TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Ana Koiava

Challenges of GDPR Compliance with the Data Altruism Concept under DGA: Lessons from the Estonian X-Road Model

Master's thesis

Programme - HAJM, Specialisation -Law and Technology

Supervisor: Professor Thomas Hoffmann

Co-supervisor: Dr. Archil Chochia

Tallinn

2024

I hereby declare that I have compiled the thesis/paper independently and all works, important standpoints and data by other authors have been properly referenced and the same paper has not been previously presented for grading. The document length is 19 257 words from the introduction to the end of the conclusion.

Ana Koiava (07.05.2024)

Table of Contents

Abstract

The introduction of the Data Governance Act (DGA) has marked a significant development in the European data landscape. The DGA entered into force on 23 June 2022 and became applicable in September 2023[1]. This landmark legislation aims to reshape data governance practices within the European Union, setting the stage for a new era of data utilization and regulation[2]. However, it presents a complex challenge - how to align these goals with the strict data protection standards outlined in the General Data Protection Regulation (GDPR). This research is driven by the recognition that understanding and addressing the compliance challenges that arise when balancing data altruism, data sharing, and data protection in the European data landscape are more crucial than ever.

The relevance of this research topic is evident in the objectives set forth by the DGA. By increasing data availability, the European market seeks to gain a competitive advantage, stimulate innovation, and foster economic growth. This not only has implications for commercial enterprises but also for research initiatives[3]. Therefore, it is crucial to understand the compliance challenges and potential solutions, particularly when posed with the requirements of GDPR.

This research seeks to address How can GDPR-compliant approaches be established to facilitate efficient, secure, practicable, and simple data exchange under the DGA, especially in the context of data altruism, and drawing from the experiences of the Estonian X-Road. This research question emerges from the complexities and potential contradictions between the aims of the DGA and the strict data protection requirements under GDPR. Also, it is important to determine how data altruism can be practically executed according to the data portability principle.

Key Words: Data Governance Act, Data Altruism, Data Altruism Consent, GDPR.

[1] European Data Governance Act, Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.
[2] *Ibid.*
[3] A European strategy for data, Brussels, 19.2.2020 COM (2020) 66 final.

Introduction

In this modern, technological era, digital technologies have undergone significant advancements, profoundly impacting both the economy and society. This transformation has deeply influenced various sectors of activity and has become an integral part of people's daily lives. At the core of this transition lies the centrality of the data, a fundamental element that maintains its critical importance and is set to continue shaping future advancements[4].

The utilization of data-driven innovation holds the promise of delivering substantial benefits to citizens across various areas. However, in a landscape where individuals are generating ever-increasing volumes of data, the collection and utilization of this data must prioritize the interests of the individuals. Building and maintaining trust in data-driven innovations depends on ensuring that personal data shared within the European Union is handled in strict compliance with the General Data Protection Regulation (GDPR)[5], thus ensuring trust in this process.

Therefore, it was imperative to enhance data-sharing conditions within the internal market by establishing a standardized framework for data exchanges and defining essential and structured requirements for data governance. Special attention was given to facilitating collaboration among Member States. Due to that, The European Commission adopted the Data Governance Act (DGA), which was enacted on June 23, 2022, and became enforceable in September 2023. This regulation aims to further develop the digital internal market and encourage a data society and economy that prioritizes human values, human rights, trustworthiness, and security. This is especially important because the adoption of the DGA by the Commission signifies its commitment to promoting harmonized data governance practices across the EU[6].

As discussed before, the Digital Governance Act represents a significant milestone within the scope of data utilization and the digital market, offering various advantages that will be explored further in this research. It's crucial to highlight that this Act introduces new concepts essential for effective data governance, shedding light on the principles of data sharing and its appropriate

[4] A European strategy for data, Brussels, *supra nota* 3, p.1.
[5] *Ibid.*
[6] Regulation (EU) 2022/868 of the European Parliament and Council, of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44.

usage. One of these essential concepts is "data altruism," along with the establishment of data altruism organizations, which are integral components of the Digital Governance Act. According to Article 2, Part 16 of the Act, "data altruism" refers to the voluntary sharing of data, either personal or non-personal, based on the consent of data subjects or the permissions of data holders. This sharing is undertaken without seeking or receiving any reward beyond compensation for incurred costs. Such data sharing serves objectives of general interest, as outlined in national law, including but not limited to healthcare, environmental conservation, transportation improvement, statistical analysis, public service enhancement, policy formulation, and scientific research. These objectives underscore the Act's commitment to promoting social welfare and advancing public interest initiatives[7].

Despite the significant benefits of data altruism for the sharing and utilization of data for the collective good, thereby expanding research and innovation opportunities, there are potential compliance issues with the General Data Protection Regulation. Additionally, as the regulation is relatively new, the full operational and practical mechanisms and implications are not yet fully understood. However, this research aims to examine the data-sharing challenges under the Digital Governance Act and analyze its compliance with the strict provisions of the GDPR. The fundamental question arises as to whether it is possible to ensure secure and ethical data sharing under the DGA, considering the potential risks associated with the voluntary sharing of personal data. The GDPR has established practical and robust guidelines for data protection, yet breaches still occur. In this context, it becomes imperative to assess whether the DGA should impose stricter regulations to mitigate these risks effectively. It is essential to distinguish the differences between the GDPR and the DGA to understand their respective roles in data governance. While the GDPR primarily focuses on protecting and processing of personal data and ensuring individuals' rights, the DGA aims to regulate data governance practices more broadly. However, the effectiveness of the DGA in achieving these objectives remains uncertain, particularly in light of the challenges posed by data altruism. Moreover, with the GDPR already in force, the necessity of the DGA and the concept of data altruism comes into question. Also, there is still a question of whether the DGA offers significant added value in terms of data governance[8], or does it risk duplicating efforts

[7] Regulation (EU) 2022/868, *supra nota* 6, Article 2 (16).
[8] Ferrè, G. R. (2023, April 26). Data donation and data altruism to face algorithmic bias for an inclusive digital healthcare. https://doi.org/10.15168/2284-4503-2624

already covered by the GDPR. This highlights the need for a critical examination of whether the introduction of the DGA and data altruism is truly warranted in the current regulatory landscape.

While the concept of data altruism holds considerable promise, certain complexities arise, particularly within the framework of GDPR. The DGA appears to contradict some fundamental principles outlined in the GDPR[9]. Notably, GDPR's Article 5 emphasizes that personal data should only be collected for specific, explicit, and legitimate purposes, with no further processing that is incompatible with these purposes[10]. Although exceptions are made for public interest data archiving, scientific research, and statistical applications, concerns arise regarding the reuse of personal data collected by public sector bodies under the DGA. There is apprehension about whether such data will be utilized in unexpected or potentially risky ways for the data subjects[11]. Moreover, while GDPR does not apply to anonymized data, the DGA's provision for data reuse within the extent of GDPR's purpose limitation hinges on the effective anonymization of the data. This underscores the critical importance of proper anonymization techniques in ensuring compliance and mitigating privacy risks within the context of data sharing under the DGA[12].

The research will primarily focus on the concepts outlined in the Data Governance Act, particularly concerning data altruism and data sharing in relation to GDPR and data portability principles. Given the novelty of this legislation, understanding its compliance and challenges is crucial. Furthermore, the examination will extend to successful cases such as Estonia's X-Road, a prime example of effective data sharing. By closely analyzing how X-Road operates in Estonia and its alignment with GDPR, the research aims to uncover any encountered challenges and the valuable lessons that can be drawn from its implementation. This is essential, especially considering the limited practice and research conducted in this field.

During the research, the examination of findings, contributions, and limitations will be conducted. This analysis will encompass insights gained, their relevance, and practical implications. Additionally, potential solutions to address these limitations or overcome identified challenges

[9] Ruohonen, J., & Mickelsson, S. (2023). Reflections on the Data Governance Act. Digital Society, 2(1). doi:10.1007/s44206-023-00041-7.
[10] 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, p. 1–88, Article 5
[11] Ruohonen, & Mickelsson, (2023), *supra nota* 9, p. 6.
[12] *Ibid.*

will be explored. This comprehensive discussion aims to enrich the research, providing a clear understanding of the topic. Moreover, the timeliness and relevance of the research topic to EU data governance and the addressed research problem justify its significance. The compliance challenges and potential solutions in the context of data altruism and GDPR under the DGA highlight a critical concern in the evolving data landscape, making this research both necessary and impactful.

1. Data Governance Act

Addressing the challenge of market dominance and fostering innovation necessitates the establishment of policies mandating the sharing of user information within data-driven markets. Despite existing legal frameworks such as those outlined in EU competition regulations and the General Data Protection Regulation (GDPR), their effectiveness in resolving this issue remains limited[13]. Therefore, there was a pressing need for the implementation of new regulations compelling companies to engage in data-sharing practices. However, the formulation of such regulations presented a multifaceted challenge, demanding a delicate balance between promoting efficiency and ensuring compliance with legal data-sharing requirements and individual privacy rights. This balance is crucial not only for ensuring the effectiveness of regulated data sharing but also for safeguarding the interests and rights of data subjects. Thus, it is imperative to create a governance structure that harmonizes these seemingly conflicting objectives to encourage a fair, competitive, and innovative data-driven market[14].

The discourse surrounding this topic is highly relevant, given the numerous challenges it presents, which have captured the attention of the European Commission. According to the European Commission's strategy on data, both businesses and the public sector within the EU can be empowered by using data to enhance decision-making processes[15].

The recognition of data as a fundamental resource for driving economic growth is widely acknowledged[16]. The value of data for social and economic advancement is underscored by its unique characteristics, such as its replicability at minimal cost and its non-exclusivity, allowing for simultaneous utilization by multiple entities without interference with each other[17]. To utilize this potential for increasing individual welfare and fostering economic and social development, it

[13] Graef, I., & Prüfer, J. (2021, November 1). Governance of data sharing: A law & economics proposal. Research Policy. https://doi.org/10.1016/j.respol.2021.104330.
[14] *Ibid.*
[15] A European strategy for data, Brussels, *supra nota* 3, p.1.
[16] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on Building a European Data Economy, COM (2017) 9 final (Jan. 10, 2017)
[17] A European strategy for data, Brussels, *supra nota* 3, p.5.

is imperative to prioritize the enhancement of data accessibility and its application[18], especially in today's digital era.

The European Union aims to promote an enabling policy environment productive to fostering the growth of the data economy. To a certain degree, the emphasis on the data economy was already discussed during the policy development process of the GDPR[19]. For numerous policymakers and stakeholders, the regulation was perceived as having dual objectives: safeguarding personal data while also promoting the movement of such data within the internal market[20]. Another noteworthy point to highlight is the incorporation of the data economy concept into the General Data Protection Regulation, specifically within the Article 20[21]. This article introduced a novel advantage for data subjects, granting them the right to transfer their personal data between different data controllers[22]. The primary objective behind this provision was to encourage improved data sharing and interoperability. However, in practical implementation, this right has posed several challenges, particularly concerning issues associated with data reuse[23]. It's essential to emphasize the significance of this article, as discussions regarding data reuse began long before its formal introduction[24].

By 2030, the aspiration is for the EU's share of the data economy—encompassing data storage, processing, and utilization—to align proportionally with its economic significance, organically driven by choice rather than regulatory imposition[25]. The goal of this attempt is the creation of a unified European data space. This space is envisioned to be inclusive of both personal and non-personal data, including sensitive business data, safeguarded against security and privacy risks[26].

An essential aspect of achieving this extensive vision lies in the implementation of legislation adapted to specific requirements, along with the establishment of robust governance frameworks aimed at guaranteeing the accessibility of data. This requires significant investments in the

[18] *Ibid.*
[19] König, P. D. (2022, January 1). Analyzing EU Data Governance Through the Lens of the Resource Regime Concept. https://doi.org/10.2139/ssrn.4050804.
[20] *Ibid.*
[21] Van Ooijen, I., & Vrabec, H. U. (2018, December 11). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. https://doi.org/10.1007/s10603-018-9399-7.
[22] Regulation (EU) 2016/679, *supra nota* 9, Article 20.
[23] Van Ooijen & Vrabec (2018, December 11), *supra nota* 21, p. 101-102
[24] *Ibid.*
[25] A European strategy for data, Brussels, *supra nota* 3, p.5
[26] *Ibid.*

development of standards, tools, infrastructure, guidelines, practices, and the necessary competencies for effective data management[27]. The success of these initiatives depends on striking a delicate balance between regulatory measures and fostering innovation. By providing a useful environment for businesses to develop while ensuring compliance with legal standards, an ecosystem can be fostered where data-driven advancements succeed, ultimately resulting in sustained economic growth, social benefit, and security.

Directive (EU) 2019/1024 and sector-specific Union laws aim to enhance the accessibility and reusability of data generated by public sector bodies[28]. However, certain types of data, such as commercially sensitive information, data regarding statistical confidentiality, and data protected by intellectual property rights, including personal data and trade secrets, are often not made available, even for research or innovative purposes in the public interest[29]. Despite the potential for such data to be utilized in accordance with relevant Union laws, including Regulation (EU) 2016/679 and Directives 2002/58/EC[30] and (EU) 2016/680[31], various technical and legal obstacles exist, requiring compliance with strict procedural requirements to safeguard rights and uphold fundamental principles such as non-discrimination, data protection, and security. Addressing these challenges typically demands considerable time and expertise.

Although certain Member States have taken steps to establish frameworks or enact legislation facilitating data reuse, uniform approaches are lacking across the Union. As previously mentioned, the reuse of data can indeed provide significant benefits. However, a critical issue lies in whether member states can effectively safeguard data reuse without compromising data protection and privacy rights. Building trust is essential for citizens to feel comfortable sharing their data, yet this is challenging given the frequency of data breaches despite theoretical safeguards being in place.

To promote the use of data for European research and innovation purposes by both public and private entities, it is imperative to establish clear and consistent conditions governing access to and utilization of such data throughout the Union[32].

[27] *Ibid*.
[28] OJ L 172, 26.6.2019, p. 56–83.
[29] Regulation (EU) 2022/868, *supra nota* 6, Recital (6)
[30] OJ L 201, 31.7.2002, p. 37–47.
[31] OJ L 119, 4.5.2016, p. 89–131.
[32] Regulation (EU) 2022/868, *supra nota* 6, Recital (6).

The necessity for standardized access conditions directly led to the adoption of the Data Governance Act by the European Union. The European Union is often criticized for its tendency towards overregulation, and while this may sometimes be the case, in the instance of the Data Governance Act, it may be said, that such regulation was not only justified but also crucial. Despite the significance of the Data Governance Act, issues persist regarding overlap with the GDPR. While the law frequently references the GDPR, particularly concerning the processing of personal data, it also introduces numerous new definitions not provided in the GDPR. In addition to the challenges with overlapping references to the GDPR, another issue arises concerning consent. While the definition of consent remains the same as in the GDPR, the Data Governance Act introduces different types of consent. This raises the question of whether it is truly necessary to implement a new form of consent when the GDPR already provides a framework. Instead of introducing a new consent form for the data altruism concept, it is worth considering whether the GDPR's consent provisions could be made more detailed to accommodate evolving data governance needs effectively. This approach could potentially streamline regulatory processes and enhance clarity for both data subjects and controllers. By creating more detailed and adaptable consent templates under the GDPR, individuals would have clearer options for consenting to different data uses, including altruistic purposes. However, the issue with this approach is that the GDPR consent form is already very detailed and it involves strict requirements for data processing.

It is also essential to delve into the interconnection between the Data Governance Act and the Data Act. The Data Act follows the European Data Governance Act, reflecting the EU's leadership in the data-driven society in order to achieve the goals set in the European Data Strategy[33]. It clarifies data value creation and access conditions, facilitating data sharing across different sectors. The DGA, designed to regulate data-sharing practices and foster responsible data use across various sectors, intersects with the Data Act, which specifically targets the regulation of data sharing within the context of the Internet of Things (IoT)[34]. These legislative initiatives align with the broader goal of promoting and developing a data economy within the EU by facilitating efficient and compliant data-sharing practices. The DGA introduces a legal framework for entities known as data intermediaries, aimed at streamlining the process of data sharing while ensuring adherence

[33] The European Data Act, Retrieved from:https://www.eu-data-act.com/.
[34] Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. https://doi.org/10.1016/j.clsr.2023.105830.

to legal and ethical standards. It was enacted to improve data sharing and utilization within the EU and provides a comprehensive framework for governing access to data while ensuring compliance with legal and ethical considerations. It sets forth guidelines for data intermediaries, establishes mechanisms for data sharing, and outlines procedures for resolving disputes and safeguarding rights. The DGA aims to create an atmosphere that encourages the access and use of data, thereby supporting research, innovation, and economic development across the European Union. Conversely, the draft Data Act focuses on regulating data-sharing practices within the IoT sector, addressing challenges related to data ownership, interoperability, and security unique to this area[35]. As mentioned before, the EU's introduction of numerous new legislations is aimed at achieving the goals outlined in the EU Data Strategy. The objective of this regulation is to encourage data sharing within the internal market by establishing a standardized legal framework for data exchanges, while still adhering to the principles outlined in the GDPR[36]. It's important to note that the DGA doesn't introduce novel methods of data processing, rather, it references the GDPR's existing regulations on data processing. While the intention is to ensure comprehensive data governance and protection, there is a risk of overregulation, which the EU has faced in some cases. This is particularly pertinent when dealing with emerging areas where practical implementation is yet to be established, leading to discussions based solely on theoretical evidence. In such instances, there is a possibility of overlapping regulations, which could potentially create complexities and challenges.

Article 1 of the Data Governance Act lays out the foundational principles and objectives of the regulation. Firstly, it establishes the conditions under which certain categories of data held by public sector bodies within the European Union can be reused. Additionally, it introduces a notification and supervisory framework for entities providing data intermediation services. Moreover, it outlines a framework for the voluntary registration of organizations that collect and process data for altruistic purposes, as well as the establishment of a European Data Innovation Board to promote innovation in data usage[37].

[35] *Ibid.*
[36] Bravo. (2022). Data Governance Act and Re-Use of Data in the Public Sector. European Review of Digital Administration & Law - Erdal, 3(2), 13–22.
[37] Regulation (EU) 2022/868, *supra nota* 6, Article 1.

This article clarifies that the regulation does not impose obligations on public sector bodies to permit data re-use nor does it exempt them from confidentiality obligations under Union or national law. It also specifies that certain provisions in Union or national law regarding data access and re-use will prevail, along with any sector-specific requirements[38]. This ensures that the regulation operates within the existing legal framework and respects confidentiality obligations and specific provisions in Union or national law.

Furthermore, the article emphasizes that Union and national laws concerning the protection of personal data apply to any personal data processed under this regulation. It ensures compliance with existing regulations such as Regulations (EU) 2016/679 (GDPR) and (EU) 2018/1725[39], and Directives 2002/58/EC and (EU) 2016/680. This underscores the importance of adhering to data protection laws and clarifies that the regulation does not create new legal bases for personal data processing. In addition, the regulation explicitly states that it does not affect the application of competition law. This ensures that competition law remains applicable and unaffected by the regulation[40].

Despite this, challenges regarding uniformity persist. While each member state has its own laws compliant with the GDPR and other regulations, the governance of data reuse within each remains uncertain. Furthermore, the non-obligatory nature of ensuring the reuse of data raises concerns about the efficacy of the DGA. The success of the DGA depends on member states' willingness to allow data reuse and incorporate mechanisms into their legal frameworks, as well as on the public's acceptance of data reuse, especially when it involves voluntary sharing with its risks. Addressing these concerns requires substantial efforts, including within member states to establish governance frameworks and communicate with citizens to assure them that data usage complies with GDPR. However, achieving this is challenging, as even with stringent data protection rules, complete safety is hard to achieve.

[38] *Ibid.*
[39] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1 OJ L 295, 21.11.2018, p. 39–98.
[40]Regulation (EU) 2022/868, *supra nota* 6, Article 1.

In contrast to GDPR, the Data Governance Act extends beyond personal data to encompass data in general. It introduces the concept of a "data holder," described as a legal entity, including public sector bodies and international organizations, or a natural person who is not the subject of the data in question. This data holder possesses the authority, as per applicable Union or national law, to grant access to or share certain personal or non-personal data[41]. Also, it is essential to discuss the connection of definitions with other regulations. The definition of 'data' provided in the EU Regulation on the free flow of non-personal data and the Data Governance Act appears similar at first glance, but the subtle differences between the two definitions could potentially lead to confusion or misunderstanding, particularly regarding the scope and applicability of the regulations. In the EU Regulation on the free flow of non-personal data, 'data' is defined as all data other than personal data as defined in Article 4(1) of the GDPR[42]. This definition essentially excludes personal data from its scope, focusing solely on non-personal data. On the other hand, under Article 2 of the Data Governance Act (DGA), 'data' is defined more broadly as any digital representation of acts, facts, or information, including compilations of such data in various formats such as sound, visual, or audiovisual recordings. Article 2(1) of the Data Act adopts the same broad definition of data as found in the Data Governance Act and Digital Markets Act. Additionally, it introduces specific definitions, such as product data and related service data, which are included within its context[43]. This definition encompasses a wider range of data types, including both personal and non-personal data. The potential for confusion or misunderstanding arises from the fact that the DGA's definition of 'data' is broader and more inclusive compared to the definition provided in the EU Regulation on the free flow of non-personal data. While the DGA acknowledges the existence of personal data within its definition of 'data,' the EU Regulation focuses solely on non-personal data, which may lead to confusion regarding the regulatory scope and requirements applicable to different types of data. This difference in definitions could create challenges in interpreting and applying the regulations, particularly in situations where both personal and non-personal data are involved. It may also affect compliance efforts and regulatory

[41] Regulation (EU) 2022/868, *supra nota* 5, Article 2 (8).
[42] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) OJ L 303, 28.11.2018, p. 59–68, Article 2(1).
[43] Mylly, U. M. (2024). Trade Secrets and the Data Act. IIC - International Review of Intellectual Property and Competition Law. https://doi.org/10.1007/s40319-024-01432-0.

enforcement, as organizations may struggle to determine which regulations apply to their data processing activities.

The Data Governance Act not only establishes rules for voluntary data sharing but also introduces new concepts such as data altruism. Data sharing, as defined in Article 2(10), involves the provision of data by a data subject or holder to a data user for joint or individual use, based on voluntary agreements or legal frameworks, either directly or through intermediaries. This sharing can occur under various arrangements, including open or commercial licenses, whether subject to a fee or free of charge[44]. In parallel, data altruism, outlined in Article 2 (16), entails the voluntary sharing of data with the consent of data subjects or permissions from data holders. This sharing is motivated by contributing to objectives of general interest as specified in national laws, such as healthcare, climate change mitigation, mobility improvement, statistical dissemination, public service enhancement, policy-making support, and scientific research facilitation[45].

Article 3 of the Data Governance Act involves the categories of data eligible for reuse, offering a structured framework for data accessibility and utilization. The regulation applies to data maintained by public sector entities that are safeguarded under various grounds such as commercial confidentiality, statistical confidentiality, protection of intellectual property, and protection of personal data[46]. This inclusivity ensures that personal data held by public sector bodies falls within the purview of the regulation, thereby aligning with the principles and regulations outlined in the General Data Protection Regulation[47]. Additionally, certain exclusions are outlined to clarify the scope of the regulation. These exclusions encompass data held by public undertakings, public service broadcasters and their subsidiaries, cultural establishments, and educational institutions[48]. The positive aspects of these provisions lie in their comprehensive approach to regulating data reuse while simultaneously safeguarding sensitive information and upholding data protection standards. By encompassing a wide range of data categories, including personal data, the regulation promotes transparency and accountability in data management practices within the public sector. Furthermore, the illustration of exclusions ensures clarity regarding the application of the regulation, preventing ambiguity and potential misuse of data.

[44] Regulation (EU) 2022/868, *supra nota* 6, Article 2 (10).
[45] Regulation (EU) 2022/868, *supra nota* 6, Article 2 (16).
[46] Regulation (EU) 2022/868, *supra nota* 6, Article 3(1).
[47] Ruohonen & Mickelsson, S. (2023), *supra nota* 9, p. 3.
[48] Regulation (EU) 2022/868, *supra nota 6*, Article 3 (2).

Nevertheless, the practical implementation remains largely theoretical, and the effectiveness of these measures in practice is yet to be seen. While safeguards are theoretically in place, the question of their reliability and trustworthiness remains unanswered.

Under Article 5 of the Data Governance Act, the conditions for data reuse are defined, setting forth a comprehensive framework to regulate the utilization of data resources within the European Union. The article includes several fundamental principles, including non-discrimination, transparency, proportionality, and proper justification, aimed at fostering access to data while preserving competition[49]. Additionally, it mandates public sector bodies to implement stringent measures to protect data privacy and confidentiality. This includes the requirement for proper anonymization of personal data and the careful handling of commercially sensitive information through appropriate modification or aggregation techniques[50]. Furthermore, Articles 7 and 12 of the Data Governance Act continue to address the concept of pseudonymization. Additionally, recital 15 emphasizes that the reuse of pseudonymized data may be permissible, as long as it ensures the impossibility of re-identifying data subjects[51].

To assist public sector bodies in fulfilling their newly assigned responsibilities, Article 7 of the Data Governance Act mandates that member states designate specific competent bodies. These designated bodies are tasked with providing support in various areas, including offering technical guidance on data storage and processing, aiding in anonymization, suppression and other privacy-enhancing techniques to safeguard personal data[52]. While public authorities have obligations outlined in the Data Governance Act, Article 6 allows public sector bodies to charge fees for granting permission for the reuse of data within their possession[53].

While the Data Governance Act aligns well with the European data strategy and aims to support the data economy, it faces several challenges that require attention. One notable concern is the potential conflict between the DGA and certain fundamental principles outlined in the General Data Protection Regulation. Specifically, Article 5 of the GDPR stipulates that personal data should only be collected for specified, explicit, and legitimate purposes, and not further processed

[49] Regulation (EU) 2022/868, *supra nota 6*, Article 5.
[50] *Ibid.*
[51] Ruohonen & Mickelsson, (2023), *supra nota* 9, p. 6.
[52] Regulation (EU) 2022/868, *supra nota 6*, Article 7.
[53] Regulation (EU) 2022/868, *supra nota* 6, Article 6.

in a manner incompatible with those purposes. Although exceptions exist for public interest data archiving, scientific research, and statistical applications, the goal of public sector data reuse under the DGA raises apprehensions about whether personal data collected by public sector bodies will be used unexpectedly or pose risks to data subjects[54]. In this case, the primary concern lies in the adequacy of mechanisms for safeguarding data usage and trust in data sharing. Especially in light of recent findings regarding the European Commission's infringement of data protection rules when using Microsoft 365[55]. Despite the specific concerns about data sharing outside the EU, this case underscores broader questions about safeguarding data usage. When a prominent institution like the European Commission encounters such challenges, it raises doubts about the adequacy of mechanisms for sharing and reusing data across all member states, particularly when such reuse is intended for the public good. The findings by the European Data Protection Supervisor (EDPS) highlight deficiencies in ensuring appropriate safeguards and specifying data usage in contracts, which are fundamental aspects of data protection compliance[56]. This raises concerns about whether similar issues may arise at the national level and whether existing mechanisms are robust enough to prevent such infringements, especially in connection with new legislation, when there is no sufficient practice or expertise.

Additionally, the DGA's provision for data reuse under the GDPR's purpose limitation hinges on proper anonymization, given that the GDPR does not apply to anonymized data[57]. Another concern pertains to the increased responsibilities placed on national data protection authorities under the DGA[58]. In cases where providing anonymized or modified data does not meet the re-user's requirements, and provided that any necessary data protection impact assessment has been conducted and the supervisory authority has been consulted as per Articles 35 and 36 of Regulation (EU) 2016/679, public sector bodies may permit the on-premise or remote reuse of data within a secure processing environment, if the risks to data subjects' rights and interests are deemed minimal. This arrangement is particularly suitable for the reuse of pseudonymized data. In such secure processing environments, data analyses should be supervised by the public sector body to

[54] Ruohonen, & Mickelsson (2023), *supra nota* 9, p. 6.
[55]European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en.
[56] *Ibid.*
[57]Ruohonen, & Mickelsson (2023), *supra nota* 9, p. 6-7
[58] *Ibid.*

safeguard the rights and interests of third parties. Specifically, personal data should only be transmitted to a third party for reuse if there is a legal basis under data protection law permitting such transmission. Non-personal data should only be transmitted if there is no risk of identifying data subjects through the combination of non-personal datasets[59]. This requirement also extends to pseudonymized data that still qualify as personal data. In the event of data subjects being re-identified, there should be an obligation to notify the public sector body of such a data breach, in addition to notifying the supervisory authority and the data subjects themselves in accordance with Regulation (EU) 2016/679.[60] However, given the existing challenges concerning resourcing, coordination, and other issues faced by European data protection authorities[61], concerns persist regarding the effective administration and enforcement of the DGA.

While the Data Governance Act is undoubtedly necessary, it's crucial not to overlook the significance of the General Data Protection Regulation. The GDPR serves as a fundamental regulation governing the use and processing of personal data, outlining the rights of data subjects. The Data Governance Act functions alongside the GDPR without modifying its scope, allowing both regulations to operate simultaneously. Nonetheless, as certain elements of the DGA have implications for personal data, its provisions are designed to fully comply with data protection laws and enhance individuals' authority over their data[62]. This is particularly crucial for regulations like the Data Governance Act, which are relatively new and lack extensive practical implementation or case law.

Therefore, it's essential to ensure alignment with the GDPR. To ensure compliance with GDPR and clarity in the provisions of the Data Governance Act, several approaches can be adopted, with a focus on defining key terms. Firstly, it's crucial to define what falls under "general interest." While Recital 45 of the DGA provides examples such as healthcare, combating climate change, and supporting scientific research[63], there remains a need for a comprehensive definition to address scenarios where data usage extends beyond these examples. This definition should clarify the

[59] Regulation (EU) 2022/868, *supra nota* 6, Recital 15.
[60] *Ibid.*
[61] Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at glance. https://doi.org/10.1016/j.is.2021.101876.
[62] Garske, B., Holz, W., & Ekardt, F. (2024). Digital twins in sustainable transition: exploring the role of EU data governance. Frontiers in Research Metrics and Analytics, 9. https://doi.org/10.3389/frma.2024.1303024.
[63] Regulation (EU) 2022/868, *supra nota* 6, Recital 45.

scope of activities considered to be in the general interest and provide clarity to data subjects about the purposes for which their data may be used. Additionally, it's essential to distinguish between the definitions of "public interest" in the GDPR and "general interest" in the DGA. While they may overlap in some aspects, they may also encompass different concepts and objectives. Clear differentiation between these terms is necessary to avoid confusion and ensure that data subjects understand the specific interests for which their data is being utilized.

Also, the issue of consent forms under the Data Governance Act (DGA) raises questions about the necessity of introducing a new form when the GDPR already establishes consent practices, which will be further discussed in the research. It is essential to avoid overlap between the two regulations. However, the lack of practical experience with the new consent form provided by the DGA presents a significant challenge. Without established practices, implementing and evaluating the effectiveness of the new consent form remains uncertain. Thus, reconciling the need for clarity and specificity in consent practices with practical considerations poses a considerable challenge in the context of data governance. In this case, it is of utmost importance to discuss what can be potential solutions. One of the essential aspects can be implementing the context of dynamic consent in the data altruism consent form. Dynamic consent is a participant-based approach, which is personalized in order to provide greater engagement for clinical and research purposes[64]. The dynamic part of this consent form involves over-time interaction, which means that participants give and revoke consent based on their changed circumstances. This allows the participant to change their consent according to their preferences. Thus, it means that dynamic consent form choices are adaptable and can change over the time[65]. In this context, the consent process is not restricted by the limitations of the paper-based consent form. Implementing a technology-based platform provides flexibility. Participants can consent to various sample and data uses, for separate case-based approvals, or establish exact preferences for different research contexts[66]. Dynamic informed consent has the capacity to encourage participant engagement by allowing individuals to express their preferences effectively. This can be facilitated by offering easily comprehensible versions of consent following study amendments, or by providing a simplified overview of the

[64] Kaye, J., Whitley, E. A., Lund, D. J., Morrison, M., Teare, H., & Melham, K. (2014, May 7). Dynamic consent: a patient interface for twenty-first century research networks. https://doi.org/10.1038/ejhg.2014.71.
[65] *Ibid.*
[66] Kaye, Whitley, Lund, Morrison, Teare, & Melham, K. (2014, May 7), *supra nota* 64, p. 142.

main findings[67]. In the context of data altruism, this approach can offer multiple advantages. Primarily, it enhances transparency, ensuring that individuals who willingly share data possess a comprehensive understanding of its intended use. Furthermore, it promotes accessibility and simplicity by allowing participants the flexibility to modify their consent at any time or provide consent for different aspects of the research separately. Additionally, participants receive information about research outcomes, fostering trust in the process and encouraging continued data sharing in the future.

Furthermore, Data altruism and the Data Governance Act may present challenges in compliance with GDPR principles such as purpose limitation and data minimization. The broad concept of "common interest" associated with data altruism can lead to the collection and sharing of more data than is strictly necessary, potentially conflicting with the principle of data minimization. Therefore, stricter rules governing data sharing and handling are essential to ensure that only data relevant to the specified altruistic purpose is processed. Moreover, it's crucial to establish clear distinctions between data altruism and data portability to avoid ambiguity. While both concepts involve the sharing of data, they serve different purposes and operate within distinct frameworks. Data altruism typically involves the voluntary sharing of data for social benefit[68], whereas data portability focuses on individuals' rights to transfer their own data between services[69]. Understanding the relationship between these concepts is vital to ensure compliance with regulations and prevent unintended overlap or confusion in their implementation.

Data sharing is indeed essential, but it's imperative to explore and research its compliance with the GDPR, along with identifying challenges and potential issues. This research is highly pertinent and timely in ensuring legal and ethical compliance within the evolving data governance landscape.

[67] De Sutter, E., Barbier, L., Borry, P., Geerts, D., Ioannidis, J. P. A., & Huys, I. (2024, January 1). Personalized and longitudinal electronic informed consent in clinical trials: How to move the needle? https://doi.org/10.1177/20552076231222361.
[68] Regulation (EU) 2022/868, *supra nota* 6, Article 2 (16).
[69] Regulation (EU) 2016/679, *supra nota* 10, Article 20.

2. Data Altruism Concept

The DGA governs a range of activities including facilitating the sharing of data for reuse, providing data intermediation services, promoting data altruism, and implementing measures to safeguard data protection and commercial confidentiality. These responsibilities go beyond the conventional purview of data protection outlined in the GDPR[70]. Aligned with the principles outlined in Recital 35 of the Data Governance Act, there is a clear potential for utilizing data voluntarily, by individuals, with their informed consent, to serve broader social goals. These goals may include improving healthcare, addressing climate change, enhancing transportation systems, refining statistical datasets, bettering public services, and shaping evidence-based public policies[71], while also encouraging technological development. Additionally, supporting scientific research is highlighted as another important aspect. The legislative aim is to encourage the development of large data pools sourced from altruistic contributions, which can then be used for robust data analysis and machine learning across Europe[72].

To achieve this goal, Member States are given the flexibility to establish frameworks that promote data altruism. This could involve making it easier for people to give consent for their data to be used altruistically, running awareness campaigns, and facilitating discussions between different institutions to identify how public policies can benefit from this type of data sharing. Consequently, Member States are empowered to create national strategies outlining their approach to data altruism[73]. However, the diversity of data types, influenced by varying national traditions, can be a challenge[74].

However, it's essential to acknowledge some criticisms as well. One concern is that relying solely on altruism may not encourage enough people to participate, since data-sharing is voluntarily based it can potentially limit the creation of large data pools. This means that not everyone may be willing to share their data. For instance, certain findings suggest that people's willingness to share data can depend on whether the information's disclosure is seen as potentially stigmatizing

[70] Pathak, M. (2024). Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act. Social Science Research Network. https://doi.org/10.2139/ssrn.4718891.
[71] Regulation (EU) 2022/868, *supra nota 6*, Recital 45.
[72] *Ibid.*
[73] Regulation (EU) 2022/868, *supra nota 6*, Recital 45.
[74] *Ibid.*

or harmful. Additionally, concerns about data management and security are widespread, with worries about inappropriate access or leakage[75].

It is imperative to understand the broader framework outlined in the Data Governance Act, particularly under Article 16. This provision stipulates that Member States have the authority to establish organizational or technical frameworks to facilitate data altruism. Consequently, Member States are empowered to develop national policies governing data altruism, which may include provisions to support individuals in voluntarily sharing their personal data held by public sector entities for altruistic purposes. These policies are instrumental in providing necessary information to data subjects regarding the reuse of their data for the common good[76].

The Data Governance Act prioritizes the altruistic reuse of data and the establishment of trustworthy data intermediaries. These intermediaries are distinguished by their role as impartial facilitators, refraining from data analysis and serving solely as a way for data exchange between holders and users. They do not engage in data analysis to maintain impartiality and build trust among stakeholders[77]. Instead, their primary function is to enable seamless communication and collaboration between data holders and users, thereby fostering a conducive environment for data sharing and utilization in compliance with regulatory standards[78]. However, to effectively uphold the principles of data altruism and governance, it is imperative to employ specialized methodologies and address inquiries. This entails prioritizing transparency regarding the origins of datasets and exploring potential measures to safeguard sensitive data[79]. Studies have identified a concerning lack of awareness among individuals regarding various aspects of data governance, including specific disease registries, the presence of databases derived from general practice, the contents of electronic health records, anonymization procedures, data sharing protocols, and the nature of data used in research endeavors[80]. This limited awareness poses a significant challenge

[75] Skovgaard, L. L., Wadmann, S., & Hoeyer, K. (2019). A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. Health Policy, 123(6), 564–571. https://doi.org/10.1016/j.healthpol.2019.03.012.
[76] Regulation (EU) 2022/868, *supra nota* 6, Article 16.
[77] Esteves, B., Rodríguez-Doncel, V., Pandit, H. J., & Lewis, D. (2023, September 11). Semantics for Implementing Data Reuse and Altruism Under EU's Data Governance Act. https://doi.org/10.3233/ssw230015.

[78] *Ibid.*

[79] Judyta Lubacha, Mäihäniemi, B., & Rafał Wisła. (2023). The European Digital Economy (pp. 161–185). Taylor & Francis.
[80] Skovgaard, Wadmann & Hoeyer (2019), supra nota 75, p. 566.

to the effective implementation of initiatives such as the Data Governance Act and the concept of data altruism. If individuals are not adequately informed about the existence and functioning of data governance frameworks and data altruism initiatives, they may be hesitant to share their data due to concerns about privacy, security, and misuse. This lack of trust and understanding hampers the applicability of data altruism, as people may be reluctant to participate in data-sharing initiatives if they are unsure about the safeguards in place to protect their data.

As mentioned before, Article 2(10) of the Data Governance Act defines data altruism as the voluntary consent of individuals to allow their personal data or the permission of other data holders to use their non-personal data without seeking compensation. This is to advance general interests, such as scientific research or improve public services[81]. While Recital 35 of the DGA lists examples of general interest purposes, it lacks explicit definitions. In contrast, GDPR Recital 159 clarifies scientific research purposes, covering technological development, fundamental research, and studies benefiting public health. Given the close relationship between the GDPR and the DGA, it's reasonable to apply the GDPR's interpretation of scientific research purposes to the DGA. consistency across both regulations is crucial for EU legislation and cross-border research facilitation. Similarly, general interest should be broadly interpreted in alignment with the DGA's goals and Recital 35 examples[82].

In general, Altruistic data sharing holds significance not just in the context of data owners' control and governance but also in its potential impact on advancing data analytics and machine learning systems through the aggregation of extensive datasets[83]. This implies that when individuals or entities contribute their data selflessly, it not only influences how data is managed and overseen but also contributes significantly to the enhancement and evolution of analytical and learning systems that rely on large amounts of data for their operation[84]. Various actors may interpret the significance and potential hazards of collecting, sharing, and reusing data differently. These variations could stem from their roles, specific contextual understanding, or personal perceptions.

[81] Regulation (EU) 2022/868, *supra nota* 6, Article 2 (10).
[82] Kruesz, C., & Zopf, F. (2021). European Union · the concept of data altruism of the draft DGA and the GDPR: Inconsistencies and why a regulatory sandbox model may facilitate data sharing in the EU. European Data Protection Law Review, 7(4), 569–579. https://doi.org/10.21552/edpl/2021/4/13
[83] Ferrè (2023, April 26), *supra nota* 8, p.126.
[84] *Ibid.*

Consequently, the value and risk associated with data are subjective and contingent upon the viewpoints of the involved parties[85]. But the issue is, that DGA fails to offer definitive guidelines regarding the process of donating to data altruism organizations or specifying the subsequent utilization of data. This ambiguity leads to hesitation among prospective data altruism organization creators, data providers, and users due to uncertainties surrounding associated risks and expenses. Regulatory gaps contribute to the absence of legal clarity and compliance expenses, particularly concerning the application of GDPR in cases involving the sharing of personal data for public interest purposes. These uncertainties pose reputational and financial risks, thereby dissuading potential data providers[86]. It is essential for individuals who donate data to have clear guidelines in place. These guidelines should encompass various aspects, such as facilitating data interpretation, supporting donors in reassessing their participation and defining their boundaries and creating opportunities for donors to understand the value of their contribution[87]. Furthermore, throughout the data donation process, donors should be actively involved in contributing to research efforts. Therefore, it is recommended that they have the opportunity to explore their personal data and acquire contextualized knowledge about its contents. Additionally, donors should receive information that helps them understand the purpose behind their data donation, how their data will be processed, how they can access their data, and what specific data they are contributing. This awareness is essential to ensure that donors are fully informed and empowered throughout the data donation process[88], which will also ensure transparency.

According to DGA, to facilitate the gathering of data through the principle of data altruism, the Commission must create implementing acts that introduce and refine a standardized European data altruism consent form. This consent form will adopt a modular structure, enabling customized adaptations to suit various sectors and objectives[89]. Furthermore, when personal data is involved, the European data altruism consent form will guarantee that individuals can provide and revoke

[85] Grafenstein, M. (2022). Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4104502.
[86] Finck, M., & Mueller, M.-S. (2023). Access to Data for Environmental Purposes: Setting the Scene and Evaluating Recent Changes in EU Data Law. *Journal of Environmental Law*, 35(1), 109–131. https://doi.org/10.1093/jel/eqad006.
[87] Gomez Ortega, A., Bourgeois, J., Hutiri, W. T., & Kortuem, G. (2023). Beyond data transactions: a framework for meaningfully informed data donation. *AI & SOCIETY*. https://doi.org/10.1007/s00146-023-01755-5.
[88] *Ibid.*
[89] Regulation (EU) 2022/868, *supra nota* 6, Article 25 (1).

consent for a particular data processing activity. This process must adhere to the stipulations outlined in GDPR[90].

However, the DGA does not explicitly clarify whether this consent mechanism should be viewed as an additional requirement for legitimate data exchange and processing or as an alternative model of consent specifically for activities serving the general interest. It's important to note the contrast between the DGA and the GDPR regarding the definition of consent[91]. Under Article 4 of GDPR consent is an expression of the data subject's wishes, freely provided, clearly defined, well-informed, and unambiguous, demonstrating their agreement to the processing of personal data about themselves, either through a statement or through a clear affirmative action[92]. This discrepancy underscores the need for further clarification and alignment between the DGA's provisions and the established principles of consent outlined in the GDPR[93].

There's a growing concern about the efficacy of the data altruism provisions as outlined in the Data Governance Act to truly stimulate data altruism. The existing evidence doesn't convincingly demonstrate that these provisions will effectively encourage individuals and organizations to share their data for altruistic purposes[94]. Consequently, it's imperative to explore alternative approaches to foster a culture of data altruism. One crucial aspect is the exchange of information and practices related to data altruism. While the GDPR has established practices regarding the use of data, there's a need for clarity and awareness specifically regarding data altruism. Individuals and organizations need to understand the concept and be assured that their rights will be respected. Since data altruism is closely related to the GDPR, informational exchange between data altruism organizations and data protection authorities can be highly beneficial. Additionally, considering the GDPR exemptions regarding the reuse of data for research purposes, sharing information between these entities can facilitate better compliance and understanding, ultimately promoting responsible data-sharing practices[95]. Collaboration between data protection authorities (DPAs) and data altruism organizations is essential for ensuring compliance with data protection regulations.

[90] Regulation (EU) 2022/868, *supra nota* 6, Article 25 (3).
[91] Vardanyan, L., & Kocharyan, H. (2022). The GDPR and the DGA proposal: Are they in controversial relationship? European Studies, 9(1), 91–109. https://doi.org/10.2478/eustu-2022-0004.
[92] Regulation (EU) 2016/679, *supra nota* 10, Article 4 (11).
[93] Vardanyan & Kocharyan (2022), *supra nota* 91, p. 99-100.
[94] Finck & Mueller (2023), supra nota 86, p. 128.
[95] Kruesz & Zopf (2021), *supra nota* 82, p. 576-577.

DPAs can share vital information and provide educational resources to help organizations understand and adhere to these regulations effectively, especially regarding data handling. This exchange enables organizations to stay updated on legal requirements and best practices, promoting consistency and effectiveness in data management. This is particularly relevant in terms of data processing and data anonymization, as the DGA does not introduce new rules in this regard, and processing will continue to be governed by the GDPR. Furthermore, DPAs and data altruism organizations can collaborate to develop guidelines and standards for responsible data sharing and donation practices. This joint effort considers both legal requirements and ethical considerations, promoting transparency, accountability, and trust in data-sharing initiatives.

In summary, Data altruism is a key component of the Data Governance Act, demanding discussion at the most authoritative levels. Accessing valuable insights, hinges upon the establishment of a robust data infrastructure[96]. This infrastructure necessitates well-organized data sources that can be readily accessed by authorized individuals for their intended purposes[97]. Currently, many aspects of this framework remain unclear. Due to the recent application of the legislation, there is a lack of established practice or relevant literature. Nevertheless, the objective of this research is to identify the main challenges, particularly regarding compliance with the General Data Protection Regulation and to explore similar successful examples.

[96] Kamocki, P., Linden, K., Puksas, A., & Kelli, A. (2023). EU Data governance act: Outlining a potential role for Clarin. Linköping Electronic Conference Proceedings. doi:10.3384/ecp198006.
[97] Iphofen, R., & O'Mathúna, D. (2021). Ethical Issues in Covert, Security and Surveillance Research. Emerald Group Publishing, p 93-119.

3. Data Altruism Concept and GDPR

The notion of data altruism remains in its early stages of development, with limited practical implementations. A scholarly examination is warranted to assess the extent to which data altruism aligns with the regulatory framework included in the General Data Protection Regulation. Thus, it's imperative to determine the compatibility between the concept of data altruism and the principles mandated by GDPR.

The concentration of control over personal data processing threatens people's privacy by reducing transparency and hindering their access to their own information. To safeguard privacy, individuals should have more control over their data, as emphasized in regulations like the GDPR[98]. This control not only protects privacy but also promotes a culture of data altruism. As previously mentioned, data altruism plays a significant role in facilitating research by allowing the sharing of data for the common good and general interest.

It should be noted that concerning anonymized statistics, GDPR is seen as advantageous because it promotes and defines the sharing of anonymized data. While GDPR imposes strict regulations on sharing identifiable data, it does not impede the sharing of anonymized data[99]. On the contrary, while the Data Governance Act encompasses various types of data, including personal and non-personal data, there exists potential ambiguity regarding the classification of non-personal data.[100] The DGA lacks detailed definitions regarding non-personal data, which may lead to uncertainty regarding its interpretation and application. According to Article 2 of the DGA, non-personal data is defined as data that does not qualify as personal data under the GDPR. To ensure alignment with the GDPR and establish robust safeguards and measures for anonymization of data, it is imperative to have comprehensive definitions in place within the DGA. Detailed definitions would help avoid misunderstandings and ensure clarity in distinguishing between different categories of data, including non-personal data and anonymized data. However, it is imperative to delve into whether

[98] Zichichi, M., Ferretti, S., D'Angelo, G., & Rodríguez-Doncel, V. (2022). Data governance through a multi-DLT architecture in view of the GDPR. Cluster Computing. https://doi.org/10.1007/s10586-022-03691-3.
[99] Vukovic, J., Ivankovic, D., Habl, C., & Dimnjakovic, J. (2022). Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. Archives of Public Health, 80(1). https://doi.org/10.1186/s13690-022-00866-7.
[100] Skovgaard, Wadmann, & Hoeyer (2019), *supra nota* 75.

GDPR permits such data sharing for research purposes and how it intersects with data altruism, potentially resulting in overlapping or complementary frameworks.

Under Recital 157 of the GDPR personal data can be processed for scientific research purposes, However, this processing must adhere to appropriate conditions and safeguards established by Union or Member State law[101]. Recital 159 of GDPR clarifies that the Regulation applies to the processing of personal data for scientific research, covering a wide range including technological development, fundamental and applied research, and privately funded efforts. This interpretation also aligns with the EU's goal of establishing a European Research Area.

Scientific research purposes include studies conducted in the public interest, particularly in public health. Specific conditions regulate the processing of personal data for research, especially regarding data publication or disclosure. If scientific research, particularly in health, requires further actions in the interest of data subjects, the Regulation's general rules should be applied to facilitate those measures[102]. This objective is manifested through the provision of several legitimate bases for processing special categories of data in research contexts, such as obtaining consent, addressing serious cross-border health risks, and conducting research activities[103]. However, it should be noted that the Data Governance Act does not explicitly cover the sharing of health-related data[104]. Health data carries particularly sensitive information about individuals' well-being and medical history, making its handling and sharing subject to higher protection measures. Data altruism involves the voluntary sharing of personal data, including health data, for research or public interest purposes. Therefore, clear and comprehensive definitions and guidelines are crucial to protect individuals' privacy rights, foster trust, and promote responsible data-sharing practices.

The legitimate bases provided by the GDPR for processing personal data in research can be combined with specific rules designated for research activities, commonly known as research exceptions. These exceptions encompass provisions that guarantee alignment with the principle of purpose limitation, exceptions from certain general principles like data storage limitations, and

[101] Regulation (EU) 2016/679, *supra nota* 10, Recital 157.
[102] Regulation (EU) 2016/679, *supra nota* 10, Recital 159.
[103] Schneider, G., & Comandè, G. (2021). Can the GDPR make data flow for research easier? yes it can, by differentiating! A careful reading of the GDPR shows how EU Data Protection Law leaves open some significant flexibilities for data protection-sound research activities. SSRN Electronic Journal. doi:10.2139/ssrn.3795554.
[104] Skovgaard, Wadmann, & Hoeyer (2019), *supra nota* 75.

exemptions from specific rights of data subjects, such as the right to erasure and the right to access[105]. Article 89 of the GDPR holds significance in overseeing the processing of personal data for research purposes. It provides a framework that permits specific exemptions from certain rights of data subjects, such as the right to object to processing activities, as allowed by national laws. Simultaneously, Article 89 mandates the implementation of organizational and technical measures to safeguard the rights of data subjects[106].

In general, under Article 6 of the GDPR, processing of personal data is only lawful if at least one of the specified conditions is met, with consent being a common prerequisite for data processing[107]. However, exemptions exist under Article 9 for certain purposes, such as research. Recital 33 of the GDPR recognizes the difficulty in obtaining specific consent for scientific research due to the dynamic nature of research activities[108]. As a solution, it permits the concept of broad consent, where individuals can consent to certain areas of scientific research in line with ethical standards. When discussing GDPR exemptions, it's pertinent to consider the European Health Data Space (EHDS). The concept of secondary uses is elaborated in Article 2(2)(e) in conjunction with Article 34 of the EHDS. Article 34 of the EHDS outlines various purposes for processing data in the context of Big Data, including public health care, regulatory activities, scientific research, development, innovation activities, training, testing, and evaluation[109]. However, Article 35 of the draft EHDS lists prohibited purposes for secondary uses, such as decisions to the harm of individuals, amending insurance contracts, healthcare advertising or marketing, unauthorized disclosure to third parties, and developing and marketing illegal or immoral products, particularly drugs[110].

Despite this allowance, concerns arise regarding the GDPR's requirement for specific consent when the purposes of data processing are uncertain[111]. The European Data Protection Board

[105] Schneider & Comandè (2021), *supra nota* 103, p. 3.
[106] Shabani, M., & Yilmaz, S. (2022). Lawfulness in secondary use of health data: Interplay between three regulatory frameworks of GDPR, DGA & EHDS. Technology and Regulation, 2022, 128–134. https://doi.org/10.26116/techreg.2022.013.
[107] Regulation (EU) 2016/679, *supra nota* 10, Article 6 (1).
[108] Regulation (EU) 2016/679, *supra nota* 10, Recital 33.
[109] Denga, M., & Hoffmann, T. (2023). The Estonian Electronic Health Record – a Prototype for Data governance in the European Health Data Space? European Health & Pharmaceutical Law Review, 7(1), 5–15. https://doi.org/10.21552/ehpl/2023/1/4.
[110] *Ibid.*
[111] Shabani & Yilmaz (2022), *supra nota* 106, p. 129-130.

(EDPB) maintains that organizations must still strive to obtain specific consent whenever feasible. Specific consent ensures individuals are fully informed and retain control over their data usage, safeguarding against potential misuse[112]. This leads us to the principles of purpose limitation and data minimization. According to Article 5 of the GDPR, data controllers must comply with specific requirements. Personal data must be processed lawfully, fairly, and transparently[113]. It should be collected for specified, explicit, and legitimate purposes, adhering to the principle of purpose limitation. Additionally, the data collected must be adequate and necessary for the intended purposes, aligning with the principle of data minimization. While it's acknowledged that defining research purposes and specifying the use of data for public or general interests can be challenging, there remains a potential to exceed these boundaries. This presents a dilemma, particularly concerning the protection of data subjects' rights, as it is their data being utilized. Ambiguity in regulations can lead to uncertainty and potential misuse of personal data. Therefore, regulations should prioritize the interests of data subjects to ensure clarity and transparency in data usage. Implementing data protection impact assessments specifically customized for data altruism initiatives could help mitigate risks and ensure compliance with data protection regulations. Moreover, it's crucial to note that while the Data Governance Act touches upon the data protection impact assessment in its recitals, it does not explicitly address it within the main text. Given the broad purposes for which personal data may be utilized within data altruism initiatives, it would be highly beneficial to include explicit provisions within the DGA.

Purpose limitation principle is one of the fundamental principles outlined in the GDPR, thus it should be stated that the specification of the purpose isn't the sole factor determining whether there's a specific or nonspecific risk involved. Even if the controller misstates its purpose, failing to accurately identify the real risk posed by its processing to an individual's fundamental rights, it's still possible to assess the actual specific risk based on other factors in the case, such as the nature of the data and the processing context. However, the purpose outlined by the controller remains a crucial indicator, primarily establishing a causal link between data processing and potential harm to an individual's exercise of fundamental rights.[114] This emphasizes the significance of clearly defining the purpose of data processing, even in the presence of stringent

[112] *Ibid.*
[113] Regulation (EU) 2016/679, *supra nota* 10, Article 5.
[114] Von Grafenstein, M. (2021). Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II. European Data Protection Law Review, 7(2), 190–205. https://doi.org/10.21552/edpl/2021/2/8.

consent regulations. Ensuring that data subjects understand how their data is utilized and preventing any misuse of their information is paramount. This is particularly crucial in the context of data altruism, where trust is fundamental as data is shared voluntarily. Those contributing their data must have confidence that it will be handled accurately, highlighting the utmost importance of transparency.

Furthermore, adhering to the principle of data minimization is essential, considering the challenges associated with managing large volumes of data. Additionally, in research contexts, where data is utilized for public good and general interest, it must be directly relevant to the intended purpose. Data employed in research should not merely be readily available but should specifically serve the precise objectives to advance public welfare.

When discussing purpose limitation, it is essential to address the ambiguity surrounding the concept of purpose, particularly concerning public interest in GDPR and general interest in the DGA. While the main purpose of processing in these cases revolves around these interests, there is a lack of clarity regarding whether the terms are synonymous or their differences. For example, the introduction of the concept of processing for purposes of general interest in the DGA suggests that it may permit, under certain circumstances, the processing of personal data for research purposes that are not strictly defined but serve the general interest[115]. The DGA does not precisely define what constitutes general interest, although it is understandable that it pertains to the common good. However, the specifics of how this is defined remain unclear. While some may argue against the necessity of defining general interest, the effectiveness of data altruism initiatives must have clear definitions. Understanding whether public interest and general interest are the same or distinct concepts is essential for fostering transparency and alignment in data-sharing practices. The discrepancy between the terms "public interest" in the GDPR and "general interest" in the DGA suggests potential differences in their meanings or applications. Despite the examples provided in the recitals of the Data Governance Act, the absence of explicit definitions within the regulatory text itself creates ambiguity. Establishing precise definitions for different purposes serves several purposes.

[115] Gefenas, E., Lekstutiene, J., Lukaseviciene, V., Hartlev, M., Mourby, M., & Cathaoir, K. Ó. (2021). Controversies between regulations of research ethics and protection of personal data: informed consent at a crossroad. Medicine, Health Care and Philosophy. https://doi.org/10.1007/s11019-021-10060-1.

It is essential to include definitions within the regulations that clarify the concept of general interest and outline the specific areas that fall under this concept. Furthermore, considering the distinction between general interest and public interest, legislation should encompass the term "public interest" alongside "general interest." Given the DGA's reliance on the GDPR regarding personal data, it becomes imperative to establish what constitutes general interest and the scope it encompasses. The definition of public interest should align with its purpose within the GDPR, focusing on areas such as healthcare, environmental policy, and research. Similarly, the definition of general interest should reflect the goals and objectives of the DGA, encompassing various sectors. However, due to the broad nature of these definitions, it is advisable to establish limitations to ensure they are applied appropriately. These limitations would define the boundaries within which these interests can be utilized. Firstly, it helps to emphasize the exact purpose of data sharing, providing clarity and transparency for all stakeholders involved. Secondly, it empowers data subjects to make informed decisions about sharing their data and understanding the broad concepts under which their data may be utilized. Additionally, clear definitions facilitate alignment for organizations and authorities, ensuring that data-sharing practices align with the specified interests.

Furthermore, there arises a potential issue regarding the conduct of data intermediaries when conflicting public interests arise[116]. It is imperative to clearly outline the differences between what constitutes public interest and general interest. The DGA typically follows the guidelines outlined in the GDPR regarding the handling of personal data, emphasizing the importance of providing thorough explanations. In this scenario, the jurisprudence of the Court of Justice of the European Union may offer valuable insights. However, even the court may encounter challenges in differentiating between these two terms.

[116] Vardanyan & Kocharyan (2022), *supra nota* 91, p. 105.

3.1 New Consent Form for Data Altruism

Consent under GDPR must be freely given, informed, and clear, and individuals must have the ability to withdraw it easily. Organizations must ensure this option not only for their own data processing but also for any processing done by data users. Additionally, data sharing must be justified under Article 6 of GDPR, tied to specific public interest purposes previously established. There's no allowance for creating big data for any broad public interest, it must align with explicit legal purposes compatible with GDPR[117].

Initially, it appears that the DGA sets a somewhat lower standard for consent in scientific research compared to the GDPR[118]. The implementation of a novel consent framework for data sharing presents both prospects and hurdles for researchers. Initially, the suggested uniform consent approach might appear as an additional obligation amidst existing requirements for research involving human subjects and personal data processing[119]. The GDPR emphasizes strict purpose limitation, implying that data subjects must consent to specific, predefined purposes for data processing (Article 5(1)(b) GDPR)[120]. However, the DGA recognizes the essential difficulty in fully identifying the purpose of personal data processing for scientific research at the time of data collection. This recognition manifests in the allowance for data subjects to consent to data processing in certain areas or parts of research projects, aligning with recognized ethical standards for scientific research[121]. The impact of utilizing consent as the foundation of the data altruism mechanism intersects with the selection of legal bases necessary for processing personal data for scientific research purposes, as outlined in the GDPR. Understanding the role of consent in data altruism is crucial because it directly influences the personal autonomy of individuals who provide such consent[122]. Interestingly, the GDPR also acknowledges the challenge of identifying the precise purpose of data processing for scientific research upfront. It underscores the importance of

[117] Poullet, Y. (2021). Artificial Intelligence and Public Services: the Role of Public Authorities in the Service of the "Third Way" Drawn up by the European Commission. European review of digital administration & law, 2(2), 129-148.
[118] Kruesz & Zopf (2021), *supra nota* 87, p.574.
[119] Shabani, M. (2021, March). The Data Governance Act and the EU's move towards facilitating data sharing. Molecular Systems Biology, 17(3). https://doi.org/10.15252/msb.202110229.
[120] Regulation (EU) 2016/679, *supra nota* 9, Article 5 (1).
[121] Kruesz & Zopf (2021), supra nota 87, p. 575.
[122] Smart Ethics in the Digital World Proceedings of the ETHICOMP 2024. (2024), 137-142. Retrieved from https://dialnet.unirioja.es/descarga/articulo/9326110.pdf.

allowing data subjects to consent to specific areas or parts of research projects in line with ethical standards[123]. Moreover, the DGA explicitly references key provisions of the GDPR and emphasizes compliance with recognized ethical standards in data processing, thereby incorporating the requirements of data protection law. This incorporation suggests a convergence of standards for data subject consent across both regulations[124]. However, on a positive note, a standardized European consent mechanism for altruistic purposes could offer an opportunity to streamline legislation across EU Member States, facilitating data sharing within the EU[125].

3.1.1. Ambiguity of Data Altruism Consent

The ambiguity surrounding the concept of data altruism presents a significant challenge. Specifically, it remains uncertain whether the consent model proposed aligns with the established notion of 'consent' under the GDPR, which includes stringent conditions for its lawfulness. Additionally, the utility or added value of data altruism is questionable, given the already established legal framework for consent within the GDPR[126]. This framework covers specific conditions that must be met for consent to be considered valid. The problematic nature of this situation lies in the potential confusion and uncertainty it creates for both data subjects and data controllers. Without a clear understanding of what data altruism entails and how it intersects with existing regulatory requirements, there is a risk of inadequate protection for individuals' data rights. Moreover, the lack of clarity may delay the effective implementation of data altruism initiatives, potentially undermining their intended societal benefits. Therefore, it is imperative to address these ambiguities and provide clarity on the concept of data altruism to ensure its effective integration within the broader data protection framework[127].

The issue surrounding the definition of consent under the DGA is complex and requires careful consideration. While the DGA references Article 4 of the GDPR for the definition of consent, it introduces a specialized consent form for data altruism under Article 25 of the DGA. This data

[123]Kruesz & Zopf (2021), supra nota 87, p. 575.
[124] Ferrè, (2023, April 26), *supra nota* 8, p.123.
[125] Shabani (2021, March), supra nota 110, p. 3.
[126] Grafenstein (2022), supra nota 85, p. 32.
[127] *Ibid.*

altruism consent form is expected to utilize a modular approach, allowing customization for specific sectors and purposes[128]. However, there remains ambiguity regarding the distinction between consent for personal data and non-personal data within the context of data altruism. Despite the DGA referencing consent requirements in the GDPR, it's unclear why a separate consent form for data altruism is necessary, especially if it mirrors the consent provided under the GDPR. The modular approach introduced by the DGA, as highlighted in Recital 52, is a positive aspect as it allows data subjects to choose consent options tailored to specific sectors[129].

In general, as mentioned above, the GDPR introduces the concept of consent forms and imposes stringent rules regarding their use. However, when considering the need for a specific consent form for data altruism within the context of the DGA, questions arise regarding its necessity. The DGA references consent in the GDPR and introduces a new modular form that provides detailed options for research purposes and general interest. Nevertheless, it's debatable whether this new consent form is truly required, or if the existing consent form under the GDPR is sufficient but needs to be more detailed. Introducing two separate consent forms could pose challenges for organizations, making it harder to understand the distinctions between them. To arrive at a conclusive answer, practice, and experimentation are necessary to determine how the new consent form would differ from the one provided in the GDPR and whether it adequately serves the purpose of data altruism. Given the novelty of data altruism and the lack of practical implementation, exploring different approaches and assessing their effectiveness is crucial for ensuring the successful integration of data altruism practices within the regulatory framework.

The ongoing registration of data altruism organizations further complicates matters. Each member state retains the autonomy to govern data altruism, leading to potential variations in implementation and interpretation. Without established practices, it is challenging to provide definitive answers regarding the interconnection between consent in the GDPR and consent for data altruism. Moving forward, it is essential to address the ambiguity surrounding the necessity and differentiation of consent forms for data altruism. The objective is to foster meaningful dialogue between research participants and organizations by clearly describing the scope and actions involved in obtaining consent. By specifying the individuals or legal representatives

[128] Regulation (EU) 2022/868, *supra nota* 6, Article 25.
[129] Regulation (EU) 2022/868, *supra nota* 6, Recital 52.

granting consent, the precise issue under consideration, and the agent seeking consent, we aim to enhance the ability to evaluate trustworthiness[130].

3.1.2 Data Processing for Research Purposes

Determining whether a public institution's role provides a legal foundation for data collection, or if explicit consent from citizens is necessary, hinges on the intended use of the data. This constitutes a pivotal question that underscores the importance of data governance practices[131]. The discourse surrounding data processing for research purposes under the General Data Protection Regulation has become a focal point for numerous data protection authorities throughout Europe. Despite the clear importance of data subject consent, debates persist regarding its necessity. Various approaches and explanations have emerged, reflecting the nuanced interpretations of GDPR provisions. Nevertheless, the consensus remains that data subject consent is of paramount importance in ensuring ethical and lawful data processing practices for research purposes.

For instance, in a decision by the Garante per la Protezione dei dati personali (Italy), the Data Protection Authority (DPA) highlighted that certain categories of sensitive data, such as health data, may be processed for scientific research purposes under Article 9(2)(j) of the GDPR. However, this processing is contingent upon the implementation of appropriate safeguards outlined in Article 89(1) of the GDPR, such as pseudonymization, to ensure data minimization principles are upheld. Additionally, Article 9(4) of the GDPR grants Member States the flexibility to adopt stricter regulations for the processing of health data. Italian Law, specifically Article 110 of the Privacy Code, aligns with this provision by stipulating that consent for processing health data for scientific research may be waived only when obtaining consent proves to be excessively burdensome for the controller or would compromise the scientific integrity of the research.

[130] Rivas Velarde, M. C., Lovis, C., Ienca, M., Samer, Caroline., & Hurst, S. (2024). Consent as a compositional act – a framework that provides clarity for the retention and use of data. Philosophy, Ethics, and Humanities in Medicine, 19(1). doi:10.1186/s13010-024-00152-0.

[131] Benfeldt, O., Persson, J. S., & Madsen, S. (2019, April 27). Data Governance as a Collective Action Problem. Information Systems Frontiers, 22(2), 299–313. https://doi.org/10.1007/s10796-019-09923-z.

Furthermore, such processing requires prior approval from both an ethical committee and the DPA under Article 36 of the GDPR[132].

The French Data Protection Authority (CNIL) made a similar decision. The French Data Protection Authority (CNIL) approved the processing of data for a national epilepsy study, finding it fell within the legal provisions of Article 6(1)(e) and Article 9(2)(j) of the GDPR. These articles allow processing for tasks in the public interest and sensitive data processing for public interest purposes, respectively. The CNIL deemed the study's aim of improving the national healthcare system as fitting within the definition of public interest[133].

These examples highlight instances where data processing for research purposes was deemed lawful under the GDPR due to its alignment with public interest objectives. In both cases, the controllers relied on specific provisions of the GDPR, such as Article 6(1)(e) and Article 9(2)(j), to justify their processing activities involving sensitive data. Connecting these examples with consent under the GDPR and the Data Governance Act, it's essential to note that while consent is a fundamental principle of data protection, it's not always required in research contexts, especially when processing sensitive data. The GDPR recognizes certain lawful bases for processing, including tasks carried out in the public interest and scientific research purposes. Under the GDPR, explicit consent is one of the lawful bases for processing sensitive data, but it's not the only option. Article 9(2)(j) provides an alternative legal basis for processing such data when it's necessary for scientific research purposes, subject to appropriate safeguards. DGA complements the GDPR by providing additional guidance and frameworks for data processing, including in the context of scientific research and data altruism. While the examples cited do not directly involve data altruism, they do underscore the importance of aligning data processing activities with broader societal interests and the need for robust safeguards, as outlined in both the GDPR and the DGA.

On the other hand, in a ruling by VG Hamburg - 21 K 1802/21, the court found that the transfer and processing of highly sensitive health data by the HKA posed a significant risk to the data subject's fundamental rights. Despite serving specific and lawful purposes, the court found the processing disproportionate and therefore unlawful under Article 9(2)(h), (i), and (j) of the GDPR.

[132] Garante per la protezione dei dati personali - 9875254
[133] CNIL (France) - SAN-2023-0076

The ruling underscores the need for clear legislative provisions ensuring effective protection of sensitive data against misuse[134].

3.1.3 Data Altruism Consent in Practice

The necessity for consent is indisputable, but the specifics of how consent operates within the scope of data altruism raise questions. Additionally, there are no doubts about ensuring the protection of the data subject's fundamental rights through appropriate measures. A modular consent form is seen as essential and beneficial, allowing data subjects to understand and select the research purposes they consent to. However, uncertainties persist regarding how consent operates across different research fields and whether consent granted for one purpose extends to others. The unpredictability of research trajectories and data needs, as acknowledged in both GDPR and DGA recitals, complicates the consent process. On the other hand, it should be noted that, on an individual level, relying solely on traditional risk management approaches such as informed consent can be problematic because it might provide false assurances[135]. In today's digital age, despite having safeguards in place, data usage can still pose risks. It's challenging to guarantee that even with consent, there won't be any risks involved. For instance, there's always a possibility of predictive misuse of health and personal information, potentially harming individuals[136]. While processing for public or general interest may be permissible, stringent measures must ensure data protection. While the GDPR provides exemptions for obtaining consent in certain situations deemed to be in the public interest, the Data Governance Act may not have equivalent exemptions[137]. Consent remains a fundamental principle of data protection, emphasizing individuals' autonomy and control over their data. Therefore, even in cases where data processing is pursued for altruistic purposes or the greater public good, obtaining consent from data subjects is crucial. Newly emerging concerns may lead to questioning the significance of data altruism, particularly in light of the already established legal framework for consent within the GDPR. This

[134] VG Hamburg - 21 K 1802/21, ECLI:DE: VGHH:2022:0728.21K1802.21.00.
[135] McMahon, A., Buyx, A., & Prainsack, B. (2019, August 4). Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond. Medical Law Review. https://doi.org/10.1093/medlaw/fwz016.
[136] *Ibid.*
[137] Ferrè (2023, April 26), *supra nota* 8, p.120-121.

framework sets forth specific conditions for the validity of consent. However, the added value of introducing data altruism may still be unclear[138].

Nonetheless, the Data Governance Act fails to provide definitive solutions to these challenges. In this context, it would be beneficial if legislation could establish an "altruism exemption"[139]. Such an exemption could provide a legal framework that encourages and facilitates data altruism initiatives by exempting certain data processing activities undertaken for altruistic purposes from certain GDPR requirements, particularly those related to consent and purpose limitation. This exemption could help simplify the process for organizations and individuals wishing to contribute their data for the greater good, such as scientific research[140]. Furthermore, it is recommended to develop guidelines for data altruism consent and provide visibility materials for it. Given the lack of established practice, it is challenging to determine the precise format and content of this consent form. However, it should comply with the principles outlined in GDPR, ensuring clarity and comprehension. Distinctions between GDPR consent and data altruism consent forms must be clearly distinguished. Guidelines should clarify the differences in meaning and content between these consent forms to ensure transparency and consistency in their implementation.

Moreover, the distinction between consent in GDPR and DGA remains unclear. Although the DGA makes reference to GDPR provisions, it fails to clarify the operational differences in consent within the data altruism concept. While it may seem altruistic on the surface, its actual impact and benefits need to be carefully evaluated. Given the robust framework for consent already in place under the GDPR, there may be skepticism regarding the need for an additional concept like data altruism. Additionally, the potential risks and implications of data altruism, such as issues related to consent clarity and data protection, should be thoroughly considered. It can be positively evaluated that DGA presents a modular approach to consent, which offers more depth, but its explanation is ambiguous. Consequently, further clarification and guidance are needed to address these challenging issues effectively. Therefore, regulations should provide a clear distinction of the differences between consent forms. As mentioned earlier, integrating dynamic consent content would aid in clearly differentiating between GDPR consent and DGA consent. While both GDPR

[138] *Ibid.*
[139] Veil. (2022). Data altruism: how the EU is screwing up a good idea. AW AlgorithmWatch gGmbH. Retrieved from https://algorithmwatch.org/de/wp-content/uploads/2022/01/2022_AW_Data_Altruism_final_publish.pdf.
[140] *Ibid.*

and DGA offer the option to revoke consent, the ability to modify consent over time based on changing circumstances, and the flexibility for participants to provide consent gradually, can be highly advantageous. This not only simplifies the process for researchers and organizations but also provides overall efficiency.

3.2Data Portability Principle within Data Altruism Concept

The control rights outlined in the GDPR hold significant value for individuals, granting them authority over their personal data. These rights, specifically designed to encourage individual control, include the right to data portability[141]. Facilitating the free portability of personal data between controllers can greatly empower data subjects. It fosters competition among digital services and enhances interoperability between platforms. This, in turn, strengthens individuals' control over their own data[142]. Data portability, as stipulated in Article 20 of the General Data Protection Regulation, refers to the right of individuals to receive their personal data from a data controller in a commonly used and machine-readable format[143]. Article 20 of GDPR offers two methods for transferring and reusing such data[144]. Initially, individuals have the right to request and obtain personal data supplied to a data controller in a structured, commonly used, and machine-readable format[145]. Additionally, individuals are entitled to request the original controller to directly transmit available personal data to another controller, provided it is technically feasible[146].

The Article 29 Working Party emphasized in its discussion of Article 20 of the GDPR that the goal of portability is to foster interoperable systems rather than merely compatible ones[147]. Compatibility would require the data controller to guarantee that the provided data aligns directly with the intended purposes and processing systems of the new controller[148]. The European

[141] Van Ooijen & Vrabec, *supra nota* 21.
[142] De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review, 34(2), 193–203. https://doi.org/10.1016/j.clsr.2017.10.003.
[143] Wong, J., & Henderson, T. (2019). The right to data portability in practice: exploring the implications of the technologically neutral GDPR. International Data Privacy Law, 9(3), 173–191. https://doi.org/10.1093/idpl/ipz008.
[144] Turner, S., & Tanczer, L. M. (2024). In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things. Computer Law & Security Review, 52, 105912. https://doi.org/10.1016/j.clsr.2023.105912.
[145] Regulation (EU) 2016/679, *supra nota* 10, Article 20 (1).
[146] Regulation (EU) 2016/679, *supra nota* 10, Article 20 (2).
[147] Article 29 Data Protection Working Party (WP29), 'Guidelines on the right to data portability' (2017) 17.
[148] Li, W., & Quinn, P. (2024). The European Health Data Space: An expanded right to data portability? Computer Law & Security Review, 52, 105913. https://doi.org/10.1016/j.clsr.2023.105913.

Commission defines interoperability as the capability for various organizations, despite their differences, to collaborate toward mutually beneficial and agreed-upon objectives[149]. This involves the exchange of data between their respective ICT systems, facilitating the sharing of information and knowledge among organizations through the business processes they support[150].

When discussing data portability, it's crucial that the environment is user-friendly, particularly in the context of the Data Governance Act and the concept of data altruism, where data sharing is based on voluntary participation. The key aspect here is fostering trust among data subjects to safely share their data. In a seamlessly integrated ecosystem of services, the extent of personal data shared directly influences the benefits users receive. The broader the sharing of personal data, the more significant the advantages experienced within this user-friendly environment[151]. Data portability, the ability for individuals to employ their data across diverse devices and services, marks a significant shift from passive data subjects to active reusers. This emerging right holds transformative potential, empowering individuals to reclaim control over their data and engage proactively in its reuse across a wide range of platforms and services[152].

To enable data subjects to altruistically share their personal data, they must initially possess it[153]. The European Commission identifies ensuring data portability as a key objective of the European Strategy for Data, emphasizing every citizen's right to control their data. Additionally, the Data Governance Architecture introduces a specialized class of data intermediation services designed to aid data subjects in exercising their GDPR rights, including data portability[154]. This framework is particularly pertinent in scenarios where entities such as hospitals or academic institutions initially collect and process health data. Here, the right to data portability could serve as a mechanism for data subjects to assert control over their personal information and engage in altruistic data sharing[155].

---

[149] European Commission, Directorate-General for Informatics, 'European interoperability framework (EIF): towards interoperability for European public services' (2011).
[150] Li & Quinn (2024), *Supra Nota*, 148.
[151] De Hert, Papakonstantinou, Malgieri, Beslay, & Sanchez (2018), Supra Nota, 142.
[152] Custers, B., & Uršič, H. (2016). Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. International Data Privacy Law, ipv028. https://doi.org/10.1093/idpl/ipv028.
[153] A European strategy for data, Brussels, *supra nota* 3.
[154] *Ibid.*
[155] 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, 10. https://doi.org/10.3389/fmed.2023.1141685.

According to GDPR regulations, data subject-provided data falls under the right to data portability only if processed based on consent or contract performance and carried out through automated means[156]. However, in clinical research, different legal bases combinations, such as legal obligation, public interest, or legitimate interest, are often preferred, depending on the specific case or national legal framework in place[157]. Within the confines of a single clinical trial, there exists the potential for divergence in the exercise of data portability rights and the provision of consent for data altruism among patients. While some may opt to utilize their right to data portability and consent to the altruistic reuse of their data, others may not have access to this option[158]. Given the restricted application of data portability[159], the practical execution of data altruism in clinical research raises significant questions[160].

In this instance, it is crucial to reference the EHDS proposal and the Data Act, which outline data portability in alignment with GDPR but incorporate modifications and clarifications. Under the EU Data Act, the entire legal mechanism of cooperation between the data holder, user, and third party is very different from the usual notion of a data portability right, due to this negotiated licensing agreement between the data holder and the third party. Thus, the Data Act uses the term data portability in this context in analogy to the data portability right of Art. 20 GDPR[161]. Expanding the scope of data portability, the DA includes both natural and legal persons in the context of Internet-of-Things products, regardless of the legal basis for data processing. Additionally, also encompasses both actively provided and passively observed personal data. This comprehensive approach aims to address the evolving landscape of data usage and rights[162]. On one hand, the EHDS Proposal includes elements that are indirectly associated with the notion of portability. These implicit elements align with a common understanding of portability but do not directly correspond to the right as defined within the GDPR. On the other hand, the proposal also

[156] Hansen J, Wilson P, Verhoeven E, Kroneman M, Kirwan M, Verheij R, et al. Assessment of the EU Member States' Rules on Health Data in the Light of GDPR. (2021), https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf.
[157] EDPB. Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR). (2019).
[158] Lalova-Spinks, Meszaros, & Huys, (2023), *supra nota* 155.
[159] De Hert, Papakonstantinou, Malgieri, Beslay, & Sanchez, I. (2018), Supra Nota 142.
[160] Lalova-Spinks, Meszaros, & Huys, (2023), *supra nota* 155.
[161] Kerber, W. (2022). Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. GRUR International, 72(2), 120–135. https://doi.org/10.1093/grurint/ikac107.
[162] Lalova-Spinks, Meszaros, & Huys, (2023), *supra nota*, 155.

incorporates explicit elements that appear to directly aim at improving upon the rights outlined in Article 20 of the GDPR[163].

Despite being distinct pieces of legislation, the Data Governance Act, Data Act, and EHDS Proposal are aligned with the goals outlined in the Data Strategy. This alignment suggests that these legislations may need to be interconnected in certain instances. Despite the fact that it is not explicitly outlined in legislation, the often-overlooked yet potentially impactful tool for advancing data altruism is the right of access[164]. Unlike the constraints posed by data portability, this right offers a broader scope for individuals to engage in altruistic endeavors. It affords individuals the authority to ascertain from data controllers whether their personal information undergoes processing and, if so, to obtain a copy of the data in question[165]. By exercising this right and acquiring a copy of their personal data, individuals not only gain insight into the processing of their information but also wield the ability to actively participate in initiatives promoting data altruism[166]. This proactive engagement enables individuals to contribute meaningfully to endeavors seeking to leverage data for social good. Embracing the right of access as a mechanism for promoting data altruism underscores the importance of recognizing and leveraging existing legal frameworks to foster a culture of responsible data sharing and ethical data practices.

Although Data Governance Act does not explicitly address data portability matters, it could provide opportunities for improved governance that align well with the goals of the Data Act[167]. Fundamentally, the DGA establishes a framework for trust in data exchange, whereas the Data Act focuses on the obligation to share data across various contexts, often guided by principles of fairness[168]. A primary objective of data governance is to resolve conflicting interests among different stakeholders involved in data management. Given that data frequently intersects with multiple and potentially conflicting interests, the flexibility of data governance becomes crucial for achieving balance[169]. Data intermediaries, as regulated by the DGA, play an essential role in

[163] De Hert, Papakonstantinou, Malgieri, Beslay, & Sanchez (2018), Supra Nota, 142.
[164] *Ibid.*
[165] *Ibid.*
[166] *Ibid.*
[167] Margoni, T., Ducuing, C., & Schirru, L. (2023). Data Property, Data Governance and Common European Data Spaces. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4428364.
[168] *Ibid.*
[169] *Ibid.*

establishing commercial relationships for data sharing between numerous data holders and users[170]. In such a scenario, their involvement could be invaluable to ensure that the Data Act effectively achieves its goal of equitable data allocation. Utilizing the services of data intermediaries could enhance transparency, trust, and efficiency in data exchange processes, addressing concerns related to fairness and access. Additionally, their facilitative role could simplify data-sharing practices, fostering collaboration and innovation while minimizing the risks associated with data misuse or exploitation.

[170] Margoni, Ducuing, & Schirru, (2023), *supra nota*, 167.

4. Estonian X – Road

The Estonian e-Government infrastructure, X-Road, plays a pivotal role in fostering interoperability throughout the country. Serving as a unified and secure platform, X-Road facilitates seamless data exchange and communication among diverse organizations, operating at various levels within Estonia's administrative framework[171].

The X-Road, conceived by the government, aims to ensure continuous availability of databases, operating round-the-clock, seven days a week. This initiative by the Republic of Estonia Information System Authority underscores the commitment to seamless data accessibility and exchange[172]. Access to the X-Road empowers users to leverage the services and data of fellow members, thereby enhancing their own business processes. However, it's worth noting that private entities must obtain explicit prior consent to access personal data[173]. The establishment of X-Road reflects Estonia's commitment to digital innovation and efficiency. By ensuring uninterrupted access to databases, X-Road facilitates real-time data exchange, enabling businesses and government agencies to operate more efficiently. Furthermore, the ability for authorized users to leverage each other's services and data fosters collaboration and innovation, driving economic growth and competitiveness. Overall, X-Road serves as a catalyst for digital transformation, promoting transparency, efficiency, and innovation within Estonia's governance framework.

A key feature of the X-Road is the incorporation of the 'once-only principle' (OOP), mandated by Estonian law[174]. This principle dictates that individuals provide their personal data to the state just once, with subsequent data processing operations being handled exclusively by public authorities accessing this centralized repository[175]. This approach not only streamlines administrative processes but also enhances data privacy by minimizing unnecessary data exchanges. By centralizing personal data access, the 'once-only principle' reduces the risk of data breaches and fosters greater trust in the handling of sensitive information by government agencies.

---

[171] Paide, K., Pappel, I., Vainsalu, H., & Draheim, D. (2018). On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships. Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance. https://doi.org/10.1145/3209415.3209441.
[172] Tropp, E. M., Hoffmann, T., & Chochia, A. (2022). Open Data: A Stepchild in e-Estonia's Data Management Strategy? TalTech Journal of European Studies, 12(1), 123–144. https://doi.org/10.2478/bjes-2022-0006.
[173] *Ibid.*
[174] Tropp, Hoffmann, & Chochia (2022), *supra nota*, 172.
[175] *Ibid.*

The challenges of ensuring compliance with GDPR arise concerning the Estonian data protection framework, particularly regarding the X-Road and the 'once-only principle' (OOP). While these mechanisms may initially raise concerns about adherence to the GDPR's principle of purpose limitation[176], Estonia's approach emphasizes transparency to address data subject interests. Despite potential issues with consent at the access level, robust transparency measures ensure comprehensive oversight at the processing level[177]. Through the state portals, individuals can access real-time, detailed information on who accessed their data, under what authorization, and for what specific purpose[178]. This transparency not only fosters accountability but also empowers data subjects with greater control over their personal information, thus aligning with Estonia's commitment to data protection and transparency in governance.

The success story of Estonian ICT began with the establishment of X-Road[179]. As evidenced by practice, Estonia remains a leading country in e-governance and digitalization, underscoring the effectiveness of its approach. Therefore, it is valuable to explore the Estonian model concerning data altruism to glean insights and understand how to implement data altruism in a manner that prioritizes individuals' trust in data handling. Data altruism is a relatively new concept, lacking established practices, which presents a significant challenge due to limited literature on practical implementations. Therefore, making comparisons with already established practices becomes imperative to address this gap.

Despite the success of the 'once-only' principle in Estonia and the effectiveness of Estonian X-Road, the 'exactly once open' principle may not be suitable for data altruism concept. Firstly, the 'once-only' principal functions well within a single country where information sharing occurs within a unified system, which may not align with the broader scope of data altruism. Additionally, data shared for altruistic purposes serves general interests, a concept with a broad scope that may not fit within the confines of a singular principle. Success in achieving the once only principal objective in Estonia hinges on its compatibility with European Union data protection law,

[176] *Ibid.*
[177] Hoffmann, T, (2020), The Impact of Digital Autonomous Tools on Private Autonomy, Baltic Yearbook of International Law Online, 18, 18−31., Available at SSRN: https://ssrn.com/abstract=3771306.
[178] Tropp, Hoffmann, & Chochia (2022), *supra nota*, 172.
[179] Kerikmäe, T., Pärn-Lee, E. Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race. AI & Soc 36, 561–572 (2021). https://doi.org/10.1007/s00146-020-01009-8.

particularly the purpose limitation principle outlined in Article 5 of the GDPR[180]. This principle mandates that personal data should only be collected and processed for specific purposes. However, challenges arise with data altruism, where the purpose is often broad and not well-defined. The principle of purpose limitation is vital for ensuring transparency, predictability, and user control over data handling. The precise articulation of the processing purpose enables data subjects to effectively exercise their rights, including the right to object to the processing.

Therefore, it becomes crucial to draw upon transparency examples from Estonia. Transparency is essential for fostering trust, a critical challenge regarding data altruism, where individuals must willingly share their data without direct incentives such as public services. Ensuring transparency involves providing individuals with information about how their data is used. Access to personal data by the state without explicit consent is generally perceived as less concerning compared to similar access by private companies or individuals. In a 2020 survey, two-thirds of Estonian inhabitants expressed confidence in the security of data collection by the state. They believe that when the state acts as the data collector, data is well protected[181]. This sentiment is expected to be consistent with data altruism practices. Therefore, legislation and data altruism organizations must prioritize transparency and trust by providing detailed information to data subjects.

While the Data Governance Act mandates security and technical measures for data altruism organizations, further measures are necessary to encourage voluntary data sharing. This requires legislation that not only ensures security but also motivates individuals to share their data for altruistic purposes. In the case of Estonia, transparency regarding data usage plays a crucial role in fostering trust. When individuals have insight into how their data is accessed and processed, they are more likely to trust the system. In Estonia, the state portal allows individuals to request real-time information about who accessed their data, when, and for what purpose, creating transparency and accountability. This level of transparency is essential for building trust, as individuals can see exactly how their data is being used[182]. Aligning with this example, the Data Governance Act should prioritize transparency, providing detailed information for data subjects about how their data is utilized. It would be beneficial for data altruism organizations to have a

[180] Mikiver, M., & Tupay, P. K. (2023). Has the GDPR killed e-government? The "once-only" principle vs the principle of purpose limitation. https://doi.org/10.1093/idpl/ipad010.
[181] *Ibid.*
[182] Tropp, Hoffmann, & Chochia (2022), *supra nota*, 172.

portal where individuals can access information about how, when, and by whom their data is used, especially for research or clinical trials. This portal should establish a dynamic system capable of adapting over time[183], consistently reinforcing trust through its responsiveness to evolving needs and circumstances. This ensures that individuals have full visibility and control over the usage of their data, further enhancing trust and confidence in data-sharing practices.

[183] Jain, S., Spelliscy, C., Vance-Law, S., & Moore, S. (2023). AI and Democracy's Digital Identity Crisis. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4593685.

5. GDPR Compliance approaches and implications

It's important to note that, DGA aims to provide a foundational framework for sector-specific legislation concerning data access, use, and re-use. This common background allows specialized laws to operate effectively, especially when they do not address certain issues or when European regulations have not yet been established[184]. This implies that the Data Governance Act, GDPR, and other legislations within the European data strategy should collaborate and complement each other. In essence, they should function as a cohesive framework, with each regulation filling in gaps and enhancing the effectiveness of the others. This collaborative approach ensures a comprehensive and harmonized system for data governance and protection within the European Union, promoting consistency and alignment across various legislative measures.

Although the Data Governance Act aims to facilitate data sharing across various sectors, it's important to note that it does not establish a distinct legal foundation for processing personal data on its own. The DGA operates horizontally, meaning it provides overarching principles and guidelines for data governance practices but relies on existing legal frameworks, such as the General Data Protection Regulation, for specific requirements related to personal data processing. Therefore, while the DGA facilitates data-sharing efforts, organizations must still comply with the GDPR and other relevant regulations when processing personal data[185]. This underscores the interrelation of these regulations and emphasizes the importance of ensuring alignment with GDPR requirements to maintain consistency and legal compliance in data processing practices governed by the DGA.

With the introduction of these new legal acts, research entities must demonstrate a legal basis for processing personal data under the GDPR[186]. Under this framework, research entities may acquire personal data through various channels, including obtaining consent from data subjects as per Article 9(2)(a) of the GDPR, processing data for scientific research in accordance with Article

[184] De Hert, P. (2023). Post-GDPR Lawmaking in the Digital Data Society: Mimesis Without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4601974.
[185] Regulation (EU) 2022/868, *supra nota* 6, Recital (14).
[186] Hajduk, P. (2024). A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research. IFIP Advances in Information and Communication Technology, 127–142. https://doi.org/10.1007/978-3-031-57978-3_9.

89(1) of the GDPR, acquiring data for re-use from public bodies or through data altruism under the DGA, and retrieving data from IoT medical devices as outlined in the Data Act[187]. This means that research entities must navigate a complex regulatory landscape encompassing the GDPR, sectoral laws of Member States, and ethical guidelines when handling personal data[188].

Hence, in cases where GDPR compliance is mandatory and the Data Governance Act is applicable, a significant challenge arises regarding the alignment of DGA provisions with GDPR requirements, particularly concerning the principle of purpose limitation. This challenge becomes pronounced when the DGA references general interest purposes for processing personal data. As mentioned before during the research data altruism is based on general interest purposes like healthcare and scientific research. Data altruism organizations registered and recognized in the EU will collect and manage consents and permissions. These organizations will have the authority to process the altruistically shared data or make it accessible for use by other data users[189].

In general, Insufficient enforcement by authorities in defining clear and explicit purposes for data collection and processing is posited as a primary cause of existing data protection challenges[190]. The Purpose Limitation principle, which mandates that data should only be collected and processed for specific purposes, offers a potential solution to address these challenges effectively. By emphasizing the necessity of collecting and processing data for specific purposes only, the Purpose Limitation principle aims to enhance transparency, accountability, and trust in data processing practices, ultimately strengthening data protection efforts[191]. This implies that in the context of data altruism, it's essential to clearly define the purpose of data usage. This not only aligns with GDPR requirements but also ensures transparency and trust in data sharing practices. Given the distinction between "general interest" and "public interest" as outlined in the GDPR, it's evident that these terms have distinct meanings and should be treated as such. Therefore, the Data Governance Act (DGA) should offer detailed definitions of what constitutes "general interest." This is crucial for two reasons: firstly, it provides clarity to data subjects and intermediaries,

[187] *Ibid.*
[188] *Ibid.*
[189] Lalova-Spinks, T., Saesen, R., Silva, M., Geissler, J., Shakhnenko, I., Camaradou, J. C., & Huys, I. (2024). Patients' knowledge, preferences, and perspectives about data protection and data control: an exploratory survey. Frontiers in Pharmacology, 14. https://doi.org/10.3389/fphar.2023.1280173.
[190] Hahn, I. (2021). Purpose Limitation in the Time of Data Power: Is There a Way Forward? European Data Protection Law Review, 7(1), 31–44. https://doi.org/10.21552/edpl/2021/1/7.
[191] *Ibid.*

enabling them to understand and make informed choices; secondly, it specifies the exact purpose of data processing, which is a requirement under the GDPR. By defining "general interest" in detail, the DGA can enhance transparency, facilitate informed decision-making, and ensure compliance with GDPR principles.

Within the framework of data governance, it is essential to highlight the importance of public authorities' obligation to prioritize the common good in their actions[192]. Thus, it becomes paramount that all stakeholders exercise their authority, rights, roles, and responsibilities within meticulously defined boundaries[193]. General definitions must steer clear of being overly broad to prevent unintended expansions of their scope. However, grappling with the concept of "general interest" poses significant challenges due to its inherent extent, making it difficult to provide precise explanations. Consequently, legislation must establish comprehensive limitations to offer clarity and guidance. Rather than exhaustively detailing what falls within the purview of "general interest," legislation can proactively specify what falls outside of this scope. Such an approach not only fortifies security and trust but also ensures that the purposes of data usage remain well within reasonable bounds, adhering firmly to the parameters established by regulatory oversight.

In the definition section of this legislation, it is advisable to include a definition of "general interest," specifying that matters not considered general interest under this regulation including personal preferences or individual desires unrelated to broader social welfare, private commercial interests not aligned with public welfare objectives, discriminatory policies favoring specific groups, actions undermining data privacy or violating individuals' rights to data protection, decisions prioritizing short-term gains for certain stakeholders, initiatives compromising data security or contributing to cyber threats and vulnerabilities, and any activities conflicting with established legal and ethical standards regarding data usage and management. Furthermore, it is crucial that provisions within the legislation mandate strict compliance with the public interest as outlined in the General Data Protection Regulation concerning the processing of personal data. This requirement ensures that any data processing activities undertaken under the legislation prioritize the broader social and public good objectives. By aligning with the principles of the

[192] Mazzucato, M. (2023). Governing the economics of the common good: from correcting market failures to shaping collective goals. Journal of Economic Policy Reform, 27(1), 1–24. https://doi.org/10.1080/17487870.2023.2280969.
[193] Paparova, D., Aanestad, M., Vassilakopoulou, P., & Bahus, M. K. (2023). Data governance spaces: The case of a national digital service for personal health data. Information and Organization, 33(1), 100451. https://doi.org/10.1016/j.infoandorg.2023.100451.

GDPR, which emphasize the protection of individual's rights and freedoms with regard to their personal data, the legislation upholds a standard of accountability and responsibility in data governance. Additionally, the definition should incorporate elements from Recital 12, where Member States are granted the authority to apply the regulation to public or private entities performing public sector duties or providing services considered of general interest. However, exemptions from certain provisions of the regulation are granted for data exchanges conducted solely for public tasks among public sector bodies within the EU, or between these bodies and those in third countries or international organizations. Additionally, exchanges of data between researchers for non-commercial scientific research purposes are exempted[194]. These exemptions aim to facilitate essential data exchange for functions serving the general interest and scientific research, ensuring they are not unnecessarily burdened by regulatory requirements. Lastly, considering the individuality of each national law, provisions should grant Member States the right to determine the sense and exemptions of general interest within national law where needed.

[194] Regulation (EU) 2022/868, *supra nota* 6, Article Recital (12).

6. Conclusion

As evidenced through this research, The European Commission's Data Governance Act, designed to foster data sharing by establishing a trustworthy digital ecosystem among diverse stakeholders[195], represents a significant advancement toward aligning with the European data strategy. The aim of this research was to explore the challenges associated with the Data Governance Act, focusing particularly on the concept of data altruism while ensuring compliance with GDPR and data altruism consent requirements. A mixed-methods approach was employed, involving an analysis of existing literature, practices, and case studies, as well as a comparison of different legislations. This comparative analysis was especially pertinent within the broader context of the European data strategy, where numerous new legislations were introduced to align with shared objectives. The primary objectives of the research were to define and identify challenges related to data altruism and to examine practical approaches for its implementation. Additionally, the research aimed to assess the necessary strategies and address challenges to facilitate the effective execution of data altruism initiatives.

The primary contribution of this research is to propose ideas on how data altruism within the Data Governance Act should function effectively. The main findings consist of several key aspects. Firstly, the research identifies challenges related to definitions and highlights issues with consent mechanisms. Additionally, the study examines data-sharing practices among various authorities and suggests strategies for improvement. Given that the legislation is relatively new, the research draws upon existing experiences, such as those from the Estonian X-Road, to enhance trust and ensure the successful implementation of data altruism initiatives.

When it comes to defining terms, it's essential to recognize that various legislations, such as the Data Governance Act, Data Act, and GDPR, offer differing definitions for data. Therefore, it becomes crucial to comprehend which definition applies in a given context. In light of this, it's advisable to incorporate the definition of data into consent agreements to ensure alignment with the scope of the Data Governance Act. By explicitly including the definition within consent documents, individuals can have a clear understanding of the type of data being referred to and the

[195] Laamech, N., Munier, M., & Pham, C. (2022). IdSM-O. Proceedings of the 14th International Conference on Management of Digital EcoSystems. https://doi.org/10.1145/3508397.3564825.

legal framework under which it falls. This approach not only enhances transparency but also helps to mitigate potential misunderstandings or discrepancies regarding the handling of data. Ultimately, ensuring clarity and consistency in defining data promotes adherence to relevant regulations and fosters trust.

Another significant aspect of the definition challenge involves clarifying the concept of "general interest," as discussed previously. It's crucial to provide a definition that clearly distinguishes between the general interest in the Data Governance Act and the concept of public interest within the GDPR framework to prevent confusion. Notably, the term "general interest" is not explicitly defined in the text of the regulation but can only be inferred from the recitals. Additionally, due to the broad nature of the definition and the potential for it to encompass every aspect, it may be challenging to ensure regulatory compliance and maintain a clear purpose for data processing. To ensure clarity and guidance for all parties involved, it is recommended to establish limitations within the definition, as discussed above. This involves structuring the definition to explicitly outline what is not included in the general interest definition. These exclusions should encompass personal preferences or individual desires unrelated to broader societal welfare, private commercial interests not aligned with public welfare objectives, discriminatory policies favoring specific groups, actions undermining data privacy or violating individuals' rights to data protection, decisions prioritizing short-term gains for certain stakeholders, initiatives compromising data security or contributing to cyber threats and vulnerabilities, and any activities conflicting with established legal and ethical standards regarding data usage and management.

Additionally, Informational exchange between data altruism organizations and data protection authorities can greatly benefit the practical implementation of the data altruism concept. This exchange fosters better compliance and understanding, particularly considering the GDPR exemptions regarding data reuse for research purposes[196]. Ultimately, promoting responsible data-sharing practices hinges on enhancing communication and collaboration between these entities. It is advisable to collaborate with data altruism organizations to develop comprehensive guidelines aimed at sharing best practices and experiences in handling, using, and processing data. By fostering collaboration and knowledge exchange, these guidelines can serve as valuable resources

[196] Kruesz & Zopf (2021), *supra nota* 73, p. 576-577.

for promoting responsible data sharing practices. Furthermore, they can facilitate the dissemination of innovative approaches and effective strategies for navigating data governance challenges. Additionally, involving data altruism organizations in the development of these guidelines ensures that diverse perspectives and expertise are considered, leading to more robust and inclusive frameworks.

Another significant challenge lies in the landscape of data altruism consent. While the Data Governance Act offers a modular approach to consent, which is highly beneficial, the primary issue remains ensuring that the entire system encourages data subjects to share their data voluntarily, as data altruism revolves around voluntary data sharing. Legislation must prioritize building trust, which necessitates providing detailed information. In the context of data altruism, it's crucial to develop consent mechanisms in a way that aligns with the modular approach while also being dynamic. This means that dynamic consent forms should be adaptable and capable of evolving over time. Data subjects should have the flexibility to give or revoke consent at any time, reflecting changes in circumstances or preferences. For instance, they may initially withhold consent but later decide to provide it based on evolving factors. Dynamic consent is particularly crucial in scenarios where research purposes may change, empowering data subjects to adjust their consent accordingly. Adopting dynamic consent for data altruism not only enhances transparency but also fosters trust by providing individuals with greater information and control over their data. Additionally, it's crucial to draw upon the practices and lessons from Estonia when addressing data altruism. Reflecting this example, the Data Governance Act should prioritize transparency, ensuring that data subjects receive detailed insights into how their data is utilized. To achieve this, establishing a portal within data altruism organizations would be advantageous, enabling individuals to access comprehensive information regarding the utilization of their data, especially in research or clinical trial settings. This portal should operate dynamically, adapting over time to maintain transparency throughout the data processing journey. By providing clear visibility into data usage, individuals can exercise greater control over their data, empowering them to revoke consent or implement necessary safeguards for data protection.

As the legislation is still in its early stages of development, there is no established practice yet. Although new legislations have been adopted within the European data strategy, it remains questionable how all these regulations will harmonize and function together. The complexity arises

from the potential overlap between various legislative frameworks and how they interact in practice. Questions persist regarding the coherence and consistency of these laws, particularly concerning their implementation and enforcement across different sectors and jurisdictions within Europe. The registration of data altruism organizations is ongoing, and given that the adoption of the Data Governance Act and its essential parts such as data altruism is optional for countries, there is uncertainty about how it will operate, with practices potentially varying widely. Despite these uncertainties, the approaches and findings of this research set a foundation for the practical implementation of data altruism. This implementation is crucial in fostering trust in the system and encouraging individuals to voluntarily share their data. However, it's important to acknowledge that as the concept is put into practice, new challenges may emerge, necessitating further research to address them effectively.

List Of References:

Scientific books:

1. Benfeldt, O., Persson, J. S., & Madsen, S. (2019, April 27). Data Governance as a Collective Action Problem. *Information Systems Frontiers*, 22(2), 299–313. https://doi.org/10.1007/s10796-019-09923-z.
2. Kruesz, C., & Zopf, F. (2021). European Union · The concept of data altruism of the draft DGA and the GDPR: Inconsistencies and why a regulatory sandbox model may facilitate data sharing in the EU. *European Data Protection Law Review*, 7(4), 569–579. https://doi.org/10.21552/edpl/2021/4/13.
3. Skovgaard, L. L., Wadmann, S., & Hoeyer, K. (2019). A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. *Health Policy*, 123(6), 564–571. https://doi.org/10.1016/j.healthpol.2019.03.012.

Scientific Articles:

1. Bravo. (2022). Data Governance Act and Re-Use of Data in the Public Sector. *European Review of Digital Administration & Law - Erdal*, 3(2), 13–22.
2. Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. https://doi.org/10.1016/j.clsr.2023.105830.
3. Custers, B., & Uršič, H. (2016). Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*, https://doi.org/10.1093/idpl/ipv028.
4. De Hert, P. (2023). Post-GDPR Lawmaking in the Digital Data Society: Mimesis Without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4601974.
5. De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services.

Computer Law & Security Review, 34(2), 193–203. https://doi.org/10.1016/j.clsr.2017.10.003.

6. De Sutter, E., Barbier, L., Borry, P., Geerts, D., Ioannidis, J. P. A., & Huys, I. (2024, January 1). Personalized and longitudinal electronic informed consent in clinical trials: How to move the needle? https://doi.org/10.1177/20552076231222361.
7. Denga, M., & Hoffmann, T. (2023). The Estonian Electronic Health Record – a Prototype for Data Governance in the European Health Data Space? *European Health & Pharmaceutical Law Review*, 7(1), 5–15. https://doi.org/10.21552/ehpl/2023/1/4.
8. Esteves, B., Rodríguez-Doncel, V., Pandit, H. J., & Lewis, D. (2023, September 11). Semantics for Implementing Data Reuse and Altruism Under EU's Data Governance Act. https://doi.org/10.3233/ssw230015.
9. Ferrè, G. R. (2023, April 26). Data donation and data altruism to face algorithmic bias for an inclusive digital healthcare. https://doi.org/10.15168/2284-4503-2624
10. Finck, M., & Mueller, M.-S. (2023). Access to Data for Environmental Purposes: Setting the Scene and Evaluating Recent Changes in EU Data Law. *Journal of Environmental Law*, 35(1), 109–131. https://doi.org/10.1093/jel/eqad006.
11. Garske, B., Holz, W., & Ekardt, F. (2024). Digital twins in sustainable transition: exploring the role of EU data governance. *Frontiers in Research Metrics and Analytics*, 9. https://doi.org/10.3389/frma.2024.1303024.
12. Gefenas, E., Lekstutiene, J., Lukaseviciene, V., Hartlev, M., Mourby, M., & Cathaoir, K. Ó. (2021). Controversies between regulations of research ethics and protection of personal data: informed consent at a crossroad. *Medicine, Health Care and Philosophy*. https://doi.org/10.1007/s11019-021-10060-1.
13. Gomez Ortega, A., Bourgeois, J., Hutiri, W. T., & Kortuem, G. (2023). Beyond data transactions: a framework for meaningfully informed data donation. *AI & SOCIETY*. https://doi.org/10.1007/s00146-023-01755-5.
14. Graef, I., & Prüfer, J. (2021, November 1). Governance of data sharing: A law & economics proposal. Research Policy. https://doi.org/10.1016/j.respol.2021.104330.
15. Grafenstein, M. (2022). Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance

Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4104502.

16. Hahn, I. (2021). Purpose Limitation in the Time of Data Power: Is There a Way Forward? European *Data Protection Law Review*, 7(1), 31–44. https://doi.org/10.21552/edpl/2021/1/7.
17. Hajduk, P. (2024). A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research. *IFIP Advances in Information and Communication Technology*, 127–142. https://doi.org/10.1007/978-3-031-57978-3_9.
18. Hansen J, Wilson P, Verhoeven E, Kroneman M, Kirwan M, Verheij R, et al. Assessment of the EU Member States' Rules on Health Data in the Light of GDPR. (2021), https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf.
19. Hoffmann, T, (2020), The Impact of Digital Autonomous Tools on Private Autonomy, Baltic Yearbook of International Law Online, 18, 18−31., Available at SSRN: https://ssrn.com/abstract=3771306.
20. Iphofen, R., & O'Mathúna, D. (2021). Ethical Issues in Covert, Security and Surveillance Research. *Emerald Group Publishing*, p 93-119.
21. Jain, S., Spelliscy, C., Vance-Law, S., & Moore, S. (2023). AI and Democracy's Digital Identity Crisis. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4593685.
22. Judyta Lubacha, Mäihäniemi, B., & Rafał Wisła. (2023). *The European Digital Economy* (pp. 161–185). Taylor & Francis.
23. Kamocki, P., Linden, K., Puksas, A., & Kelli, A. (2023). EU Data governance act: Outlining a potential role for Clarin. *Linköping Electronic Conference Proceedings*. doi:10.3384/ecp198006.
24. Kaye, J., Whitley, E. A., Lund, D. J., Morrison, M., Teare, H., & Melham, K. (2014, May 7). Dynamic consent: a patient interface for twenty-first century research networks. https://doi.org/10.1038/ejhg.2014.71.
25. Kerber, W. (2022). Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. *GRUR International*, 72(2), 120–135. https://doi.org/10.1093/grurint/ikac107.

26. Kerikmäe, T., Pärn-Lee, E. Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race. *AI & Soc* 36, 561–572 (2021). https://doi.org/10.1007/s00146-020-01009-8.
27. König, P. D. (2022, January 1). Analyzing EU Data Governance Through the Lens of the Resource Regime Concept. https://doi.org/10.2139/ssrn.4050804.
28. Laamech, N., Munier, M., & Pham, C. (2022). IdSM-O. Proceedings of the 14th International Conference on Management of Digital EcoSystems. https://doi.org/10.1145/3508397.3564825.
29. 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*, 10. https://doi.org/10.3389/fmed.2023.1141685.
30. Lalova-Spinks, T., Saesen, R., Silva, M., Geissler, J., Shakhnenko, I., Camaradou, J. C., & Huys, I. (2024). Patients' knowledge, preferences, and perspectives about data protection and data control: an exploratory survey. *Frontiers in Pharmacology*, 14. https://doi.org/10.3389/fphar.2023.1280173.
31. Li, W., & Quinn, P. (2024). The European Health Data Space: An expanded right to data portability? *Computer Law & Security Review*, 52, 105913. https://doi.org/10.1016/j.clsr.2023.105913.
32. Margoni, T., Ducuing, C., & Schirru, L. (2023). Data Property, Data Governance and Common European Data Spaces. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4428364.
33. Mazzucato, M. (2023). Governing the economics of the common good: from correcting market failures to shaping collective goals. *Journal of Economic Policy Reform*, 27(1), 1–24. https://doi.org/10.1080/17487870.2023.2280969.
34. McMahon, A., Buyx, A., & Prainsack, B. (2019, August 4). Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond. *Medical Law Review*. https://doi.org/10.1093/medlaw/fwz016.
35. Mikiver, M., & Tupay, P. K. (2023). Has the GDPR killed e-government? The "once-only" principle vs the principle of purpose limitation. https://doi.org/10.1093/idpl/ipad010.

36. Mylly, U. M. (2024). Trade Secrets and the Data Act. IIC - *International Review of Intellectual Property and Competition Law*. https://doi.org/10.1007/s40319-024-01432-0.
37. Paide, K., Pappel, I., Vainsalu, H., & Draheim, D. (2018). On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships. Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance. https://doi.org/10.1145/3209415.3209441.
38. Paparova, D., Aanestad, M., Vassilakopoulou, P., & Bahus, M. K. (2023). Data governance spaces: The case of a national digital service for personal health data. Information and Organization, 33(1), 100451. https://doi.org/10.1016/j.infoandorg.2023.100451.
39. Pathak, M. (2024). Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4718891.
40. Poullet, Y. (2021). Artificial Intelligence and Public Services: the Role of Public Authorities in the Service of the "Third Way" Drawn up by the European Commission. *European review of digital administration & law*, 2(2), 129-148.
41. Rivas Velarde, M. C., Lovis, C., Ienca, M., Samer, Caroline., & Hurst, S. (2024). Consent as a compositional act – a framework that provides clarity for the retention and use of data. *Philosophy, Ethics, and Humanities in Medicine*, 19(1). doi:10.1186/s13010-024-00152-0.
42. Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at glance. https://doi.org/10.1016/j.is.2021.101876.
43. Ruohonen, J., & Mickelsson, S. (2023). Reflections on the Data Governance Act. Digital Society, 2(1). doi:10.1007/s44206-023-00041-7.
44. Schneider, G., & Comandè, G. (2021). Can the GDPR make data flow for research easier? yes it can, by differentiating! A careful reading of the GDPR shows how EU Data Protection Law leaves open some significant flexibilities for data protection-sound research activities. *SSRN Electronic Journal*. doi:10.2139/ssrn.3795554.
45. Shabani, M. (2021, March). The Data Governance Act and the EU's move towards facilitating data sharing. *Molecular Systems Biology*, 17(3). https://doi.org/10.15252/msb.202110229.

46. Shabani, M., & Yilmaz, S. (2022). Lawfulness in secondary use of health data: Interplay between three regulatory frameworks of GDPR, DGA & EHDS. *Technology and Regulation*, 2022, 128–134. https://doi.org/10.26116/techreg.2022.013.
47. Smart Ethics in the Digital World Proceedings of the ETHICOMP 2024. (2024), 137-142. Retrieved from https://dialnet.unirioja.es/descarga/articulo/9326110.pdf.
48. Tropp, E. M., Hoffmann, T., & Chochia, A. (2022). Open Data: A Stepchild in e-Estonia's Data Management Strategy? *TalTech Journal of European Studies*, 12(1), 123–144. https://doi.org/10.2478/bjes-2022-0006.
49. Turner, S., & Tanczer, L. M. (2024). In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things. *Computer Law & Security Review*, 52, 105912. https://doi.org/10.1016/j.clsr.2023.105912.
50. Van Ooijen, I., & Vrabec, H. U. (2018, December 11). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. https://doi.org/10.1007/s10603-018-9399-7.
51. Vardanyan, L., & Kocharyan, H. (2022). The GDPR and the DGA proposal: Are they in controversial relationship? *European Studies*, 9(1), 91–109. https://doi.org/10.2478/eustu-2022-0004.
52. Veil. (2022). Data altruism: how the EU is screwing up a good idea. AW AlgorithmWatch gGmbH. Retrieved from https://algorithmwatch.org/de/wp-content/uploads/2022/01/2022_AW_Data_Altruism_final_publish.pdf.
53. Von Grafenstein, M. (2021). Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II. *European Data Protection Law Review*, 7(2), 190–205. https://doi.org/10.21552/edpl/2021/2/8.
54. Vukovic, J., Ivankovic, D., Habl, C., & Dimnjakovic, J. (2022). Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. *Archives of Public Health*, 80(1). https://doi.org/10.1186/s13690-022-00866-7.
55. Wong, J., & Henderson, T. (2019). The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law*, 9(3), 173–191. https://doi.org/10.1093/idpl/ipz008.

56. Zichichi, M., Ferretti, S., D'Angelo, G., & Rodríguez-Doncel, V. (2022). Data governance through a multi-DLT architecture in view of the GDPR. Cluster Computing. https://doi.org/10.1007/s10586-022-03691-3.

Other Sources:

1. A European strategy for data, Brussels, 19.2.2020 COM (2020) 66 final.
2. Article 29 Data Protection Working Party (WP29), 'Guidelines on the right to data portability' (2017) 17.
3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on Building a European Data Economy, COM (2017) 9 final (Jan. 10, 2017)
4. EDPB. Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR). (2019).
5. European Commission, Directorate-General for Informatics, 'European interoperability framework (EIF): towards interoperability for European public services' (2011).
6. The European Data Governance Act, Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
7. The European Data Act, retrieved from: https://www.eu-data-act.com/
8. European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies, retrieved from: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en.

EU and International Legislation:

1. 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, p. 1–88.

2. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1 OJ L 295, 21.11.2018, p. 39–98.
3. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) OJ L 303, 28.11.2018, p. 59–68.
4. Regulation (EU) 2022/868 of the European Parliament and Council, of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022.

Other Courts Decisions:

1. CNIL (France) - SAN-2023-0076
2. Garante per la protezione dei dati personali – 9875254
3. VG Hamburg - 21 K 1802/21, ECLI:DE: VGHH:2022:0728.21K1802.21.00.

Other Sources:

1. A European strategy for data, Brussels, 19.2.2020 COM (2020) 66 final.
2. Article 29 Data Protection Working Party (WP29), ‘Guidelines on the right to data portability’ (2017) 17.
3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on Building a European Data Economy, COM (2017) 9 final (Jan. 10, 2017)
4. EDPB. Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR). (2019).
5. European Commission, Directorate-General for Informatics, ‘European interoperability framework (EIF): towards interoperability for European public services’ (2011).

6. European Data Governance Act, Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
7. The European Data Act, retrieved from: https://www.eu-data-act.com/
8. European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies, retrieved from: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en.

Appendix 1 – The non-exclusive license

I Ana Koiava, Grant Tallinn University of Technology a free license (non-exclusive license) for my thesis - Challenges of GDPR Compliance with the Data Altruism Concept under DGA: Lessons from the Estonian X-Road Model, supervised by Professor Thomas Hoffman and Dr. Archil Chochia:

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive license.

3. I confirm that granting the non-exclusive license does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.