives. Firstly, this legislation is applicable to cooperatives that are registered within the European Economic Area (EEA), which includes the 27 EU Member States as well as Norway, Iceland and Liechtenstein. Secondly, while the United Kingdom has left the EU, the GDPR and the ePrivacy Directive has been transposed into domestic legislation prior to the UK's exit (e.g., the so-called UK GDPR). However, as EU legislation such as the ePrivacy Directive is in the process of being replaced, and the UK begins to adopt its own domestic laws on data protection, gaps and differences will begin to appear between the EU's legal framework and the UK's autochthonous regime.

Thirdly, both the GDPR and the ePrivacy Directive have extraterritorial effect, which means that under certain conditions these laws may be applicable to entities that do not have an establishment in the EU (e.g., in the United States or India). In the case of the GDPR, the regulation applies to data processors and controllers that do not have establishments in the EU if the processing concerns individuals ('data subjects') in the EU and is targeted at them for the purpose of selling goods or services, or for monitoring their behavior within the EU (usually for a specific purpose).²² Article 3(1) of the GDPR further provides that the Regulation "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (emphasis added). As the *Google Spain*²³ decision revealed, the Court of Justice of the European Union (CJEU) takes a capacious

²⁰ Charter of Fundamental Rights of the European Union, OJ C 326/391, 26/10/2012, arts. 7-8.

²¹ Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31/07/2002 [ePrivacy Directive]. It should be noted that the ePrivacy Directive concerns more than just personal data, as it also applies to e.g., traffic data.

²² GDPR, art 3(2). Orla Lynskey, "The Extraterritorial Impact of Data Protection Law through an EU Law Lens", in Federico Fabbrini, Edoardo Celeste and John Quinn (eds.) *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, Oxford, 2020, pp. 191-210, p. 194..

²³ C-131/12, *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD)* ECLI:EU:C:2014:317.

view in interpreting whether processing takes place within the context of a business's activities: even when Google did not have an establishment processing data within the EU, the fact that its establishment sold advertisements which subsidised this extraterritorial processing was a sufficiently inextricable link to fall within the regulation.²⁴ In turn, while not addressing extra-territoriality at length, the ePrivacy Directive implicitly applies to businesses that are established outside of the EU, but installs 'cookies' on the devices of EU-based users as part of providing "publicly available electronic communications services in public communications networks in the Community".²⁵ This includes traditional telecommunications companies, webmail providers, and internet service providers, but is not limited to them. Services that wholly or primarily involve the conveyance of signals, as opposed to content, can fall within the directive.²⁶ Moreover, as explained by the Article 29 Data Protection Working Party in opinions on search engines and online behavioral advertising, certain provisions of the ePrivacy Directive (e.g., article 5(3) on obtaining informed consent) are applicable beyond publicly available electronic communications services to other services that also use tracking cookies.²⁷ The ePrivacy Directive and the GDPR are intended to complement each other, with the latter not applying to electronic communications service providers if there are specific rules provided in the former.

As such, data cooperatives—as well as, platform cooperatives and cooperatives that collect and process personal data more broadly—have strong reasons for both appreciating existing EU legislation, as well as keeping abreast of new proposals.

It is evident that both primary cooperatives and representative organizations of the cooperative movement have endeavored to comply with the requirements of the existing legal framework. The following two subsections provide a brief overview of the content of the ePrivacy Directive and the GDPR. They also consider the implications that these two important legislative texts have for (data) cooperatives. We focus on these two due to their more general applicability, as compared to more sector-specific directives and regulations which may also be relevant for certain data cooperatives, such as the Directive on the Application of Patients' Rights in Cross-Border Healthcare.²⁸

GDPR

The [General Data Protection Regulation](#) (GDPR) came into force in May 2018, repealing the previous data protection regime and reconfiguring privacy protection in Europe and

²⁴ *ibid*, paras 55-56. See Lynskey above for more on this.

²⁵ ePrivacy Directive, art 3(1). See Giuseppe B. Abbamonte, "The Protection of Computer Privacy under EU Law", *Columbia Journal of European Law*, Vol. 21, No. 1, 2014, pp. 71-87, p. 86; Frederic Debusseré, "The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?", *International Journal of Law and Information Technology*, Vol. 13, No. 1, 2005, pp. 70-97, p. 86.

²⁶ Jos Dumortier, "Evaluation and Review of the ePrivacy Directive," *European Data Protection Law Review*, Vol. 2, No. 2, 2016, pp. 247-252, p. 248.

²⁷ Article 29 Working Party, "Opinion 2/2010 on online behavioural advertising", 2010, p. 9; Article 29 Working Party, "Opinion 1/2008 on data protection issues related to search engines", 2008.

²⁸ Directive 2011/24/EU of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88/45, 04/04/2011. Recital 25, for instance, clarifies that the individual right to access personal data concerning their health, such as medical records, examination results, assessments, etc. are also applicable in the context of cross-border healthcare provision. This is potentially relevant to healthcare data cooperatives that match patients in one Member State to medical institutions in another.

worldwide because of its extraterritorial scope of application. It reinforced the requirements for informed consent as one of the bases, and not the only basis, for legitimate data processing by any entity (corporations, public bodies, cooperatives), and introduced new inalienable data subject rights that cannot be waived: expanded rights to access information about the personal data being processed, rights to rectify and erase personal data, the right to data portability, the right to have human intervention in AI-based decision-making. There is at present no provision allowing data subjects to delegate their rights to self-manage data, other than Articles 77-80 which provide possibilities for data subjects to delegate their rights to lodge complaints and request remedies against data protection authorities, controllers and processors. Some of the cooperatives we spoke to, e.g. Salus coop, rely on data subject access as a basis for their model. The GDPR also introduced new compliance mechanisms: internal codes of conduct for companies; data protection impact assessments (DPIAs) whereby companies are encouraged to describe and evaluate aspects of their data processing practices likely to result in high risk; data protection seals and certifications overseen by apposite certification bodies; and perhaps most importantly data protection by design and by default which for example require setting up appropriate data minimization standards. The Regulation further puts in place a network of regulatory bodies across the EU, requiring each EU Member State to have a National Data Protection Authority (NDA). Each organization that processes data has breach reporting obligations and must appoint a data protection officer under the Regulation.

There can be legitimate bases for which a cooperative processes non-sensitive personal data of a member. This can be to collect information (including personal data) that is mandatorily required by cooperative law for the maintenance of membership registers,²⁹ to process a contract with a member,³⁰ to pursue the legitimate interests of the cooperative,³¹ and if “freely given, specific, informed and unambiguous”³² consent is given to the processing by the member.³³ Legitimate interest can be a vague term, but there is some guidance on what purposes are likely to be construed as being legitimate and what would not be: the processing of a members’ personal contact data for notifying them about an upcoming annual general meeting is legitimate, while using that same data for sending unsolicited marketing emails from the cooperative is not.³⁴ Relatedly, members must be given a meaningful opt-in choice to how their data is processed (e.g., for coop marketing) and should easily and freely be able to withdraw their consent. It is also essential that the request for consent is unambiguously phrased and identifies specific purposes, otherwise the member will not be truly informed about why their data is being processed.

Several data cooperatives are involved in the healthcare sector, so it is pertinent that the GDPR’s default rule is to prohibit the processing of health, genetic and biometric data that is used to identify an individual.³⁵ However, the GDPR itself provides several exceptions to this. It is possible to give explicit consent to processing of this data for specifically articulated purposes.³⁶ A foundation, association or other not-for-profit body with a political,

²⁹ GDPR, art 6(1)(c).

³⁰ GDPR, art 6(1)(b).

³¹ GDPR, art 6(1)(f).

³² GDPR, art 4(11).

³³ GDPR, arts 6(1)(a), 7.

³⁴ Anthony Collins Solicitors, above, p. 4.

³⁵ GDPR, art 9(1).

³⁶ GDPR, art 9(2)(a).

philosophical, religious or trade union aim can also carry out processing if there is a legitimate aim to the processing and appropriate safeguards in place, so long as the processing concerns members, former members, or those persons who have contact with the entity in connection with its purposes. This personal data cannot be shared with third parties without these members or persons' consent.³⁷

The inalienable rights enjoyed by data subjects also translates into the cooperative context. For instance, as a data subject, a former member of a cooperative can request access to information about how long their membership data (or health data, as the case may be) is held before it is destroyed. Both members and non-members who are data subjects can also request information on who the recipients of their personal data are.³⁸

In view of the rights and protections enjoyed by data subjects under the GDPR, as well as the requirements created under this legislation, all cooperatives are required to have an internal data protection policy, which informs the management of the cooperative on how to collect data in compliance with the GDPR, as well as privacy notices and website privacy policies that explains the reasons and basis for collecting personal data to data subjects.³⁹ The website privacy policy should also address how cookies are used, as cookies can be used to create profiles of data subjects and identify them, thereby bringing many types of cookies within the purview of the GDPR. The exception to this is if the ePrivacy Directive is applicable to the service providing cooperative, in which case the latter more specialised directive will apply.

ePrivacy Directive

The [ePrivacy Directive](#) was adopted on 12 July 2002, repealing an earlier directive concerning the processing of personal data and the protection of privacy in the telecom sector. A Directive requires Member States to transpose its provisions into national law. As a consequence, there is a possibility that the directive is not transposed in an identical manner or, indeed, not enacted within the set time frame.⁴⁰

As mentioned above, with certain important exceptions, this directive applies to publicly available electronic communications services in public communications networks in the Community. The directive provides for the confidentiality of communications and prohibits surveillance of communication and relevant network traffic data. When using cookies, which requires the storing of information on a user's device and accessing this information, the express informed consent of the user is required. 'Traffic' data, which is data that is collected "for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof",⁴¹ must be deleted or anonymized when the data is no longer needed for the transmission.⁴² With the users (withdrawable) consent, this traffic data

³⁷ GDPR, art 9(2)(d).

³⁸ GDPR, art. 13(1)-(2).

³⁹ Anthony Collins Solicitors, above, pp. 6-7.

⁴⁰ Dumortier, above, p. 248; Debusseré, above, p. 73 (nine EU Member States failed to transpose the ePrivacy Directive by the deadline of 31.10.2003).

⁴¹ ePrivacy Directive, art 2(b).

⁴² ePrivacy Directive, art 6(1).

can be processed for the purpose of marketing electronic communication services.⁴³ Outside of traffic data, only limited types of location data can be processed, namely location data that is offered through public communications networks or publicly available electronic communications services.⁴⁴ In other words, location data gathered by information society services such as social media applications through, for instance, wifi network proximity, would not fall within the directive.⁴⁵ The directive also prohibits automated communication systems, such as email, to be used for direct marketing without obtaining prior consent of users.⁴⁶ In other words, for cooperatives, this means that members have to clearly and affirmatively opt-in to direct marketing by the cooperative by email (or SMS) and cannot be automatically enrolled.

B. Legal proposals that are of relevance for data cooperatives

DGA

The [Data Governance Act](#) (DGA) was proposed on 25 November 2020, with the intention of promoting the exercise of data rights in the EU, including by enabling greater access and use of data for novel commercial and altruistic ends. As part of a new European strategy for data that aims to create a single market for data,⁴⁷ the proposal presents a “Union-wide governance framework for data access and use”.⁴⁸ It has far-reaching ambitions in terms of data use, re-use and sharing that cuts across the public, private and third sectors. On the premise that there is a large volume of underutilized public sector data, which should be made available for the benefit of society as they are generated through the expenditure of public budgets,⁴⁹ the DGA sets out the conditions under which certain categories of this data can be reused and mandates the creation of a ‘single information point’ to access this data.⁵⁰ These conditions potentially include the anonymization/pseudonymization of the data, access and re-use being limited to secure processing environments, setting conditions on the technical integrity of these environments—all with the technical support of ‘competent bodies’ to assist in granting access for data re-use.⁵¹ Requirements are also placed on transmitting public sector data to third countries, including a requirement for the third country

⁴³ ePrivacy Directive, art 6(3).

⁴⁴ ePrivacy Directive, art 9(1).

⁴⁵ Dumortier, above, pp. 250-251.

⁴⁶ ePrivacy Directive, art 13(1).

⁴⁷ European Commission, A European strategy for data, COM(2020) 66 final, Brussels, 19.2.2020, p. 4.

⁴⁸ DGA, recital 4.

⁴⁹ DGA, recital 5.

⁵⁰ DGA, art 8(1), recital 21.

⁵¹ DGA, arts 5(3)-(5), 7, recital 11. Please note that these measures are not universally seen as being adequate, especially from the perspective of protecting personal data. The European Data Protection Board (EPDB) and European Data Protection Supervisor (EPDS), for instance, opined that: “given the rapid developments in re-identification techniques and the availability of advanced computational resources, the legislator should take into account that anonymisation, pseudonymisation, and even the use of secure environments cannot be considered in all cases as free from vulnerabilities”. European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, version 1.1, 10 March 2021, para 89.

re-user to submit to the jurisdiction of the Member State where the public sector body is domiciled.⁵²

Turning to the private sector, the DGA envisions data sharing services being provided by intermediaries to both aggregate data pools and exchange data bilaterally.⁵³ This would involve both personal and non-personal data. Intermediation is clearly the operative word here, as the proposal only applies to providers who are ‘neutral’ and whose main business objective is to legally (and potentially technically) connect data holders and data users, as well as assist in their transaction of data assets.⁵⁴ It deliberately excludes a wide variety of other service providers, including cloud services, content intermediaries, data brokers and businesses that develop products by adding value to data. Instead, three types of data sharing services are mentioned: (1) intermediaries that facilitate B2B data-sharing, to enable bilateral data exchanges or pooling to allow joint exploitation of data; (2) intermediaries that facilitate C2B data-sharing, by making technical means available for businesses to access individual data subjects’ data, and (3) data cooperatives that facilitate data subjects or MSMEs better realizing their rights, specifically by negotiating terms with data users prior to giving consent to use, helping them make informed consent decisions and fostering dialogue between them on data processing purposes and conditions.⁵⁵ Those organizations wishing to provide data sharing services, which includes data cooperatives, are required to provide notice to a designated authority in the Member State where it has its main establishment (or where the legal representative of a non-EU/EEA organization has their establishment).⁵⁶ Only if the data sharing service submits notice and meets a host of conditions, such as limiting the use of collected metadata, maintaining adequate high level of security, and acting in data subjects’ best interests when offering them services, can it provide these services across all Member States.⁵⁷ Significantly, the proposal clarifies that data sharing service providers will hold “fiduciary duties” to data subjects, if they are intermediating exchanges of data between data subjects and legal persons.⁵⁸

Thirdly, the DGA introduces the concept of ‘data altruism’, whereby personal and non-personal data is voluntarily donated for purposes of general interest. Such purposes can range from applied research on mobility to scientific research on combating climate change.⁵⁹ The proposal actively encourages the donation of such data for the purpose of creating data pools and enabling big data analytics. To this end, the proposal encourages the formation of legal entities that can collect and process personal and non-personal data, so as to make this data available for general interest purposes. Given the inherent risks involved in this endeavor, the DGA establishes a registration framework to register ‘Data Altruism Organisations recognised in the Union’. This process, first, involves meeting certain organizational prerequisites, namely possessing a not-for-profit status, having general interest objectives in its foundational documents, and being independent from for-profit entities and other activities of the organization.⁶⁰ In addition, the registered organisation will

⁵² DGA, recital 16.

⁵³ DGA, art 9(1), recital 22.

⁵⁴ DGA, recitals 22, 26

⁵⁵ DGA, art 9(1).

⁵⁶ DGA, art 10(2)-(3).

⁵⁷ DGA, art 10(4)-(5), art 11.

⁵⁸ DGA, recital 26.

⁵⁹ DGA, recital 35.

⁶⁰ DGA, article 16.

be required to maintain records (e.g., on the persons that process data held by the entity and the purposes), annually report on its activities to a designated competent national authority,⁶¹ and inform data holders about the purposes to which their data is being processed and whether data is leaving the EU. A registered data altruism organisation will be recognized in all Member States and will be able to facilitate cross-border data uses.⁶² To facilitate the collection of data in a uniform manner, the proposal also provides the European Commission the option to develop a European data altruism consent form, so as to enable data holders to give and withdraw consent.⁶³

Furthermore, the DGA provides two new remedies: (1) to lodge a complaint to a competent authority against a data sharing services provider or a data altruism organisation and (2) to pursue a judicial remedy against a competent authority for failure to either act on the aforementioned complaint or for certain decisions made by said authority.⁶⁴ Finally, an expert group known as the 'European Data Innovation Board' will be empanelled to support the European Commission in *inter alia* develop technical standards, consistent practice on applying the requirements placed on data sharing service providers and best practices for cross-sector data sharing and data use.⁶⁵

In sum, according to the drafters, on the one hand, the DGA seeks to help businesses build new products and services for a pan-European market, enable big data analytics for both commercial and altruistic ends, and encourage scientific research. On the other hand, they want to ensure the protection of personal data, and respect for existing confidentiality, intellectual property and competition laws,⁶⁶ so as to build trust in the organizations and processes involved in data re-use and sharing.

Of particular relevance to cooperatives and the cooperative movement at large is the fact that the DGA advances a specific, and arguably muddled, conception of what data cooperatives are. As mentioned above, data cooperatives are defined in the proposal by three possible functions, without providing a clear, general definition.⁶⁷ As a consequence, it risks simultaneously excluding several cooperatives that may be seen by themselves and others as being data cooperatives, as well as including activities that may not be the primary function of many cooperatives. For instance, cooperatives that seek to pool and process aggregated data would not fit within the three functions. Conversely, the task-based definition suggested by the proposal encompasses cooperatives that help user-members make informed choices prior to consenting to data use and negotiate terms and conditions with data users prior to individual consent being given. This is contradictory with other provisions of the DGA which underscore the fact that individual rights under the GDPR are inalienable and "cannot be conferred or delegated to a data cooperative".⁶⁸ While this might be seen as an example of the limits of the individualistic, consent model of the GDPR, it also raises wider questions about the actors that are appropriate for carrying out functions like negotiation with corporate data users. Recent decisions from a Dutch court reveal the

⁶¹ DGA, articles 18-20.

⁶² DGA, recital 36.

⁶³ DGA, article 22, recital 39.

⁶⁴ DGA, articles 24-25.

⁶⁵ DGA, articles 26, 27(a)-(b), recitals 40-41.

⁶⁶ DGA, recitals 9, 12-13.

⁶⁷ EPDB and EPDS, above, para 128.

⁶⁸ DGA, recital 24; EPDB and EPDS, above, para 131.

importance of trade unions, and allied nonprofits such as Worker Info Exchange, in making data access requests to corporate platforms (e.g., Uber) and investigating alleged instances of automated decision-making.⁶⁹ By saying that negotiating and dialogue-building activities fall within the purview of *for-profit* data cooperatives—the only type of data cooperative recognized by the DGA—it distracts from the efforts of other actors involved in these activities and contributes to its commercialization.⁷⁰ Finally, this conception of data cooperative also fails to acknowledge *non-profit* data cooperatives that exist, both in the EU (e.g., Salus) and beyond (e.g., MIDATA). While these might appear to be an issue of semantics at first blush, should the proposal be enacted as currently drafted, it raises questions about whether existing data cooperatives, like the ones studied in this paper, will be able to continue describing themselves as such.

Setting aside the definitional issues presented by the proposal, the DGA provides both commercial and philanthropic organizations—including cooperatives of various types—a framework with which to engage in data sharing services. In addition to the respective notification or registration procedures summarized above, it is important to note the narrow conception of data intermediary defined in the text. While data intermediaries can have business models that “seek to enhance individual agency”⁷¹ (e.g., polypoly), advise individuals on how their data is being used and make due diligence checks on data users (e.g., Salus), it could potentially preclude the activities of cooperatives like Drivers’ Seat which add value to aggregated driver data for the purpose of selling it.⁷² Moreover, even those cooperatives engaging in permissible activities must bear in mind data minimization principles and should not seek to extract more data out of commercial interest than would be desirable in the individual data subject’s interest. Bearing in mind competition law rules, the proposal discourages the creation of exclusive agreements for data re-use, except when it is just and necessary for the general interest. Recital 9 provides an example of this exception, referring to entities that have a unique technical proficiency (e.g., in processing datasets) that would enable a public sector body to furnish new digital services. Given the interest in supporting SMEs and non-profit organizations engaged in data altruism, this could open the door for platform and data cooperatives with specialized technical competencies to benefit from this exception.

As has been shown so far, admittedly briefly, data cooperatives are subject to a complex legal (and technical) framework, one that will grow even more demanding with the potential passage of the DGA. The fact that the DGA recognizes a fiduciary duty of organizations,

⁶⁹ Sebastian Klovig Skelton, Uber and Ola ordered to hand over more data to drivers, ComputerWeekly.Com, 16 March 2021, <https://www.computerweekly.com/news/252497940/Uber-and-Ola-ordered-to-hand-over-more-data-to-drivers>; Worker Info Exchange, <https://www.workerinfoexchange.org/> (accessed 3 December 2021).

⁷⁰ The EPDB and EPDS opine that the GDPR already obligates data controllers to be transparent about data processing purposes and requires them to ensure that data subjects make informed consent decisions. As such, these are obligations to be enforced, rather than new rights to be negotiated privately. See EPDB and EPDS, above, paras 129-130.

⁷¹ DGA, recital 23.

⁷² Drivers’ Seat Cooperative, FAQ: Do you sell driver data?, <https://driversseat.co/faq/1638526415953x453226396222561340> (accessed 3 December 2021). “Yes, we do! That’s exactly how our shared ownership model works. In order to provide free data insights and services to gig drivers, we need to pool and sell our shared gig data to customers that understand and support driver-first missions. Our data is valuable, especially when we combine it with thousands of other drivers. What matters to us is making sure drivers finally have a chance to benefit from it.”

including data cooperatives, to the best interest of data subjects when handling the data of these individuals, raises the stakes of legal and technical compliance. With the above considerations in mind, we are of the view that the cooperative movement should be represented in developing the technical standards and data sharing/(re)use policies to which they are subject. Given that the proposed European Data Innovation Board will have such a function, and is poised to have a multi-stakeholder composition with representatives from Member States, the European Commission, representatives from “relevant data spaces and specific sectors”,⁷³ room can also be made for cooperatives.

DMA

The [Digital Markets Act](#) (DMA; together with the Digital Services Act, or DSA) was proposed in December 2020 and promotes a more decentralized level playing field where small EU businesses can flourish alongside US incumbents. The Act is addressed to providers of core platform services and lays down rules to ensure “contestable and fair markets in the digital sector across the Union”. It prohibits practices that “limit contestability” or “are unfair,” for example the combination of a gatekeeper’s data with third party data, bundling of different services or discrimination amongst customers on incumbents’ marketplace. It also obliges big tech to allow users to uninstall pre-installed products, to allow switching, duty to apply fair and non-discriminatory conditions of access to certain data, etc. Many of these provisions, if enacted, will radically redefine digital competition in Europe and can enable new coop-based business models to flourish. For example, they allow cooperatives to claim access to data from dominant incumbents and to develop competing non-profit models on the basis of that data. An example is how a search service such as Ecosia can be built benefiting from Google’s well developed functionality and network effects and in turn constraining the potential of Google to abuse its dominance or impede competition on the online search market. A similar scenario can be envisaged in hospitality or taxi services, where benefiting from first mover advantage will become a less clear predictor of future success.

Other Proposals

There are also other legislative proposals that are part of the European Commission’s Work Plan that are relevant for data cooperatives, including a proposal for a regulation on the European Health Data Space. While upholding data protection rules, and acknowledging the especially sensitive nature of health data, this proposal seeks to encourage the use and sharing of health data for research purposes.⁷⁴ There is also discussion about replacing the ePrivacy Directive with an ePrivacy Regulation.

⁷³ DGA, recital 40, article 26.

⁷⁴ European Commission, Published Initiatives: Digital health data and services – the European health data space, available online at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Digital-health-data-and-services-the-European-health-data-space_en (accessed 1 December 2021).

IV. Discussion & Key Takeaways

A. Understanding data cooperatives

Building upon our empirical and legal research, here are five lines of inquiry that can enrich a discussion on next steps and how to move forward in this contested legal and experimental space.

Collection and storage of data

One of the key aspects of data governance and the relationship between data cooperatives and their members is if and how personal and non-personal data is collected, stored, or analysed. As noted from our interviews, while some cooperatives want their members to have total control over their data (e.g. polypoly), other data cooperatives created a data pool in which data is pseudonymised and aggregated. In some cases, data cooperatives actively choose not to collect and process personal data at all, with the explicit indication that members must manage their own data outside of the cooperative's bounds.

Industry

Another line of inquiry is the sector and industry in which the cooperative operates, and how that affects their treatment and vision of data governance. For example, a cooperative operating in the healthcare sector has different priorities and regulatory requirements to comply with than a cooperative operating in agriculture or a cooperative acting as a neutral umbrella storage mechanism for personal data. Further, these cooperatives might differ in the technologies they rely on. A data cooperative that is built on Web3 technologies is more likely to prioritise transparency over trust⁷⁵, because members are brought together with the belief that digital tools and platforms can be used to generate greater value. This leads to typologies of cooperatives that are radically different in scope and operation.

Purpose

A third key aspect to understanding how data is managed and governed within a data cooperative is identifying the purpose of the data cooperative. While some data cooperatives clearly state their objective and aims, others use the data cooperative structure as a means to achieve broader societal aims. For some cooperatives (such as Polypoly), the main objective is to establish better agency over data, while for others, the cooperative's aim is the creation of greater collective or social value within their remit (such as SAOS, Salus and PescaData). Understanding a data cooperative's purpose also helps the identification of stakeholder engagement as well as the roles different stakeholders could play, which may be particularly relevant when assigning duties and responsibilities in the context of data-related regulations.

⁷⁵ Primavera de Filippi, Morshed Mannan, Wessel Reijers. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, Elsevier, 2020, 62, pp.101284.10.1016/j.techsoc.2020.101284.hal-03098449

Monetization

Fourth, it is worth mentioning that some cooperatives and members (e.g. Salus) are interested in using data for a common good, even if in an individualized manner. For example they are interested in donating it for research. Other cooperatives, however, are organised so as to allow their members to individually monetize data.

Individual vs Collective

A final aspect to consider is that although cooperatives are organised as groups of members that come together to co-manage certain resources or business purposes, it is surprising to see that many cooperatives in Europe remain premised on an individual-centric approach to data. This may be due to EU legislation such as the GDPR and raises questions about whether the data, particularly pooled data, governed by data cooperatives maximises common socio-economic and community values.

B. Key Takeaways and Next Steps

Based on our interviews and contextualization of the European data cooperatives landscape, we have identified the following:

a) The data cooperative space in Europe is rich, dynamic and diverse. It is a space the flourishing of which should be prioritized by digital and non-digital policy-makers in Europe and European Member States.

The cooperative movement in Europe has a long history and offers incredibly rich resources and opportunities for moving beyond existing data and digital governance models and into approaches to data and technology that are more collaborative, bottom-up and empower citizens and consumers. The many existing models remain small-scale and timid, but we see scope for real flourishing and data governance renewal in this space.

b) Data cooperatives have a keen interest in collaborating with public institutions and should be understood in continuity with public purpose data governance activities carried out by public institutions.

There is an appetite from these cooperatives to work with public institutions to see how the data cooperative model can thrive within local communities across the continent. For example, Salus works closely with public institutions to generate value in the healthcare sector. In order to better develop cooperatives infrastructures in Europe, policy-makers should be more active in speaking to data cooperatives within and outside the EU to better understand how these models could be adapted to data governance alongside existing legislative developments. This is supported by our interactions with data cooperatives, where a braver approach from public institutions was requested by our interviewees as a way to help them grow faster and generate a bigger social impact.

c) Data cooperative models tend to be under-resourced from a legal and/or policy perspective and would benefit from help and coordination at EU level

During our interviews, we noted that data cooperatives and their members have little understanding of the regulatory environment beyond incorporation and registration as cooperatives. Due to lack of financial resources, many data cooperatives only seek legal advice as and when necessary, without much consideration of future legislative developments that could impact them and affect their long-term sustainability. This may be due to many factors. For example, some data cooperatives may not believe that their work is connected to and impacted by existing EU regulation while others may want to engage in the development of laws and policies but may not know how to do so. Additionally, the lack of understanding about the SCE legal form also complicates the generation of these types of cooperatives that would help them scale more easily. As a result, data cooperatives in general tend to be law-takers as opposed to law-makers when it comes to regulatory developments regarding data cooperatives models.

d) There is awareness of the need for cooperatives to deploy more environmentally friendly solutions than are currently in place.

Irrespective of how technologically-driven a data cooperative is, there is a general understanding of the current environmental context and risk of the climate emergency. For example, polypoly explained that the cooperative takes into consideration environmental concerns when dealing with data through their technology and use of processing power from decentralized devices. SAOS also actively considers the use of aggregate data to demonstrate farming's positive contribution to climate action through its cooperative structure. As a result, it is important that when discussing future developments for data cooperatives, policies should advocate for and promote solutions that, in addition to granting data sovereignty to citizens, are also achieved in a way that respects the environment.

e) Some data cooperative models tend to rely on blockchain or multi-party computation, creating a shield against complex legal issues and responsibilities through distributed technologies by focusing on implementing technical mechanisms for facilitating trust and transparency rather than introducing a more collective approach and avoiding the legal problems this would generate.

The development and deployment of Web3 decentralised technologies are common in the data cooperative space. This is due to broadly shared beliefs regarding the potential of these technologies to redistribute power away from centralized infrastructures and toward the people. However the risks of using these technologies are that they contribute to an excessively individual-centric approach to (personal) data management. The use of these technologies also delegates control over data to individuals thus shielding data cooperatives from responsibilities under data protection and other laws.

d) There is a lack of initiatives in Europe that focus on co-managed collective pools of data, which may be a result of the stringent requirements of EU data protection law

In spite of our Research Sprint goal of fostering collaborative management of data, the data cooperative movement has not grown as significantly as we would have hoped in Europe. Noting that European data cooperatives tend to be based in certain regions, we posit that the strict requirements regarding the protection, management, and sharing of personal data

under the GDPR may limit the development of data cooperatives on the continent. While other regions have cooperatives that pool data, such as PescaData (a platform cooperative that is owned by fishers, fishing groups, NGOs, and other stakeholders in the ocean conservation community, facilitating collaboration, that provides a digital infrastructure for small-scale fishers in Latin America, and the Caribbean) and Eva (a ride-sharing data cooperative based in Montréal), the EU is relatively lacking in cooperative infrastructures that have great public reach, such as those related to environmental or city data. Decode EU may be an exception, but we are so far unclear on the initiative's precise scope. As such, we found a paradoxical lack of collective data pools in the EU cooperative ecosystem.

f) In order to increase the socio-economic and relational value of collective data for public purposes, data cooperatives can serve as carve outs from data protection law

Sitting uneasily within the requirements imposed by the GDPR or the possibilities created by the DGA, data cooperatives remain a promising yet so far missed opportunity to create social value through data. Legal changes are needed to promote a bolder and more capacious data cooperative movement. It seems necessary, for example, to extend the DGA beyond its current scope and encourage the exploration of more ambitious, collaborative attempts to support data pools beyond the economic lenses of data altruism. It also seems necessary to envisage certain exceptions to the GDPR requirements regarding the processing of personal data for collective and public-interest purposes. In keeping with the developments we've observed in practice, including the willingness of data cooperatives to work with the public sector, as well as the shortcomings we've identified in the GDPR and DGA, we suggest that the cooperative movement be involved in consultative and expert bodies such as the proposed European Data Innovation Board in order to advance a more inclusive legal and policy agenda for European data governance.

V. Conclusions

Data cooperatives present an innovative and radical approach to data management and governance of collective data while preserving data subject agency over their personal data. Taking into account the current knowledge and relationship between data cooperatives and the legal frameworks such as the GDPR and DGA, coupled with the lack of participation of these cooperatives in formulating the proposed regulations, we suggest the need for greater collaboration between data cooperatives and legislators, policy-makers, and public institutions. In this sense, rather than having a passive attitude towards the new opportunities created by data cooperatives, these institutions could support their activity through the creation of a robust regulatory framework that supports the incorporation, development and sustainability of data cooperatives within the EU digital market. A potential to generate a big social value is perceived through the collaboration of different stakeholders around data cooperatives while achieving greater data sovereignty for citizens. Current data protection law and proposed regulations regarding data continue to promote more individualistic treatment of data. Given the benefits of collective data approaches, we suggest that policy-makers should consider ambitious attempts to pursue a more collective conception of data and of data cooperative models, recognising the socio-relational value for community-driven data. Greater appreciation of using collective data for public purposes can also be explored, extending the realm of possibilities for what and how pooled data can benefit a greater number of stakeholders within data cooperative models.