One Form to Rule Them All: Towards a Personalized, But Standardized, European Data Altruism Consent Form

Arianna Rossi

Abstract Data altruism is a novel concept established by the Data Governance Act that aims to increase the availability of data for purposes that meet the general interests of society. However, realizing this future relies on the data subjects giving their consent to use the data collected. As of this time, little is known about how a European data altruism consent form might allow a transparent, user-friendly, and lawful process for granting and withdrawing consent to the re-using one's personal information. This article therefore explores some of the most pressing legal, design, and technical challenges that need to be addressed to enable a trustworthy exchange of data and consent permissions. Given that decisions about whether one's data can be used mostly depend on personal and contextual factors, I argue for the implementation of dynamic consent with standardized, interoperable semantic specifications used as viable means to personalizing consent. This would be the most lawful and efficient way to support individual autonomy.

1 The Value of Data Sharing for Altruistic Purposes

In an era where data silos and data monopolies are deprecated due to the concentration of the knowledge and power they engender, the European Union is seeking to counter this tendency by encouraging its citizens to share their data in an effort to boost innovation, optimize public services, and improve public policies. The underlying reasoning is simple, yet powerful: if organizations, especially public organizations, are spending resources to gather data in the wake of digitalization, why shouldn't this data be made available and re-used to create actionable knowledge? Among the various legislative initiatives that seek to break down the barriers to data exchange, the concept of sharing data for purposes of general interest has received

A. Rossi (✉)
LIDER-Lab, DIRPOLIS, Sant'Anna School of Advanced Studies, Pisa, Italy
e-mail: Arianna.Rossi@santannapisa.it

F. Casarosa et al. (eds.), *Enabling and Safeguarding Personalized Medicine*,
Data Science, Machine Intelligence, and Law 7,
https://doi.org/10.1007/978-3-031-99709-9_4

renewed attention. To this end, the Data Governance Act (DGA)[1] has established the concept of data altruism, defined as "the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them … without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objective of general interest as provided for in national law, where applicable, such as healthcare, […] improving the provision of public services, public policy making or scientific research purposes in the general interest".[2] Note that, because this article only focuses on the consent to share personal data for altruistic purposes in the context of healthcare, I have omitted irrelevant parts of the definition. For example, I will not touch on the conditions for processing and reusing non-personal data because it is outside of the scope of this contribution, even though non-personal data may include personal data that has been anonymized.

In particular, healthcare and health research are domains where more data could have a great impact on societal welfare. Yet, in practice, progress is hampered by a multitude of different legal, technical, data management, and trust issues.[3] The Corona Data Donation project[4] typifies the groundbreaking potential of data altruism. This project, launched by researchers during the early phases of the COVID-19 outbreak, took the form of a mobile application which collected the data of over half a million German residents for 2.5 years through their wearable devices. The data captured included the users' resting heart rates, daily step counts, and sleep duration under normal conditions. These data were then used as a baseline for comparison against algorithmically identified systematic deviations. Thus, the researchers were able to infer indicators of the virus's onset, such drops in a subject's daily step count coupled with a simultaneous rise in their resting pulse. Interestingly, those data have since been used to compute the effectiveness of vaccinations over both the short and long terms.[5] Hence, from data that were scarce or even non-existent at the time, scientists were able to derive incredibly useful information, including real-time patterns of the pandemic's spread, evidence of the efficacy of self-administered tests, and, together with some survey data, newfound insights on the social factors that influence protective behavior.[6] Such information can be transformed into actionable knowledge, like advancing scientific research; producing, developing, and disseminating statistics; promoting evidence-based policymaking; and improving public healthcare services.

All of the laudable activities have been enabled by the voluntary sharing of sensor data and coincide with the "purposes of general interest" as mentioned in the

[1] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) PE/85/2021/REV/1, OJ L 152, 3.6.2022, pp. 1–44.

[2] DGA, Article 2(16).

[3] Abboud et al. (2022).

[4] Robert Koch Institute (2025).

[5] Wiedermann et al. (2023).

[6] Corona Datenspende (2025).

definition of data altruism under the DGA. This chapter narrows the scope of data altruism to the benefits that health-related datasets gathered via scientific research studies can bring to personalized medicine, which is more broadly understood as an approach that gears medical treatment to the individual characteristics of human beings.[7] To support the free flow of information, individuals should be able to knowingly determine the permissible reuse of their data for altruistic objectives, i.e., they should be able to give consent to their data's use, while the permissions granted by that consent should be promptly shared and unambiguously interpreted across organizations. Under the legislation, data altruism organizations act as data intermediaries that obviate legal and technical barriers, address the trust issues that hamper data sharing by organizations and individuals, and lower the transaction costs associated with such activities.[8]

Such organizations may in particular support autonomy: the people's ability to help determine the use of information about them represents a fundamental concept in the functioning of modern democratic societies. However, this autonomy is threatened by a rapidly unfolding digital transformation that has, to date, been characterized by uncertain outcomes and secretive goals of exploitation. Today, corporations and nations worldwide are competing for monopolistic data appropriation and far-from-inclusive achievements, while longstanding issues of data misuse by private and public organizations alike persist. The notion of control over one's own data has been chiefly impersonated by consent as a tool for self-determination, which the DGA compounds with a wide array of instruments that supposedly restrain existing imbalances of power. By fostering more horizontal relationships between data subjects, data holders, and data users, and by cultivating more opportunities and means to access and control information, the DGA contributes to more inclusive data governance.[9] Personalizing information and the ability to make choices that respond to idiosyncratic needs may also then support mindful decision-making in line with one's own values.

From the standpoint of promoting voluntary data exchange, the DGA stipulates that the European Commission should develop a European data altruism consent form to allow uniform consent management across its Member States. However, the Commission also needs to lay down the requirements for information transparency towards data subjects prior to their decision to offer consent and for tools for managing a subject's permissions for using their data in a rulebook.[10] Both the consent form and the rulebook should be drafted in consultation with relevant stakeholders.

Within this context, this chapter makes the following contributions to the literature:

[7] National Research Council (2011), p. 12.

[8] European Commission (2020).

[9] Micheli et al. (2023), p. 18.

[10] See Article 22 of the DGA.

1) It delineates the scenarios where research organizations and individuals may want to resort to health data altruism as a supplement to the legal obligations established by the European Health Data Space (EHDS) Regulation;[11]
2) It illustrates the complex interplay of consent requirements deriving from the General Data Protection Regulation (GDPR)[12] and the DGA concerning health data collected in research settings that has been shared for altruistic purposes;
3) It identifies and critically discusses some of the challenges that arise from the regulatory framework, as well as the existing hurdles to a user-friendly and lawful implementation of consent; and
4) It examines personalized dynamic consent and semantic web technologies as potential solutions to challenges related to usability, legality, and interoperability.

2 Research Scenario

2.1 The Rise of Data Intermediation and Data Altruism

Even though the benefits of data sharing are evident, many obstacles stand in the way of us realizing a thriving society based on free-flowing information. Barriers to data sharing across organizations include fears that data may be misused, limited technical and cultural know-how, and legal concerns including privacy breaches.[13] Such concerns are particularly understandable when the data include health information. This is why an ecosystem of data intermediaries has flourished, many of which promise to empower individuals and organizations to regain control over the use of their data and direct it towards goals they endorse, instead of hopelessly relinquishing such control to other parties.

One of the concerns of the DGA is to help organize and regulate the conditions under which data intermediaries provide digital services, i.e. the organizations that facilitate data flows between data holders and data users.[14] Currently, data intermediaries offer a broad range of functionalities that inspire the trust necessary for exchanging data. As Schweihoff et al.[15] reports, these functions include:

[11] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance) PE/76/2024/REV/1 OJ L, 2025/327, 5.3.2025.

[12] 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 L 119, 4.5.2016, pp. 1–88.

[13] Schweihoff et al. (2024), p. 3.

[14] Schweihoff et al. (2024), p. 4.

[15] Schweihoff et al. (2024).

1) enhancing or ensuring the confidentiality of data; offering a way to encrypt and/or anonymize data; and providing support for legal agreements;
2) enabling data control and regulating access management;
3) providing the necessary infrastructure for exchanging data and standards (like marketplaces, APIs, and connectors);
4) compiling data catalogs that store data securely and make them available;
5) facilitating data governance through security mechanisms and making data processing including data aggregation easier, as well as helping individuals to manage their own data, including via consent management tools;
6) enabling identity management;
7) supporting transactions by connecting actors in the data economy; and
8) establishing data sharing processes with a view to their compliance, customizations, data quality, and data usage policies.

Within the broad landscape of data intermediaries, the DGA envisages two categories of actors: data intermediation services (DISs) and data altruism organizations (DAOs). Data intermediation services are defined as services that aim "to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects/data holders and data users through technical, legal, or other means, including for the purpose of exercising the rights of data subjects in relation to personal data".[16] Even though the purposes of affording technical, legal or other enablers of data exchange are shared, DISs establish relationships of a commercial nature between data users and data holders, whereas DAOs act for non-for-profit reasons.[17] Although the DGA covers both personal and non-personal data reuse, my focus in this article is on personal information that might be processed conditional to the consents made available by data altruism organizations for altruistic reasons. Noably, DAOs may collect data directly from data subjects, but they can also reuse data collected by others for either their own purposes or those of third parties.[18] In this way, they can assume the role of either data controllers or data processors. With this in mind, one way to support data altruism is to offer the means to easily manage consent permissions that allow certain entities to use these data for specific purposes, as detailed in Sect. 4.

2.2 Applicable Scenarios Where Consent to Health Data Altruism Is Pertinent

It is beyond the scope of this chapter to examine the interplay between the DGA and the recently approved EHDS Regulation. Yet, it is impossible to advance any further in this analysis of consent to health data altruism without delineating the scope of the EHDS and the conditions under which data altruism is meaningful for the reuse

[16] DGA, Article 2(11).

[17] DGA, Article 18(c).

[18] DGA, Recital 50.

of health data. Whereas the DGA delineates a common data governance model that transcends sectorial boundaries, the EHDS Regulation complements such requirements with rules that govern the sharing of health information for primary and secondary purposes. In terms of these secondary purposes, the EHDS Regulation mandates that health data holders with the right or obligation to process electronic health data for the purposes described at Article 1(2)(t)(i), including research and innovation, should make available the data they hold, so that it can be reused for other purposes.[19] Access to such data is subject to the authorization of health data access bodies[20] who may grant it only when the reuse is necessary for a closed list of purposes, including scientific research related to health or care sectors.[21] In other words, any organization dedicated to research and innovation, regardless of whether it is governed by private or public law, may act either as a data holder when it collects electronic health data via its research and innovation activities, or as a data user when it requests authorization to reuse health-related data for scientific research purposes.[22]

Since the availability of health data for reuse is obligatory under these circumstances, the success of the EHDS relies on a legal obligation as the legal basis for data sharing, rather than on consent by the data subjects. If people wish not to have their data processed for secondary purposes, they have the right to opt out.[23] Hence, if all the health-related data collected as part of research studies were made available for further use due to a legal obligation by default, my first analysis would conclude that consent to voluntary data sharing is irrelevant.

However, I can foresee a few scenarios in which consent to health data altruism may still be pertinent:

(i) Until the EHDS Regulation becomes applicable (or more particularly, until the provisions for secondary data use become applicable in 2029 and 2031 depending on the category of data), research organizations may want to resort to data altruism to maximize the accessibility to the data they collect. For instance, these organizations may wish to use the data to bolster open science and meet national policy objectives,[24] respect their funding entities' conditions or participate in self-regulatory activities;[25]
(ii) Similarly, before the 2029–31 horizon, the so-called "health-information altruists"[26] may want to make their data available to contribute to the common welfare, for instance through personal data spaces;

[19] EHDS, Article 51.

[20] EHDS, Article 57(1)(a).

[21] See the exact definition of admissible scientific research uses at Article 53(1)(e), EHDS.

[22] Defined very broadly, see Article 51, EHDS.

[23] EHDS, Article 71.

[24] See e.g., the Italian Piano Nazionale per la Scienza Aperta (PNSA), Rossi et al. (2022).

[25] See e.g., the Coalition for Advancing Research Assessment (CoARA), available at: https://coara.eu/.

[26] Kohane and Altman (2005), p. 2075.

(iii) Data subjects may have exercised their right to opt-out granted under the EHDS Regulation, but might still want to make their data available selectively, retaining more granular control, for example by selecting particular organizations that have access;
(iv) As foreseen by Article 16 of the DGA, national policies that put technical or organizational arrangements in place may support the willingness of individual citizens to grant access to their data voluntarily;
(v) Even when the EHDS Regulation becomes applicable, public bodies like research organizations may find it convenient to request or demonstrate consent for data access using DAOs. This would be a convenient way to circumvent the resource issues associated with complying with the DGA. For example, in Italy,[27] the DGA has been aligned to national legislation with a financial invariance clause that does not assign any additional resources for implementing the Act.

3 Consent to Health Data Altruism: Requirements and Challenges

The present analysis predominantly concerns a scenario where a research institution gathers health-related data from research participants who consent to the reuse of data for altruistic purposes. Necessarily, this entails that the research institution passes on the data to a DAO that provides access to data users, as illustrated in Fig. 1. In this scenario, consent needs to abide by several legal requirements deriving from the GDPR and the DGA, which are explained below. Further, this section explains that certain data flows are based on different types of consent with more or less specified purposes. Yet, despite the complexity of these data flows, the data altruism organization must support self-determination in the consent giver through a number of obligations intended to enhance trust. That said, these obligations create several legal, technical, and design challenges which are discussed in greater detail towards the end of this section.

3.1 GDPR Requirements for Consent to Scientific Research

3.1.1 Consent Requirements

Consent should involve an actual choice for the individual, i.e., it should be freely given, and should be tied to a specific purpose. Moreover, consent should be preceded by transparent information that enables informed decision-making and should

[27] Decreto Legislativo (2024).

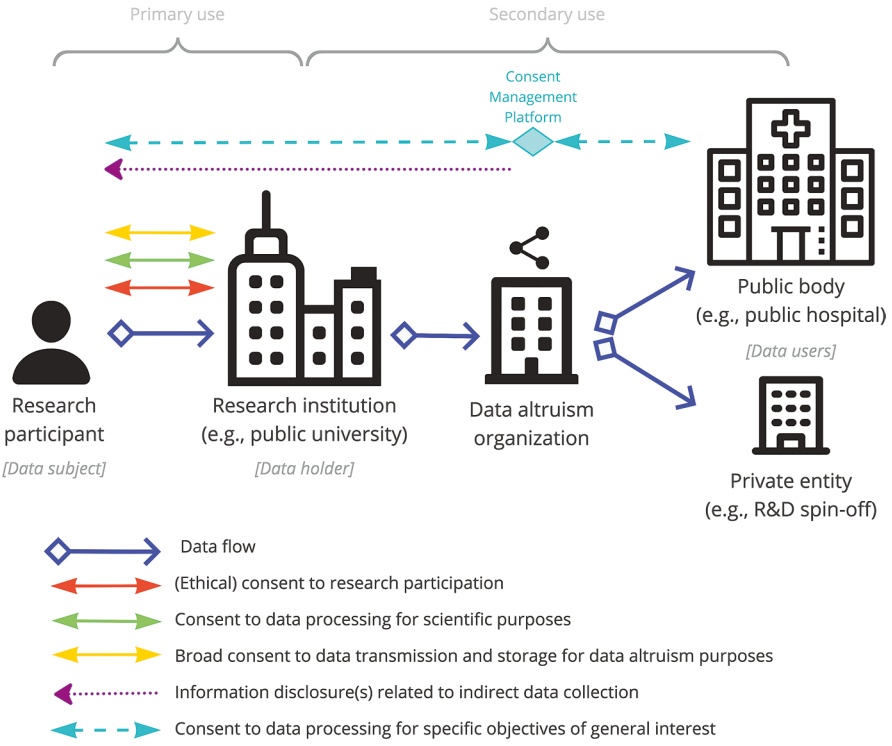

Fig. 1 This figure illustrates the data flows between the various actors, the related consent authorizations that are asked for and the information disclosures that are required when data collection is indirect

be signaled with an affirmative action, i.e., "an unambiguous indication of the data subject's wishes".[28] Further, consent should be implemented "in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language".[29] As an essential element for valid consent, the information disclosures should be transparent and should incorporate the substantial requirements listed in Articles 13–14 of the GDPR. These requirements mandate that certain information items be provided, such as the purpose of processing and the recipients of the data. This is coupled with the formal requirements provided in Article 12 of the GDPR, which mandate the quality, accessibility, and comprehensibility of the information. Dedicated guidelines specify that transparency should be user-centric,[30] meaning that information should be tailored to the information needs and abilities of the intended audience, while visual means of communication are explicitly encouraged,[31] especially when they help to inform

[28] GDPR, Article 4(11).

[29] GDPR, Article 7(2).

[30] Article 29 Working Party (2018), p. 5.

[31] Article 29 Working Party (2018), pp. 11–12.

individuals. Moreover, the data subject is entitled the "right to withdraw his or her consent at any time" which should be "as easy […] as to give consent".[32] Further, when special categories of data are at stake, the explicit consent of the data subject is one of the few legitimate grounds that constitutes an exception to the general prohibition of processing such data.[33]

3.1.2 Broad and Specific Consent to Scientific Research

All that said, the specificity of consent clashes with the open and undetermined nature of scientific research. The granularity of the consent given is intrinsically linked to the purpose specification principle, according to which the processing purpose needs to be limited in scope and rigorously defined.[34] However, Recital 33 does provide for some flexibility when it is not possible to fully identify the purpose for which the data will be used at the time they are collected. Recital 33 states that, as long as the purpose is described upfront in general terms and further specified as the research study progresses, individuals can consent to specific stages of the research as they become better defined. Still, even when not further specifiable, the European Data Protection Board recommends that the research areas be narrowed down—that is it be made clear how the purpose relates to the context where the data is gathered, and that any reasonable expectations on the part of the research participants are respected.[35] On this point, the Italian Data Protection Authority issued an opinion clarifying the conditions under which such an exceptional broad consent combined with a *consenso a fasi progressive* is admissible.[36] They state that lawful consent must be tied to specific research projects rather than mere research areas, which should conform to the methodological and deontological rules and the best practices that are specific to disciplinary domains.[37]

3.1.3 Research on Health Data and Transparency

Owing to the sensitivity of health information, the European Data Protection Board recommends applying "a stricter interpretation" to this flexible approach along with a "high degree of scrutiny".[38] To complement the breadth of the approach while upholding high standards of protection, "appropriate safeguards […] for the rights and freedoms of data subjects" should be put in place, such as data minimization,

[32] GDPR, Article 7(3).

[33] GDPR, Article 9(2)(a).

[34] European Data Protection Board (2020), p. 30.

[35] European Data Protection Board (2021), pp. 8–9.

[36] Garante per la Protezione dei Dati Personali (2022).

[37] European Data Protection Board (2020), p. 28.

[38] European Data Protection Board (2020), p. 31.

pseudonymization and anonymization[39] "to ensure the essence of the data subject's rights to valid consent are served".[40] Transparency complements such measures in the form of progressive disclosures that update the data subjects about advancements in the research project and ensure that "over time, the consent will be as specific as possible".[41]

All parties involved in the processing activities should, in addition, respect the provisions on information disclosures laid down in Article 13 when they gather data directly from data subjects. Moreover, parties need to respect Article 14 when data collection is indirect, such as is the case with data reuse by DAOs and data users. A substantial overlap between the information items required in these two conditions can be observed, with the difference that, when data collection is indirect, the source of data should also be disclosed[42] and the timing of the information provision can vary. Article 14(3) provides for a maximum of a 1-month delay after obtaining the data. If the personal data are used to communicate with the data subjects, they should be informed on such occasion, while, if the data are made available to other recipients (i.e., the data users), the disclosure should occur the first time that they are passed on. Notably, Article 14(5)(b) puts forward an exception to the information obligation in the case of scientific research and other general interest purposes when providing information proves impossible, it would require a disproportionate effort, or it would render impossible or seriously impair achieving the processing objectives. In such cases other safeguards apply, such as "making the information publicly available" (e.g., in a newspaper or on the research project's website), even though the European Data Protection Board recommends "the implementation of more dynamic ways of informing data subjects".[43]

3.2 Data Altruism Organizations' Consent Requirements in the DGA

Article 2(16) reporting the definition of data altruism leaves little doubt on the legal ground on which data altruism is based, i.e., consent as defined in article 4(1) of the GDPR.[44] However, recital 50 introduces regulatory ambiguity[45] when it states that "[t]ypically, data altruism would rely on consent of data subjects", thereby implying that a different legal basis may be admissible. This may be the case when data are further processed for scientific research purposes that should "not be considered to be incompatible with the initial purpose", in accordance with the GDPR's provision on purpose compatibility.[46] When it comes to managing multiple general interest

[39] GDPR, Article 89(1).

[40] European Data Protection Board (2021), p. 8.

[41] European Data Protection Board (2020), p. 31.

[42] GDPR, Article 14 (2)(f).

[43] European Data Protection Board (2021), p. 10.

[44] DGA, Article 2(5).

[45] Chassang and Feriol (2024), p. 68.

[46] Lalova-Spinks et al. (2023), p. 6.

purposes that entail more severe risks, though, consent may be an appropriate legal ground.[47] In line with the flexible approach delineated above, Recital 50 of the DGA recognizes that individuals may consent to using their data for certain areas of scientific research (provided that the relevant scientific research ethics standards are upheld); or only to certain areas of research; or only to parts of a research project.

In line with article 14(3) GDPR, the DAO must clearly inform data subjects "prior to any processing" of the objectives of general interest and, whenever possible, the specified, explicit and legitimate purposes for which it permits the processing by a data user.[48] Further, the DAO must also provide tools for consent management that enable data subjects to easily withdraw their consent,[49] for example when they do not agree with the processing operation they are informed of. In addition, the DGA lays down requirements for a data altruism consent form that enables data sharing operations with "additional legal certainty and user-friendliness". These clauses particularly apply when it comes to scientific research.[50] First, the form should gather consent across Member States in a uniform format as opposed to the current piecemeal approach.[51] Second, the form should be implemented a "modular approach allowing customization for specific sectors and specific purposes".[52] In other words, it should be standardized across nations and sectors, whilst still being able to accommodate any specific contextual needs that may arise, for instance, from the variety of data categories that can be donated and the related data protection rules.[53] Third, the conditions for granting and withdrawing consent should be in line with the legal requirements established by the GDPR, for instance for what concerns the granularity of the controls over "specific data processing operation[s]".[54] Lastly, the form should be printable on paper and to rendered into an electronic machine-readable format.[55]

3.3 Illustrating Research Data Flows Via Consent(s)

The data flows between the entities involved in data altruism are governed by consent permissions for the use, transmission, storage, and re-use of the data, as depicted in Fig. 1. Within the scenario introduced at the beginning of this section, the research institution asks for several consent permissions upfront, namely:

[47] Chassang and Feriol (2024), p. 65.
[48] DGA, Article 21(1).
[49] DGA, Article 21(3).
[50] DGA, Recital 52.
[51] DGA, Article 25(1).
[52] DGA, Article 25(2).
[53] DGA, Recital 52.
[54] DGA, Article 25(3).
[55] DGA, Article 25(4).

(ethical) consent to participate in scientific research and explicit consent to process their health data for a specific research project, unless another legal ground applies. Note that I have intentionally left aside the complexity that would be added by asking for informed consent for a clinical investigation, as required by Article 63 of the Medical Devices Regulation,[56] or for participating in a clinical trial as described in Article 29 of the Clinical Trials Regulation.[57]

The university as the data controller and data holder also asks for consent to transfer and store the data it has gathered with the DAO for data altruistic purposes, unless the compatibility assessment for further processing required by article 6(4) GDPR is positive. The assessment must be conducted on a case-by-case basis and, thus, it is difficult, if not impossible, to establish general conditions of compatibility between the original and the new purpose. When these are not met, the purpose must be re-specified and "a specific separate consent for the new processing" may be necessary.[58] I posit that data altruism consent would be quite broad at this stage and would require specification by the actual data users that request access to the data: only if specifically informed about the intended purposes of data use, data subjects can provide a valid consent and remain in control of their data.[59] If this is agreed, the DAO should then recontact the individuals to inform them that they store and make available the data for altruistic purposes, in accordance with Article 14(3)(a) GDPR. In addition, the organization should reach out to them "prior to any processing" to inform them of the objectives of general interest (and whenever possible of the specific purposes) pursued by the data users that it allows to access the data[60] and to disclose mandatory information about the data processing.[61] Even though current scholarly debate suggests that other legal bases for data altruism and for the further processing by data users[62] may be admissible, as exemplified earlier, these transparency obligations, coupled with those concerning the provision of tools for easy consent withdrawal[63] and the requirement for the form to enable consent withdrawal from specific data processing operations[64] suggest that the legislators envisioned a granular management of personal data based on individuals' consent.

[56] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. OJ L 117, 5.5.2017, pp. 1–175.

[57] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.OJ L 158, 27.5.2014, pp. 1–76.

[58] Article 29 Working Party (2013), pp. 26–27.

[59] European Data Protection Board (2020), p. 13.

[60] DGA, Article 21(1).

[61] GDPR, Article 14(3)(c).

[62] Lalova-Spinks et al. (2023), p. 7. The authors also suggest that data altruism consent could encompass the processing by data users, which would thus constitute primary use, rather than further processing, because the intention to enhance the availability of data motivated the data collection in the first place.

[63] DGA, Article 21(3).

[64] DGA, Article 25(3).

This interpretation may provide the specificity that is needed for the broad consent to data altruism to be further specified, as DAOs' intermediation service (e.g., in the form of a consent management platform) would enable data users to swiftly inform data subjects about data reuses once these are identified and negotiate granular permissions over time. Under this light, DAOs would fulfill an important role as enabler of research and would facilitate compliance with the transparency and consent obligations imposed by the GDPR. It remains to be understood, though, if they will help data users to additionally obtain other kinds of consent, such as research ethics consent to participation in non-interventional retrospective medical research studies.[65]

3.4 Additional Safeguards Around Data Altruism Consent

It goes without saying that making more health and other personal data available, especially those data associated with social stigmas, such as mental illnesses or sexually transmitted diseases, carries severe risks. Indeed, the EU Data Strategy strives to strike a balance between boosting the economic capacity of the continent and protecting its values and interests, under the motto "as open as possible, as closed as necessary".[66] As underscored earlier, providing consent for the vaguely defined objectives of "the general interest" appears to be at odds with the specificity requirement of the current legislative framework. Hence, additional safeguards become necessary—akin to consents for medical treatment and to participating in scientific research. Here, the autonomy of the people seems to be upheld by a "framework of supporting assurances [that] undergird and warrant consent agreements",[67] such as ethical and professional standards, institutional best practices, and codes of conduct. In this scenario, the research protocols that scientists submit to the competent ethics review boards will reasonably include the intention to share data for altruistic purposes. Moreover, data holders may formalize service agreements with trusted DAOs, constituting an additional insurance against malpractice.

In the new data governance framework designed by the DGA, the intention to establish trust mechanisms that draw a safety net around the self-determination of data subjects is well visible. For example, DAOs may want to resort to ethics councils or boards, which may include representatives from civil society, to ensure that the high standards of scientific ethics are maintained and fundamental rights are protected.[68] Further, data altruism organizations are subject to the following requirements that, I argue, strengthen the institution of consent:

[65] Lalova-Spinks et al. (2023), p. 6.

[66] European Commission (2020).

[67] Nissenbaum (2011), p. 36.

[68] DGA, Recital 46.

a. Official public registration:[69] Recognized DAOs should be included in a public register[70] maintained by a competent national authority (e.g., the AgID in Italy) and at the Union level by the European Commission. At the time of writing (May 2025), only one organization from Spain had been enrolled in such a registry;
b. Official trust seals:[71] Registered DAOs may publicly display the label "data altruism organization recognized in the Union" and a common logo[72] meant to convey a sense of safety to the public and guaranteed by a trustworthy third party, i.e., the EU;
c. EU jurisdiction: This refers to the place of establishment[73] or the legal representative[74] of the DAO , which must be a legal person pursuant to national law[75] and must be located a Member State to facilitate compliance and potential redress within the same jurisdiction;
d. Objectives of general interest: The DAO must promote objectives of general interest established in national law where applicable[76] and process data only for the purposes authorized by data subjects;[77]
e. Not-for-profit nature and neutrality: The DAO must not act for reasons of profit. They must be legally independent from any other organization that operates to make profit[78] and must perform data altruism activities via a structure with functions that are separate from its other activities;[79]
f. Transparency obligations:

    i) to ensure traceability: The DAO has obligations to keep "a full and accurate record"[80] of all data users, their processing purposes, the fees paid (if any) and the duration of processing;
    ii) to support oversight: The DAO must draft an annual activity report[81] addressed to a national competent authority with information encompassing the activities, the pursued purposes of general interest, a list of data users (including the techniques used to preserve privacy), the results of the processing, and any sources of revenue plus expenses.
    iii) to ensure informed decision-making: the DAO must also clearly and comprehensibly communicate to the data subject the objectives of general interest that it promotes, and the specific, explicit, legitimate purpose of the processing

[69] DGA, Articles 19, 17(1) and (2).
[70] European Commission (2024b).
[71] DGA, Article 17(2).
[72] European Commission (2023).
[73] DGA, Article 19(1),(2).
[74] DGA, Article 19(3).
[75] DGA, Article 18(a).
[76] DGA, Article 18(a).
[77] DGA, Article 21(2).
[78] DGA, Article 18(c).
[79] DGA, Article 18(d).
[80] DGA, Article 20(1).
[81] DGA, Article 20(2).

where applicable, "prior to any processing" (i.e., every time a data user requires access to data).[82] DAOs should find ways to keep individuals informed of the use of their data.[83] National arrangements may further specify the information that needs to be provided to data subjects.[84] The rulebook that the EC will need to draft[85] (see point i below) will further clarify how to inform data subjects of "sufficiently detailed, clear and transparent information" about use of data, about the measures against its misuse, and about the consent management tools.

g. Ease of consent management. To enable data subjects to easily give and withdraw consent,[86] DAOs must provide "easily usable" tools, that should constitute "effective and clearly communicated technical means to withdraw and modify consent at any moment".[87] The European Commission rulebook should further specify the requirements for ensuring the security of the tools;
h. Prohibitions to misleading marketing practices (fairness).[88] DAOs must avoid using misleading practices that entice data subjects to provide their data, for example by providing false information or somehow unduly influencing their decision-making, thereby recalling the Unfair Commercial Practices Directive's prohibition on misleading practices[89] (it goes without saying that data altruism organizations cannot be assimilated to traders as defined in the Directive and their relation with data subjects is not of a commercial nature);
i. Compliance with the EC rulebook.[90] The European Commission, through delegated acts, will develop a rulebook to guide DAOs in four crucial respects:[91] (1) laying down information requirements that enhance user-facing transparency on the use of data (see point f(iii)) above), on the tools for consent management, and on the measures adopted to avoid any data misuse. This is complemented by (2) "communication roadmaps" to raise awareness among data subjects on data altruism; (3) necessary technical and security requirements for reaching an appropriate level of security of the data storage and processing and of the consent tools; and (4) recommendations on the interoperability standards that will facilitate data exchange.

All these measures come together to form a novel governance framework that aims to strengthen the accountability and trustworthiness of data processing for altruistic

[82] DGA, Article 21(1).

[83] DGA, Recital 46.

[84] DGA, Article 16.

[85] DGA, Article 22(a).

[86] DGA, Article 21(3).

[87] DGA, Recital 46.

[88] DGA, Article 21(2).

[89] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the in-ternal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') OJ L 149, 11.6.2005, pp. 22–39.

[90] DGA, Article 18(d).

[91] DGA, Article 22.

reasons. Evidently, these factors need to be complemented with the measures foreseen in the GDPR on responsible data management by data controllers and data processors (depending on which role the data altruism organization takes on). This includes the adoption of a data protection by design and by default approach,[92] the likely appointment of a Data Protection Officer (e.g., if sensitive data are processed at scale)[93] and the evaluation and mitigation of risk with appropriate means,[94] including by conducting Data Protection Impact Assessments when necessary.[95] National provisions often supplement such measures, notably regarding the processing of health data.[96]

3.5 Challenges of Health Data Altruism Consent

A number of challenges arise from this analysis so far that are briefly summarized as follows. First, what exactly constitutes scientific research is not defined in the DGA,[97] which does not only bring indeterminacy to the application of the norm but also collides with the definitions provided in other legislations such as the GDPR, while the notion of public interest is equally blurred.[98] It is therefore left to DAOs to determine if the purposes pursued by data users are in line with public interest, and hence if the requested data can be accessed. Compliance by data altruism organizations is monitored by the competent authorities that register the organizations, but these are ex post assessments that may, at their worst, simply mean DAOs are delisted from the national register when a violation is found as per Article 24(5). Obviously, the data protection authorities can tangentially investigate infringements related to personal data.

Second, the validity of consent is also challenged by the idiosyncratic nature of data altruism consent. The tension between the openness of scientific research and the specificity of consent may, in principle, be solved with an initial broad consent that is more narrowly specified as and when the purposes are better determined (admitting that this is possible). Notably, the same exception would not apply to other purposes of general interest, which may be equally undetermined when one asks for a consent to data altruism. If this consent is not asked at the moment of data collection by a data holder, it may be very cumbersome for DAOs to get hold of a large variety of data donated voluntarily, because the alternative would be that individuals directly donate their data to the DAOs—a scenario that, despite being

[92] GDPR, Article 25.

[93] GDPR, Article 37.

[94] GDPR, Article 24.

[95] GDPR, Article 35.

[96] GDPR, Article 9(4).

[97] See in this volume Paseri, "Defining Scientific Research under the EU Politics of Data: The Impact on Personalized Smart Medicine", sec. 1.3.

[98] See in this volume Spajic, "Data altruism consent: A move forward towards the creation of a European health data space?", sec. 2.2.

desirable, may be limited by practical obstacles, such as the lack of real incentives for data subjects who cannot be compensated due to the very nature of data altruism. In addition, at the time of collection, the categories of recipients (i.e., the data users) are generally unknown. Yet, according to the GDPR's transparency requirements, they must be spelled out for consent to be informed. In other words, data altruism consent risks not being sufficiently specific and informed, and it is not clear if these flaws can be redressed with an initial broad consent that is specified later.

Third, there is great uncertainty in terms of how consent experiences will be designed in practice. This is despite the obligations placed on DAOs to offer tools for consent management that are easy to use and to inform concerned individuals before a new processing operation starts so that they can adjust their consent preferences. For example, if we imagine these tools as mobile apps, it would be very confusing for an individual to be recontacted by various DAOs through different channels. However, to date, there is no standard digital solution for consent management—neither one specifically geared towards the needs of data altruism nor a general-purpose one.[99] That said, the data ecosystem is ripe with consent management tools that variously, but not simultaneously: i) identify and authenticate users; ii) manage consent permissions; and iii) enable the portability of data.[100] What is clear, though, is that the form envisioned by the legislators does not resemble the traditional consent document that most are familiar with.

4 Designing and Personalizing Dynamic Consent Experiences

There are many possible scenarios of data exchange. As such, data altruism organizations are subject to a highly complex set of obligations. This suggests a need for innovative and user-friendly solutions that allow data subjects to make informed, real-time decisions about who can use their data and for what purpose. Even though many voices raise criticism to consent as an instrument of self-determination,[101] consent is here to stay and we should thus design better, more dynamic ways of managing consent. By better, I mean these solutions should avoid the weaknesses of the current contemporary approaches to digital consent—approaches that deprive people of their autonomy through deceptive designs,[102] instead of bolstering it. Tomorrow's tools should inform data subjects at an appropriate time and with increasing specificity when needed. Importantly, the experience should also be user-friendly as usability is a precondition of accountability in data management practices. This is because it underpins respect for the policies governing the use of data

[99] European Commission JRC (2024a), p. 3.

[100] European Commission JRC (2024a), p. 10.

[101] See for instance Carolan (2016).

[102] See e.g., Gunawan et al. (2022) and Bielova et al. (2024b).

that are embedded in the front-end and back-end of data management tools. The access to data that consent permissions authorize needs to be accurately documented for transparency and accountability reasons. Additionally, establishing empirical guidelines for those designing the data altruism consent form is paramount to fostering trust in data sharing. However, this is beyond the scope of the limited space in this chapter. Nevertheless, my aim is to introduce existing technologies that address two elements: a user interface that incorporates both the requirements of transparency and of consent by displaying the information notice and offering controls over consent management; and technologies that enable machine-readability by expressing data permissions and by automating and documenting how one's data is used.

4.1 Beyond Consent Forms and Towards Dynamic User Experiences

4.1.1 Personalized Dynamic Consent

Traditionally, consent has been provided at a single point in time.[103] However, today, with data being constantly reused, consent must be given or withdrawn at many different points in time. As such, two-way communication is needed[104] before, during, and after consent.[105] Otherwise, how can data subjects revoke their consent in real time and at will?[106]

Given the consent requirements of personalized medical research, dynamic consent is, arguably, the most suitable solution. This is because dynamic consent can accommodate the various nuances of data altruism, such as providing numerous specific consents to data use that specify the initial broad consent. Dynamic consent is currently being experimented with in the field of biobanking research. It is formulated as a "personalized consent and communication platform"[107] that "allows participants to review and change consent choices over time via a personalized digital interface".[108] This model of consent gives rise to a continuous deliberative process that aligns with the evolution of people's preferences. Thus, it can be updated to reflect new processing opportunities that arise, such as a new organization asking for access to data or a new research project starting. Bespoke solutions are supported, both in terms of tailoring the options on data usage and in terms of methods of communication.[109] In one of the few existing longitudinal studies,

[103] Rossi and Haapio (2021), pp. 118–119.

[104] Lee et al. (2023), p. 8.

[105] Mascalzoni et al. (2022), p. 1395.

[106] Dankar et al. (2020), p. 916.

[107] Dankar et al. (2020), p. 916.

[108] Lay et al. (2025), p. 181.

[109] Lee et al. (2023), p. 8.

communication was personalized in terms of the language and the frequency of communication.[110] The authors also used a multimedia approach that could cater to either those with digital skills or those who preferred paper-based or vocal communication.

Even though empirical evidence of how this concept works in practice is still limited, dynamic consent promises to uphold the autonomy of individuals via greater transparency, control, and engagement. It also promises to support research by enabling the researcher to obtain consent for further uses, affording withdrawal options and reducing the time, burden, and administrative costs associated with reconsenting. Additionally, such platforms should help to improve compliance with ever-changing legal requirements.[111] Increased direct communication with the individuals also brings a particularly appealing benefit in the context of data altruism—namely, the possibility of receiving further information after the data processing has been completed, such as the latest developments in research, the dissemination of findings, and other outcomes generated thanks to the donated data.[112] This can be thought of as non-pecuniary compensation.

However, the sheer number of consent decisions required may be overwhelming, which would act against autonomy rather than in its favor. If information overload were to occur, individuals might withdraw their consent.[113] To date, studies have not shown that this happens, but it is still a possibility.[114] Here, tiered layered consent discussed in genetic testing contexts constitutes an interesting solution, as it provides information in layers, e.g., from general default information to specific information. Consent is given in certain categories, such as purposes, the actionability of results, or the expected level of emotional impact.[115] In this way, such approaches promote granularity without overwhelming the person. Rather, each individual gets to decide the level of detail they prefer.

Similar to consent fatigue, information fatigue represents a major concern that is only destined to grow as the amount of data exchange and consent requests increase. Providing relevant yet concise information is a recognized issue, i.e., the so-called transparency paradox.[116] Academia, business,[117] and even the data protection authorities[118] themselves have all proposed innovative solutions, such as layering information to respond to various users' profiles and needs. Transparency, though, does not necessarily need to be one-size-fits-all solution. Rather, as recommended by the

[110] Mascalzoni et al. (2022), pp. 1395–1396.

[111] Lay et al. (2025), p. 182 and pp. 195–196.

[112] Lee et al. (2023), p. 8.

[113] Dankar et al. (2020), pp. 916–917.

[114] Mascalzoni et al. (2022), p. 1396.

[115] Bunnik et al. (2013).

[116] Nissenbaum (2011).

[117] Rossi et al. (2019).

[118] Article 29 Data Protection Working Party (2018); Commission Nationale de l'Informatique et des Libertés (n.d.); Creative Commons Italy & Garante per la Protezione dei Dati Personali (2025).

European Data Protection Board in the dedicated guidelines, it should be user-centric.[119] This opens up the possibility of tailoring requests for data use to the preferences of the data subjects. For instance, some people may prefer graphics, comics, or videos, to text. Others may prefer simple vocabulary, while others still might appreciate expert-level jargon.[120] As such, these tailored requests may be more effective at informing specific individuals about what their data will be used for than traditional methods.

Of course, it needs to be determined as to whether dynamic consent can uphold comprehension and autonomy in practice in the different scenarios that data altruism enables, since it is an under-researched topic in the biomedical domain. Mostly, dynamic consent has been applied to genomic research.[121] For example, the fact that the categories to which people may consent are defined by default has been pointed out as a limitation to self-determination.[122] A lack of sufficient literacy on the part of users (be it health literacy, digital literacy, data literacy, AI literacy, risk literacy) is also another critical issue pertaining to consent models. Additionally, users need time and a certain level of motivation to be able to confidently navigate the permissions and control policies offered to them. Dynamic consent requires them to continuously express decisions that are in line with their preferred values while also understanding the implications of their choices. Without addressing these challenges, dynamic consent users risk disengagement and marginalization.[123]

Moreover, preferences are also highly personal and highly contextual. So, although one might apply some general rules to streamline how users convey their preferences, like tiered consent, this approach may still be too coarse-grained. However, there is at least one emerging technology that seeks to tackle this issue: personalized privacy assistants. These are intelligent agents that provide personalized privacy notices, explanations and recommendations, but can also automate decision-making by learning the privacy preferences of their users over time, configuring settings semi-automatically, and making privacy decisions on their behalf.[124] Currently, personalized privacy assistants are still experimental, but they have been patented.[125] Notably, though, several questions about their legal and ethical legitimacy still need to be answered.

4.1.2 Influencing Decision-Making Through Design

The way information and options are designed and presented to individuals is an extremely powerful mechanism and can either encourage or discourage their intention to share data. There is an abundant body of literature that demonstrates how the

[119] Article 29 Working Party (2018), p. 5.

[120] Doan et al. (2024).

[121] Dankar et al. (2020), p. 919.

[122] Wiertz and Boldt (2022), p. 275.

[123] Lee et al. (2023), p. 8.

[124] See e.g., Chang and Barber (2023).

[125] See the Personalized Privacy Assistant Project (2025).

behaviors, perceptions, and trust of human beings can be influenced by the way a user interface is designed—this is why design considerations for the data altruism consent form are of the utmost importance. Unfortunately, consent fatigue is presenting obstacles to a user-friendly management of consent. Taking lessons from the overly granular interactions European users have with cookie consent banners on websites, there is not only evidence that people have learned to mindlessly give consent to cookies but that this automatic behavior persists over time and will be difficult to unlearn in the case of consent for data altruism.[126] Further, many empirical studies have shown that framing choices in a positive or negative light affects whether individuals disclose their personal data, especially when people are uncertain about the reasons why they are asked to share their data and the consequences of doing so.[127] In this respect, the European Data Protection Board states that loss-gain framing is an unfair practice[128] and the DGA indeed forbids the use of misleading marketing practices to solicit the provision of data. Not all design patterns that nudge users towards preferred behaviors are intrinsically evil, though. For instance, presenting the outcomes of decisions in a positive or negative manner can bolster data sharing for altruistic purposes. Underlining its benefits to the individual and to society may inspire the motivation to make one's data available, even though the risks of doing so should be spelled out transparently. Thus, the obligation to present fair and equal choices need to be prudently balanced with the necessity to incentivize data sharing for altruistic purposes. Hence, although there is an increasing awareness of the influence that interface design choices have on the disclosure of data, more research in the specific context of health data altruism needs to be done before empirically-based guidelines can be produced.

4.2 Machine-Readable, Interoperable Semantics

The need for semantic interoperability standards governing the exchange of health data is becoming urgent.[129] Further, another essential aspect of realizing the EU's vision of freely flowing data spaces concerns the necessary automation of data practices. For example, consent permissions need to be standardized, machine-readable, and actionable across organizations, sectors, and applications. To this end, open (i.e., free and non-proprietary) semantic web technologies and their integration with international standards represent a promising approach to addressing these requirements.

For a system to process, document, and verify data exchanges so as to comply with applicable laws, that system needs to be able to interpret various types of

[126] Bielova et al. (2024a).

[127] Bongard-Blanchy et al. (2023).

[128] European Data Protection Board (2023), pp. 19–20.

[129] Abboud et al. (2022).

information,[130] including obligations, permissions, and the requirements that govern the admissible use of data. A widely adopted standard for crafting such data use policies is W3C's Open Digital Rights Language (ODRL). Its Access Control (OAC) profile allows users like researchers or DAOs to create policies that govern how personal data is used based on a particular purpose. They can also restrict access to some data after a certain period of time has passed or authorize only certain types of entities to access the data.[131] ODRL by itself only provides the structure for expressing rules and policies like permissions and obligations, but lacks semantics: it needs a vocabulary that provides terms that identify legal concepts. The Data Privacy Vocabulary (DPV) published by the W3C DPVCG is one of such semantic resources that enables users to create legally relevant policies with the use of ODRL, when this is extended to represent legislations like the GDPR.[132] The DPV is an ontology that formally expresses a wide range of information concerning data, processing purposes, processing operations, legal bases, data subjects' rights, and more.[133] Formally expressing the requirements for altruistic reuse would allow users to easily query the public registers of data altruism organizations.[134] Additionally, data access requests could, in principle, be automatically matched to the available datasets held by DAOs in line with established conditions. In a similar manner to tiered consent, the data subjects themselves can set their preferences for the data uses they authorize, instead of needing to continuously engage in an overly granular deliberative process that may be overwhelming. Semantic specifications have also been matched with international standards on consent to tackle interoperability and machine-interpretability challenges. Notably, efforts such as these intend to foster the widespread adoption of a commonly recognized format.

Informed consent generally comprises two elements. First is a consent notice that contains relevant information about the data processing operations that will occur if consent is given. This fulfills the transparency obligations of the GDPR and the DGA. Second is a consent receipt that keeps a record of the decisions made, which fulfills the obligations mandated by the GDPR and the DGA to maintain a record of any consents given.[135] The ISO/IEC 29184:2020 "Privacy Notices and Consent" specifies how information is provided to individuals via consent request notices and largely covers the GDPR's requirements but not completely.[136] ISO 29184 is helpful for demonstrating compliance and can also provide a standard format for documenting consent. It also offers options for personalization, as machine-readable consent notices can be issued in text, visual, or graphic form

[130] Esteves et al. (2023), pp. 216–217.

[131] Esteves et al. (2023), p. 217.

[132] W3C DPVCG (2025).

[133] Pandit et al. (2024a).

[134] Esteves et al. (2023), p. 222.

[135] Pandit et al. (2024b), pp. 228–229 and 231.

[136] Pandit and Krog (2021), p. 203.

through a variety of user interface mediums, such as layered notices, icons, dashboards, or just-in-time notices.[137]

In terms of documenting consent, which involves creating, maintaining, communicating, and disclosing consent decisions in a machine-readable format, the ISO/IEC TS 27560 "Privacy technologies—Consent record information structure" specifies an interoperable, standardized information structure that defines how consent decisions should be recorded and documented.[138] The standard specifies common field requirements, such as a unique identifier for the consent record, the entities involved, the processing purposes, the data categories, the status of consent, and so on. It also stipulates the form the information can take, like the format.[139] Organizations can then use these records to determine whether certain processing is allowed and, therefore, whether data processing can start, continue, or should be terminated, such as when consent is withdrawn or has expired. Additionally, the standard is flexible enough to incorporate domain-specific labels or be extended to additional fields or information types that may become necessary, for example to relate to certain legislations and jurisdictions.[140] It can also be implemented in a machine-readable format (such as JSON), which could then be integrated with some standard interoperable semantics,[141] like the W3C's Data Protection Vocabulary which can be expanded to include legal terms that pertain to the DGA or the EHDS.[142]

Without these standardization efforts, it is impractical to implement data sharing, because there will be a multitude of ad hoc consent implementations which would result in fragmented ecosystems. Instead, a pan-European implementation needs to rely on semantic interoperability for consent to be widely accepted: standardizing semantics ensures that machines not only interpret the structure but also understand the meaning of information, thereby enabling reliable data access automation at scale. Additionally, this approach supports transparency and traceability of data access decisions, and thus accountability towards reusing data. It also makes it easy for data subjects to exercise their rights. Semantic specifications may support personalization in terms of both how the information notice is presented[143] and the consent permissions individuals can express. However, such an approach means that there needs to be an agreed upon semantic specification for all the relevant concepts, including for all possible processing purposes. Purposes need to be expressed in a highly precise manner to satisfy the GDPR's requirements over consent, though. Such a top-down approach may hardly be compatible with a bottom-up approach where researchers in the role of data users progressively refine the definition of the processing purpose on a case-by-case basis. That said, the Data

[137] Pandit and Krog (2021), p. 198.

[138] Pandit et al. (2024b), p. 230.

[139] Pandit et al. (2024b), p. 229.

[140] Pandit et al. (2024b), p. 229.

[141] Pandit et al. (2024b), p. 237.

[142] See the EHDS extension HealthDCAT-AP available at: https://healthdcat-ap.github.io/.

[143] Pandit et al. (2018).

Protection Vocabulary can accommodate for jurisdictional variance. For example, if the vocabulary contains the general concept "purpose", the DGA extension can support the specification "objective of general interest", which can be further specified at the national level or even by a specific data user. The semantic interoperability derives from the common parent concept contained in the Data Protection Vocabulary. However, the pathway to a consensus on the widespread adoption of these technologies may be long and uncertain, while declarative conditions of data use policies may also be ignored, leading to data misuse.[144]

5 Future Work and Conclusions

This chapter has examined consent for data altruism from the legal, design, and technical perspectives. As such, this work may offer early solutions to the challenges that implementing consent could pose. The chapter began by delineating the scenarios where health data altruism may still be meaningful, even though the EHDS regulation imposes the legal obligation to share health-related data. Next was to identify the requirements associated with the various consents that need to be requested for information to flow between entities. Here, I argued that the DGA establishes accountability and transparency safeguards that are necessary for strengthening the institution of consent as a means of self-determination. I also sketched out several challenges relating to the legitimacy, specificity, and usability of data altruism consent. Solutions to these issues include the dynamic consent embedded in emerging semantic web technologies, which enable the real-time interoperable exchange of data use permissions and automated access to datasets based on pre-specified conditions. Thanks to technological development, information disclosures and consent management could be more personalized in the near future, which may address some of the hurdles associated with contemporary digital consent, such as information fatigue and consent fatigue. That said, imposing one model of consent onto various contexts where different sensitivities are at play needs to be well-thought out as "choosing a model becomes a matter of finding an acceptable compromise"[145] and depends on factors such as the trustworthiness of the organization, whether the data subjects participate in determining what their data is being used for, and the surrounding safeguards that strengthen the institution of consent.

With the aim of informing the European Commission's work on a rulebook governing data altruism, the goal of future work is to draft some recommendations on how to design an empowering consent experience that encourages data sharing for altruistic purposes without exploiting the subject's cognitive biases. Part of this means considering the many types of human-computer interaction, including those

[144] Esteves et al. (2023), p. 224.

[145] Wiertz and Boldt (2022), p. 277.

with artificial agents. Future research will also need to address the open challenges identified in this chapter by exploring additional scenarios related to data altruism, such as collecting data directly from the data subjects and data processing for the purposes of general interest beyond that of scientific research. Topics that also need to be considered include the benefits of anonymizing data; the requirements for identity management and the security of consent-related data; the permissible processing of non-personal data, and how to implement permission management systems. Moreover, the legal and technical challenges arising from crossovers between the EHDS Regulation, the Open Data Directive,[146] the Medical Devices Regulation, and the Clinical Trials Regulation need to be further investigated.

This chapter concludes with a plea to ground the guidelines for implementing data altruism consent in the kind of interdisciplinary evidence that reflects how human beings make decisions about their data—evidence that realistically portrays the technological maturity of the proposed solutions. Consent can still be a substantial instrument of self-determination, but we need a concerted effort to seriously address the roots of disengagement, confusion, and deception caused by existing digital consent experiences.

Acknowledgments This research was financially supported by the "Biorobotics Research and Innovation Engineering Facilities" "IR0000036" – CUP J13C22000400007 (BRIEF) project. I would like to thank Federica Casarosa, Francesca Gennari and Harshvardhan Pandit for their precious comments on an early draft of this chapter. A special thanks goes to Andrea Parziale, who helps me to bring order to the rather confusing sketches I make on the whiteboard of our shared office and, therefore, to my thoughts. In this work I have managed to join insights from various past research studies that I have conducted with many colleagues, whom I thank for their enthusiasm, ideas and time.

Disclosure of Interests The author has no competing interests.

References

Abboud L, Bogaert P, Bowers S et al (2022) Report on secondary use of health data through European case studies. TEHDAS Towards European Health Data Space

Article 29 Data Protection Working Party (2018) Guidelines on Transparency under Regulation 2016/679, 17/EN WP260 rev.01. Adopted on 29 November 2017. As last Revised and Adopted on 11 April 2018

Article 29 Working Party (2013) Opinion 03/2013 on purpose limitation

Bielova N, Litvine L, Nguyen A et al (2024a) The effect of design patterns on (present and future) cookie consent decisions. In: Proceedings of the 33rd USENIX Security Symposium. Philadelphia USA, pp 1–9

Bielova N, Santos C, Gray CM (2024b) Two worlds apart! Closing the gap between regulating EU consent and user studies. Harv J Law Technol 37:1295–1333

[146] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. PE/28/2019/REV/1. OJ L 172, 26.6.2019, pp. 56–83.

Bongard-Blanchy K, Sterckx J-L, Rossi A et al (2023) Analysing the influence of loss-gain framing on data disclosure behaviour: a study on the use case of app permission requests. In: Proceedings of the 2023 European Symposium on Usable Security. ACM, Copenhagen, Denmark

Bunnik EM, Janssens ACJW, Schermer MHN (2013) A tiered-layered-staged model for informed consent in personal genome testing. Eur J Hum Genet 21:596–601. https://doi.org/10.1038/ejhg.2012.237

Carolan E (2016) The continuing problems with online consent under the EU's emerging data protection principles. Comput Law Secur Rev 32:462–473

Chang K-C, Barber S (2023) Personalized privacy assistant: identity construction and privacy in the internet of things. Entropy 25:717

Chassang G, Feriol L (2024) Data altruism, personal health data and the consent challenge in scientific research: a difficult interplay between EU acts. Eur Data Prot Law Rev 10:57–68. https://doi.org/10.21552/edpl/2024/1/9

Commission Nationale de l'Informatique et des Libertés (n.d.) Design Patterns – Données & Design par LINC. https://design.cnil.fr/en/design-patterns/

Corona Datenspende (2025). https://corona-datenspende.github.io/en/#about

Creative Commons Italy, Garante per la Protezione dei Dati Personali (2025) White Paper - Rendere le informative privacy più comprensibili. Il legal design come approccio rivolto all'utente. GPDP, Roma

Dankar FK, Gergely M, Malin B et al (2020) Dynamic-informed consent: a potential solution for ethical dilemmas in population sequencing initiatives. Comput Struct Biotechnol J 18:913–921. https://doi.org/10.1016/j.csbj.2020.03.027

Decreto Legislativo 7 ottobre 2024, n. 144 Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724. (24G00167). https://www.gazzettaufficiale.it/eli/id/2024/10/10/24G00167/SG

Doan X, Doğan FS, Rossi A (2024) Analysis of transparency and user-relevancy of DTC company policies. In: Hoepman J-H, Jensen M, Porcedda MG, Schiffner S, Ziegler S (eds) Privacy Symposium 2024. Springer Nature Switzerland, Cham, pp 191–215

Esteves B, Rodríguez Doncel V, Pandit HJ, Lewis D (2023) Semantics for implementing data reuse and altruism under EU's Data Governance Act. In: Acosta M, Peroni S, Vahdati S et al (eds) Knowledge graphs: semantics, machine learning, and languages. IOS Press, pp 210–226

European Commission (2020) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions. A European Strategy for Data

European Commission (2023) Logos for data intermediaries and data altruism organisations recognised in the Union. Available at: https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union

European Commission (2024a) Joint Research Centre. The landscape of consent management tools: a data altruism perspective. Publications Office, LU

European Commission (2024b) EU register of recognised data altruism organisations. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations

European Data Protection Board (2020) Guidelines 05/2020 on consent under Regulation 2016/679

European Data Protection Board (2021) EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research

European Data Protection Board (2023) Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0. European Data Protection Board

Garante per la Protezione dei Dati Personali (2022) Parere ai sensi dell'article 110 del Codice e dell'article 36 del Regolamento - 30 giugno 2022 [9791886]

Gunawan J, Santos C, Kamara I (2022) Redress for dark patterns privacy harms? A case study on consent interactions. In: Proceedings of the 2022 Symposium on Computer Science and Law. pp 181–194

Kohane IS, Altman RB (2005) Health-information altruists — a potentially critical resource. N Engl J Med 353:2074–2077. https://doi.org/10.1056/NEJMsb051220

Lalova-Spinks T, Meszaros J, Huys I (2023) The application of data altruism in clinical research through empirical and legal analysis lenses Frontiers in Medicine 1010.3389/fmed.2023.1141685

Lay W, Gasparini L, Siero W, Hughes EK (2025) A rapid review of the benefits and challenges of dynamic consent. Res Ethics 21:180–202. https://doi.org/10.1177/17470161241278064

Lee AR, Koo D, Kim IK, Lee E, Kim HH, Yoo S, Kim J-H, Choi EK, Lee H-Y (2023) Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: a scoping review. BMC Med Ethics 24:107. https://doi.org/10.1186/s12910-023-00988-9

Mascalzoni D, Melotti R, Pattaro C et al (2022) Ten years of dynamic consent in the CHRIS study: informed consent as a dynamic process. Eur J Hum Genet 30:1391–1397. https://doi.org/10.1038/s41431-022-01160-4

Micheli M, Farrell E, Carballa SB, Posada SM, Signorelli S, Vespe M (2023) Mapping the landscape of data intermediaries. Joint Research Centre, Luxembourg

National Research Council (US) Committee on A Framework for Developing a New Taxonomy of Disease (2011) Toward Precision Medicine: Building a Knowledge Network for Biomedical Research and a New Taxonomy of Disease. National Academies Press (US), Washington (DC)

Nissenbaum H (2011) A contextual approach to privacy online. Daedalus 140:32–48. https://doi.org/10.1162/DAED_a_00113

Pandit HJ, Krog GP (2021) Comparison of notice requirements for consent between ISO/IEC 29184:2020 and General Data Protection Regulation. J Data Prot Priv 4:193–204

Pandit HJ, O'Sullivan D, Lewis D (2018) Personalised privacy policies. In: Benczúr A, Thalheim B, Horváth T et al (eds) New trends in databases and information systems. Springer International Publishing, Cham, pp 127–137

Pandit HJ, Esteves B, Krog GP et al (2024a) Data Privacy Vocabulary (DPV) – Version 2.0. In: Demartini G, Hose K, Acosta M et al (eds) The Semantic Web – ISWC 2024. Cham, Springer Nature Switzerland, pp 171–193

Pandit HJ, Lindquist J, Krog GP (2024b) Implementing ISO/IEC TS 27560:2023 consent records and receipts for GDPR and DGA. In: Jensen M, Lauradoux C, Rannenberg K (eds) Privacy technologies and policy. Springer Nature Switzerland, Cham, pp 228–251

Personalized Privacy Assistant Project (2025), available at: https://privacyassistant.org/

Robert Koch Institute & Research on Complex Systems of Humboldt University of Berlin (2025), Corona Data Donation Project, available at: https://corona-datenspende.github.io/en/

Rossi A, Haapio H (2021) Proactive legal design for health data sharing based on smart contracts. In: Smart contracts: technological, business and legal perspectives, Marcelo Corrales, Mark Fenwick and Stefan Wrbka. Hart Publishing, London, pp 101–122

Rossi A, Ducato R, Haapio H, Passera S (2019) When design met law: design patterns for information transparency. Droit de la Consommation = Consumenterecht: DCCR 79–121

Rossi G, Caso R, Castelli D, Giglia E (2022) Piano Nazionale per la Scienza Aperta. Ministero dell'Università e della Ricerca

Schweihoff J, Lipovetskaja A, Jussen-Lengersdorf I, Möller F (2024) Stuck in the middle with you: conceptualizing data intermediaries and data intermediation services. Electron Markets 34:48. https://doi.org/10.1007/s12525-024-00729-9

W3C DPVCG (2025) "DPV - EU General Data Protection Regulation (GDPR) version 2.1", available at: https://w3c.github.io/dpv/2.1/legal/eu/gdpr/

Wiedermann M, Rose AH, Maier BF, Kolb JJ, Hinrichs D, Brockmann D (2023) Evidence for positive long-and short-term effects of vaccinations against COVID-19 in wearable sensor metrics. PNAS nexus 2:pgad223

Wiertz S, Boldt J (2022) Evaluating models of consent in changing health research environments. Med Health Care Philos 25:269–280. https://doi.org/10.1007/s11019-022-10074-3