Consent, Control and Compliance:
Legal Perspectives on Processing Health Data in the Development of AI Through Anonymization and Pseudonymization Under the GDPR

Alari Pakarinen
University of Lapland
Faculty of Law
European law
Master's thesis
Supervisor: Markku Kiikeri
February 2025

University of Lapland

Faculty: Faculty of Law

Title of the Thesis: Consent, Control and Compliance: Legal Perspectives on Processing Health Data in the Development of AI Through Anonymization and Pseudonymization Under the GDPR

Author: Alari Pakarinen

Degree Program: Master's Programme in Law

Level: Master's thesis

Number of Pages: XV + 80

Keywords: Artificial Intelligence, GDPR, Health Data, Anonymization, Pseudonymization, Data Protection, Consent, Privacy, AI Development**.**

Year: 2025

Abstract:

This thesis explores the legal and ethical challenges associated with processing health data for artificial intelligence (AI) development under the General Data Protection Regulation (GDPR). Specifically, it examines how privacy-preserving techniques, such as anonymization and pseudonymization, reconcile GDPR's consent requirements with the practical needs of utilizing sensitive health data in AI training. The study addresses the complexities of defining personal, pseudonymized, and anonymized data, particularly in the context of multiple parties involved in AI development.

Using a legal-doctrinal approach, the research highlights that the anonymity of data can vary depending on the parties' capabilities to identify its origin. For example, data pseudonymized by a hospital may be considered anonymized once transferred to an AI developer, provided the developer does not have access to the original dataset or operate under the authority of the hospital. When data is rendered anonymous for the AI developer, consent from the data subject is no longer required under the GDPR. Consequently, the focus of consent should shift to the anonymization process itself, ensuring that robust safeguards and appropriate data handling practices are in place to achieve genuine anonymization.

The findings emphasize that the GDPR, when effectively implemented, provides a pathway to balance technological innovation and data protection. By clarifying the roles of parties and enforcing robust safeguards, such as separating data sets and ensuring access restrictions, hospitals and AI developers can mitigate risks and build trust among patients, authorities, and the public. The study offers actionable recommendations for policymakers, healthcare organizations, and AI developers to navigate the intersection of legal compliance and ethical data use. It concludes by advocating for a harmonized regulatory framework that supports responsible and compliant AI innovation in the healthcare sector.

CONTENTS

Bibliography

Literature

Aarnio, A. (1988). Laintulkinnan teoria. Helsinki: WSOY.

Aarnio, A. (2006). Tulkinnan taito – ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. Helsinki: Alma Talent.

Ailisto, H. (toim.), Heikkilä, E., Helaakoski, H., Neuvonen, A., & Seppälä, T. (2018). Tekoälyn kokonaiskuva ja osaamiskartoitus. Selvitys- ja tutkimustoiminnan julkaisusarja 46/2018. Valtioneuvoston kanslia.

Anwana, T.O., Barud, K., Cepic, M., Johnson, E., Königseder, M., Wagner, MC. (2024). Consent and Retrospective Data Collection. In: Corrales Compagnucci, M., Minssen, T., Fenwick, M., Aboy, M., Liddell, K. (eds) The Law and Ethics of Data Sharing in Health Sciences. Perspectives in Law, Business and Innovation. Springer, Singapore.

Barto, A. (2006). 'Handbook of Learning and Approximate Dynamic Programming', IEEE Transactions on Automatic Control, no pagination.

BeyLeveld, D., & Brownsword, R. (2007). Consent in the Law. Oxford: Hart Publishing.

Bygrave, L. A., Docksey, C., Kuner, C., Bygrave, L. A., Docksey, C., & Kuner, C. (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.

Cavoukian, A. (2011). Privacy by Design – The 7 Foundational Principles. Information and Privacy Commissioner of Ontario.

Clarke, N, Vale G, Reeves EP, Kirwan M, Smith D, Farrell M, Hurl G, McElvaney NG. (2019). GDPR: an impediment to research? Ir J Med Sci 188(4), p. 1129–1135.

De Filippis, R., Al Foysal, A., Rocco, V., Guglielmo, R., Sabatino, B., Pietropaoli, A., Boscarino, F., Vallese, A., & Ferracuti, S. (2024). The risk perspective of AI in healthcare: GDPR and GELSI framework (Governance, Ethical, Legal and Social Implications) and the new European AI Act. Italian Journal of Psychiatry.

De Hert, P., Papakonstantinou, V., Wright, D. and Gutwirth, S. (2013). 'The proposed regulation and the construction of a principles-driven system for individual data protection', Innovation: The European Journal of Social Science Research, 26(1–2), p. 133–144.

Deo Rahul C., 'Machine Learning in Medicine' (2015). 132(20) Circulation: Cardiovascular Quality and Outcomes, p. 1920–1930.

Donnelly, M, McDounagh M. (2019). Health research, consent and the GDPR exemption, Eur J Health Law 26(2): p. 97-119.

Dourish, P. (2016). Algorithms and their others: Algorithmic culture in context. SAGE.

Dove, E. S. (2024). 'The European Health Data Space as a case study', Ethics & Human Research, 46(6), p. 29–35.

Ducato, R. (2020). 'Data protection, scientific research, and the role of information', Computer Law and Security Review.

Duncan, G. and Lambert, D. (1989). 'The risk of disclosure for microdata', Journal of Business & Economic Statistics, 7.

Feiler, L., Forgó, N. and Weigl, M. (2018). The EU General Data Protection Regulation (GDPR) – A Commentary. London: Globe Law and Business.

Finck, M. and Pallas, F. (2020). 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', International Data Privacy Law, 10(1), p. 11–36.

Günther, C. (2024). Artificial Intelligence, Patient Autonomy and Informed Consent. Nomos Verlagsgesellschaft.

Hanninen, M., Laine, E., Rantala, K., Rusi, M., and Varhela, M. (2017). Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Helsinki: Kauppakamari.

Hildebrandt, M. (2008). 'Profiling and the identity of the European citizen', in Hildebrandt, M. and Gutwirth, S. (eds.) Profiling the European Citizen: Cross-Disciplinary Perspectives. Dordrecht: Springer Science + Business Media B.V., p. 303–343.

Hirvonen, A. (2011). Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki: University of Helsinki.

Husa, J., Mutanen, A. and Pohjolainen, T. (2008). Kirjoitetaan juridiikkaa. Helsinki: Talentum.

Hölzel, J. (2019). 'Differential privacy and the GDPR', European Data Protection Law Review, 5, p. 184–196.

Jordan, M I, and T M Mitchell. (2015). “Machine learning: Trends, perspectives, and prospects.” Science (New York, N.Y.) vol. 349,6245: p. 255–260.

Keller, M. (2023). Mitä on tietosuoja? Helsinki: Alma Talent.

Kindt, E. J. (2016). 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation', Computer Law & Security Review, 32(5), p. 729–748.

Kolehmainen, A. (2016). 'Tutkimusongelma ja metodi lainopillisessa työssä', in Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Helsinki: Edita Publishing Oy, p. 105–132.

Koskinen, I. (2018). 'Koneoppiminen ja EU:n yleisen tietosuoja-asetuksen vaatimus lainmukaisesta, kohtuullisesta ja läpinäkyvästä käsittelystä', Defensor Legis, N:o 2, p. 240–256.

Lee, H., Kim, S., Kim, J.W. (2017). Utility-preserving anonymization for health data publishing. BMC Med Inform Decis Mak 17, 104.

Leiser, M. R. and Dechesne, F. (2020). 'Governing machine-learning models: challenging the personal data presumption', International Data Privacy Law, 10(3), p. 187–200.

Lynskey, O. (2015). The Foundations of EU Data Protection Law. Oxford Studies in European law.

Mechelli, Andrea & Vieira, Sandra. (2019). Machine Learning: Methods and Applications to Brain Disorders. Elsevier.

Meszaros, J. and Ho, C. (2021). 'AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?', Computer Law & Security Review, 41.

Mueller, J. P., Massaron, L., & Massaron, L. (2016). Machine learning for dummies (1st edition.). Wiley.

Myrsky, M. (2011). Ennakkopäätökset verotuksessa. Helsinki: Alma Talent.

Määttä, T. and Paso, M. (2019). Johdatus oikeudellisen ratkaisun teoriaan. Helsinki: Helsingin yliopiston oikeustieteellinen tiedekunta.

Pitkänen, O., Korpisaari, P., and Korhonen, R. (2017). 'Miten kansallista lainsäädäntöämme pitää muuttaa EU:n yleisen tietosuoja-asetuksen vuoksi?' in Korpisaari, P. (ed.) Viestinnän muuttuva sääntely: viestintäoikeuden vuosikirja 2016. Helsinki: Helsingin yliopiston oikeustieteellinen tiedekunta, p. 1–9.

Raitio, J. and Tuominen, T. (2020). Euroopan Unionin oikeus. 2. uudistettu painos. Helsinki: Alma Talent.

Sajama, S. (2016). 'Argumentaatio oikeustieteellisessä tutkimuksessa', in Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Helsinki: Edita Publishing Oy, p. 24–50.

Sartor, G., & Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), Panel for the Future of Science and Technology. European Parliament.

Sharma, S., Menon, P. (2020). Data privacy and GDPR handbook (1st edition.). John Wiley & Sons.

Singh, J., Walden I., & Crowcroft, J. (2016). ‘Responsibility & Machine Learning: Part of a Process’ University of Cambridge.

Sokol, T. (2024). 'European Health Data Space, use of data and data subjects’ control over their own health data: Can an opt-out restore the balance?', European Journal of Health Law, 31(4), p. 365–388.

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Stalla-Bourdillon, S. and Knight, A. (2018). 'Data analytics and the GDPR: friends or foes? A call for a dynamic approach to data protection law', in Leenes, R., van Brakel, R., Gutwirth, S. and De Hert, P. (eds.) Data Protection and Privacy: The Internet of Bodies. Oxford: Hart Publishing.

Tarhonen, L. (2017). 'Pseudonymisation of personal data according to the general data protection law', Edilex.

Telaranta, K. A. (1990). Sopimusoikeus. Helsinki: Lakimiesliiton Kustannus.

Theodoridis, S. (2015). Machine Learning: A Bayesian and Optimization Perspective. (1st edition.) Academic Press.

Veale, M., Binns, R. and Edwards, L. (2018). 'Algorithms that remember: Model inversion attacks and data protection law', Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences.

Voigt, P. and Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR) – A Practical Guide. Springer International Publishing.

Wang, P. (2019). 'On defining artificial intelligence', Journal of Artificial General Intelligence, 10(2), p. 1–37.

Weitzenboeck, E. M., Lison, P., Cyndecka, M., and Langford, M. (2022). 'The GDPR and unstructured data: is anonymization possible?', International Data Privacy Law, 12(3), p. 184–206.

Internet Sources

Business Times. (2023, July 25). Sam Altman's rebranded Worldcoin ramps up iris-scanning crypto project. The Business Times. Accessed January 5, 2025, [https://www.business-times.com.sg/companies-markets/banking-finance/sam-altmans-rebranded-worldcoin-ramps-iris-scanning-crypto-project].

Crabtree, M. (2024). 'What is machine learning?', DataCamp, 8 November. Accessed 4 January 2025, [https://www.datacamp.com/blog/what-is-machine-learning].

IBM. (2021, August 4). What is artificial intelligence in medicine? Accessed January 5, 2025, [https://www.ibm.com/think/topics/artificial-intelligence-medicine].

Licensing International. (n.d.). What is Licensing? Accessed January 9, 2025, [https://licensinginternational.org/education/what-is-licensing/].

Quantib. (n.d.). Quantib ND. Accessed January 5, 2025, [https://www.quantib.com/solutions/quantib-nd].

OFFICIAL SOURCES

Article 29 Data Protection Working Party. (2007). Opinion 4/2007 on the Concept of Personal Data. WP 136.

Article 29 Data Protection Working Party. (2013). Opinion 03/2013 on Purpose Limitation. WP 203.

Article 29 Data Protection Working Party. (2014). Opinion 05/2014 on Anonymisation Techniques. WP 216.

Article 29 Data Protection Working Party. (2015). Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. WP 233.

Article 29 Data Protection Working Party. (2017). Guidelines on Transparency under Regulation 2016/679. WP 260 rev.01.

Article 29 Data Protection Working Party. (2017). Guidelines on Consent under Regulation 2016/679. WP 259 rev.01.

Centre for Information Policy Leadership. (2020). How GDPR regulates AI: A legal analysis. Accessed January 7, 2025, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf].

European Commission. (2009). Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries.

European Data Protection Board, (EDPB). (2020). Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.

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

European Data Protection Board, (EDPB). (2021). Document on Response to the Request from the European Comission for Clarifications on the Consistent Application of the GDPR, Focusing on Health Research.

European Data Protection Board, (EDPB). (2024). Guidelines 2024/01 on processing personal data based on legitimate interests.

European Data Protection Board, (EDPB). (2025). Guidelines 2025/01 on Pseudonymisation.

European Data Protection Supervisor, (EDPS). (2020). Preliminary Opinion 2020/8 on the European Health Data Space.

Ministry of Social Affairs and Health. (n.d.). Secondary use of health and social data. Accessed January 5, 2025, [https://stm.fi/en/secondary-use-of-health-and-social-data].

Court Decisions

Court of Justice of the European Union

Case C-518/07, *European Commission v Federal Republic of Germany*, ECLI:EU:C:2010:125, 9 March 2010.

Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:627, 6 October 2015.

Case C-582/14, *Breyer*, ECLI:EU:C:2016:779, 19 October 2016.

Case C-496/17, *Deutsche Post AG v Hauptzollamt Köln*, ECLI:EU:C:2019:26, 16 January 2019.

Case C-345/17, *Sergejs Buivids*, ECLI:EU:C:2019:122, 14 February 2019.

Case C-673/17, *Planet49 GmbH*, ECLI:EU:C:2019:246, 1 October 2019.

ABBREVIATIONS

AI	Artificial Intelligence
CFR	The Charter of Fundamental Rights of the European Union
CJEU	The Court of Justice of the European Union
DPD	Data Protection Directive
ECHR	The European Convention on Human Rights
ECtHR	The European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EHDS	European Health Data Space
EU	European Union
GDPR	The General Data Protection Regulation
TFEU	The Treaty on the Functioning of the European Union
WP29	Article 29 Data Protection Working Party

1. Introduction

1.1 Introduction to the Subject

The rapid development of technology and globalization have introduced new challenges to personal data protection. Personal data is now shared and collected on a much larger scale than before. Due to technological advancements, both private companies and authorities can use this kind of data more extensively than ever. Additionally, many individuals now share their personal data publicly on a global scale. Therefore, technology has transformed both the economy and social life.[1] Machine learning is a part of this revolution, and it has evolved over the past two decades from a research topic to a widely used technology. Artificial intelligence is now the go-to method for developing software in areas like computer vision, speech recognition, and robotics aiming to enhance the efficiency of other industries such as health care. Developers often find it easier to train systems using examples of desired input-output behavior rather than manually programming every possible response. This often leads to using artificial intelligence (AI) for this kind of programming.[2]

Recent breakthroughs in computer science and informatics have positioned AI at the forefront of modern healthcare. AI-powered algorithms and applications increasingly support medical professionals in both clinical practice and ongoing research. Two of the most widespread applications of AI in healthcare involve clinical decision support and imaging analysis. Clinical decision support tools provide healthcare providers with quick, relevant information—helping them make informed choices about treatments, medications, mental health issues, and other patient needs. Meanwhile, AI-driven imaging solutions examine CT scans, X-rays, MRIs, and other diagnostic images to detect potential lesions or abnormalities that a human radiologist might miss.[3] As AI continues to integrate more deeply into our daily routines, it inevitably raises privacy concerns, especially when it involves health data. All AI systems undergo an initial learning phase before they become operational, during which they collect and analyze extensive

---

[1] Korpisaari et al. 2022 p. 75.
[2] Jordan–Mitchell, 2015, p. 256.
[3] IBM 2021, What is artificial intelligence in medicine? (https://www.ibm.com/think/topics/artificial-intelligence-medicine) (Accessed January 5, 2025).

datasets—often containing both personal and sensitive information. This process enables the system to build an algorithm capable of delivering context-relevant results and recommendations.[4]

Collecting and processing personal and sensitive data on psychiatric vulnerabilities—such as family history, hospitalization, or compulsory medical treatment—can threaten individuals' privacy in case this information becomes accessible or misused. Fraudulent or discriminatory practices, like denying or limiting services, are possible outcomes. To reduce these risks, anonymization and pseudonymization techniques can help prevent identification during AI-driven data processing. At the same time, organizations operating especially in healthcare must be transparent about data use and allow people to control the information they share. Recognizing these challenges, both national and European legislators stress the importance of regulations that safeguard data privacy in AI. This includes leveraging existing laws like the 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 (General Data Protection Regulation, GDPR), which promotes responsible data use, and introducing broader, cross-sector rules governing AI design, implementation, and oversight.[5] Such protective measures have been implemented, for instance in the context of health data, by introducing national regulations on the secondary use of health data[6]. Although AI offers significant benefits, balancing innovation with privacy is essential. Through vigilant oversight, strong regulations and informed users, AI and privacy can coexist securely and effectively.[7]

---

[4] De Filippis et al. 2024, p. 12–13.
[5] De Filippis et al. 2024, p. 13.
[6] Finland has enacted a dedicated law, the Act on the Secondary Use of Health and Social Data, to ensure the effective and secure processing of personal social and health data for management, supervision, research, statistics, and development. Another aim of this legislation is to uphold individuals' legitimate expectations, as well as their rights and freedoms, when processing personal data. See Ministry of Social Affairs and Health, "Secondary use of health and social data," (https://stm.fi/en/secondary-use-of-health-and-social-data) (accessed January 5, 2025).
[7] De Filippis et al. 2024, p. 13.

Studying and refining the legal framework for medical AI is vital for protecting privacy, upholding ethical standards, and maintaining the European Union's (EU) competitiveness in the global technology arena. By establishing a clear and comprehensive set of regulations that balance privacy safeguards with innovation, the EU's healthcare sector can attract significant research investments and encourage wide-ranging collaborations. This approach enables the region to stay at the forefront of AI-driven healthcare, instead of lagging behind markets like the United States or China, by creating an environment where robust legal protections and technological advancements can flourish. Such a framework does more than prevent data misuse; it also builds the trust required for large-scale adoption of AI solutions in clinical decision-making, imaging analysis, and broader patient care. When individuals and healthcare providers have confidence in responsible data handling, they are more inclined to embrace AI-driven tools, which drives further innovation in the sector. This trust benefits patients, research institutions, and the broader industry by paving the way for safer, more reliable AI applications. In turn, a transparent and effective regulatory environment fuels economic growth and supports ongoing improvements in healthcare, empowering the EU to excel in both the technological and medical fields.

The results of this study provide critical insights into how privacy-preserving techniques, such as anonymization and pseudonymization, can reconcile the GDPR's consent requirements with the practical demands of AI development, particularly for processing sensitive health data. By addressing the legal and technical challenges of ensuring valid consent and maintaining data utility, this research highlights pathways for more effective GDPR compliance in AI training. From a regulatory perspective, the findings underline the need for clearer guidelines that define the boundary between personal and anonymized data and address the risks of re-identification, thereby reducing ambiguity for developers.

For AI developers and healthcare organizations, the study also emphasizes the importance of clearly defining the roles and responsibilities of all parties involved in processing health data. By understanding and adhering to GDPR requirements, developers and hospitals can adopt practices that safeguard sensitive health data while proceeding with innovation in the healthcare

sector. Furthermore, by leveraging privacy-preserving techniques and robust data governance strategies, AI developers and healthcare organizations can ensure compliance with legal frameworks while fostering trust among patients, investors, and the broader public. This trust is essential for gaining acceptance of AI-driven technologies in healthcare, where transparency and reliability are paramount. Ultimately, the study demonstrates how balancing privacy protection with innovation can promote responsible AI development that benefits individuals and the healthcare system as a whole.

1.1 Research Questions, Exclusions and the Structure of this Study

Data collection is a fundamental element of research study design involving human participants. In medical research, researchers typically adopt one of two approaches. The first approach involves conducting a study and enrolling participants by gathering data directly, which is known as a prospective study. The second approach involves utilizing previously collected data, such as information stored in biobanks or existing medical records and is referred to as a retrospective study.[8] Both of the approaches have their own difficulties, but they can be used if certain conditions of the GDPR are met. The development of artificial intelligence requiring health data or even biometric data, such as medical AI systems, e.g. Quantib® Neurodegenerative[9] or AI-powered KYC applications like World Network[10], necessitate the use of training data. AI developers would ideally prefer to use anonymous data for AI development, as the GDPR does not apply

[8] Anwana et al. 2024, p. 102–103.
[9] Quantib® Neurodegenerative is an AI-based software solution designed to help radiologists assess brain atrophy and monitor the progression of white matter hyperintensities. It supports both single-time-point and longitudinal analyses by segmenting brain structures and quantifying their volumes, including WMH (white matter hyperintensities). See Quantib, Quantib ND. (https://www.quantib.com/solutions/quantib-nd) (Accessed January 5, 2025).
[10] Worldcoin is a cryptocurrency and digital identity project founded by Sam Altman, the CEO of OpenAI. It aims to create a global identity and financial network by offering a "World ID" tied to proof of personhood through biometric verification, done via a device that scans individuals' irises. See (https://whitepaper.world.org/)and Sam Altman's rebranded Worldcoin ramps up iris-scanning crypto project. The Business Times. (https://www.businesstimes.com.sg/companies-markets/banking-finance/sam-altmans-rebranded-worldcoin-ramps-iris-scanning-crypto-project) (Accessed January 5, 2025).

to anonymous data.[11] However, in order to obtain anonymous data, high-quality health and biometric data must first be anonymized. Depending on the intended use of the AI, the data may not even be intended for anonymization. From a legal standpoint, one major challenge in AI development is defining where personal data ends and anonymized data begins. The GDPR considers information that can be indirectly linked to an individual as personal data, which makes it difficult to draw a clear legal line between what is truly anonymized and what remains personal. This distinction is not entirely clear in legal terms.[12]

Machine learning is often difficult to understand and lacks transparency, thus it is challenging to fully comprehend. [13] Understanding how machine learning works is essential for addressing security issues related to personal data. Since machine learning often involves processing large amounts of sensitive information, especially in the medical field, it is important to know how the data is processed in the development phase of AI to ensure that the personal data is protected. This is especially important in medical AI, where privacy is crucial. The challenges of complying with the GDPR add another layer of complexity. Therefore, this thesis investigates the basics of AI, machine learning, and privacy safeguards like anonymization and pseudonymization as key factors of the privacy side of AI development and explores how the GDPR applies to this kind of AI development, where a lot of health data is being used in the training process. This study focuses on medical AI systems designed to assist healthcare professionals, such as doctors and radiologists, by analyzing medical data like X-rays, MRI scans, or images of cancerous tissues. These systems are not intended to make fully automated decisions but rather to serve as tools that support clinical decision-making by providing enhanced diagnostic insights and aiding in the interpretation of complex medical information.

The research questions formulated in this thesis aim to address these complex challenges by focusing on the interplay between anonymization, pseudonymization, and GDPR compliance in

---

[11] Recital 26 of the GDPR: 'The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.
[12] Centre for Information Policy Leadership 2020, p. 3; GDPR Article 4.
[13] Koskinen 2018, p. 247.

the development of medical AI systems. Specifically, the primary research question is: How do anonymization and pseudonymization as privacy-preserving techniques reconcile GDPR consent requirements with the ethical and practical demands of using health data for AI development?

Additionally, this thesis addresses the following secondary research questions:

1. What are the legal and technical challenges in ensuring valid consent for the use of health data in AI systems, particularly under GDPR requirements?
2. How do the concepts of anonymization and pseudonymization influence the applicability of GDPR's provisions on consent and the categorization of personal data in AI contexts?
3. To what extent can the balance between data innovation and individual control be achieved within the GDPR framework when processing health data for AI development?

These questions are particularly significant as they address the dual necessity of fostering innovation in AI development while safeguarding individual rights under the GDPR framework. The research questions formulated in this thesis aim to address these complex challenges by focusing on the interplay between anonymization, pseudonymization, and GDPR compliance in the development of medical AI systems. Specifically, they explore how these privacy-preserving techniques can reconcile the legal requirement for consent with the practical demands of processing sensitive health data for AI training. This focus is particularly significant given the dual necessity to foster innovation in AI development while safeguarding individual rights under the GDPR framework. By addressing these questions, the thesis seeks to provide a structured analysis of the legal, ethical, and technical implications of processing health data for AI, shedding light on how compliance can be achieved without stifling technological progress. The answers to these questions not only aim to clarify ambiguities in the application of GDPR principles but also to contribute to the broader discourse on balancing privacy and innovation in the evolving field of AI.

In this thesis, the obligations imposed on AI developers by the The Regulation Laying Down Harmonized Rules on Artificial Intelligence (AI Act) regarding the use of health data for AI development are excluded due to the unique considerations they entail. Instead, the focus is placed on the requirements set out by the GDPR that influence the entire AI development process from the perspectives of both hospitals and AI-developing companies. It is important to note that although the GDPR may no longer apply once the AI developer processes only anonymized health data, the provisions of the AI Act still remain in effect, even for anonymized data.[14]

1.2 Research methods

The core of jurisprudence is considered to revolve around two questions: whether the law is valid and what its content is. The question regarding the content of jurisprudence is answered through legal doctrine.[15] In jurisprudence, the concept of "knowledge interest" concerns the type of research knowledge that a study aims to achieve. The knowledge interest of legal doctrine is to produce well-reasoned interpretations, evaluations, and systematizations of existing law and its provisions.[16] Legal doctrine, or legal dogmatics generally refer to the interpretation of current law in jurisprudence, meaning the study and systematization of the content of legal rules.[17] Legal doctrine organizes current law by arranging the legal norms established by the legislature into a coherent and unified legal system.

In systematization, it is essential to examine and organize the relevant concepts, legal principles and theories of different branches of law. Legal doctrine can therefore be divided into practical

---

[14] Even if health data used to develop a high-risk AI system is anonymous, the AI Act still imposes strict requirements for the AI systems. Developers must ensure datasets are accurate, representative, and free from bias to prevent harmful or discriminatory outcomes. Risk management systems must identify and mitigate risks throughout the AI lifecycle, ensuring compliance with safety and ethical standards. Transparency and technical documentation are required to inform users about the system's purpose, limitations, and training process. Additionally, human oversight must be incorporated to allow intervention if the system produces harmful or inaccurate outputs. See AI Act art. 9–10, 13–15.
[15] Aarnio 1988, p. 46–48.
[16] Kolehmainen 2015, p. 2.
[17] Hirvonen 2011, p. 22.

legal doctrine and theoretical legal doctrine. Theoretical and practical legal doctrine interact with one another. Systematization requires that legal norms have been interpreted, while in-depth interpretation of norms, in turn, requires the systematization of the branch of law. [18]

Thus, it can be stated that legal doctrine examines what constitutes valid law and what impact legal norms and materials from other legal sources have.[19] Legal doctrine was chosen as the research method for this thesis because it aligns with the purpose and objectives of the study. It aims to clarify the content of existing legal norms and the significance of other legal sources in relation to current law, as is the intention in this thesis regarding the GDPR and European case law, particularly in the context of consent and AI development. While the primary focus of this thesis is on the requirements set out by the GDPR, particularly concerning consent and data protection, other relevant legislative frameworks, such as the AI Act, are also considered. These additional frameworks are used to support and contextualize the analysis of GDPR compliance, ensuring a comprehensive examination of the regulatory landscape affecting the development and use of medical AI systems.

In addition to interpretation, a key task of legal doctrine is to systematize, that is, to structure existing law by creating and developing a legal conceptual framework.[20] Systematization has therefore been regarded as a continuation of the legislator's work.[21] In this thesis, I organize legal information derived from the GDPR from the perspective of health data, data privacy and medical AI development, focusing on aspects relevant to this viewpoint. This includes addressing areas that the legislator may have overlooked or insufficiently regulated with the level of detail necessary for AI development. Systematization is seen as a process incorporating elements of translation, interpretation, and condensation, in which fragmented information is organized into clear, manageable units.[22] In my thesis, I systematize the GDPR, making it easier

[18] Hirvonen 2011, p. 25. See also Määttä – Paso 2019, p. 8. Practical legal research focuses on the ambiguities found in various legal texts, aiming to clarify and refine their meaning through systematic study.
[19] Hirvonen 2011, p. 23.
[20] Husa–Mutanen–Pohjolainen 2008, p. 20; Hirvonen 2011, p. 25.
[21] Kolehmainen 2016, p. 128.
[22] Sajama 2016, p. 40.

to handle from the perspective of medical AI development by breaking it into cohesive parts. This systematization is essential for identifying the sections of the GDPR most relevant to the development of medical AI. In turn, systematization enables interpretation to be directed toward the most pertinent aspects.

Aarnio has observed that jurisprudence, in its legal sense, is not merely about describing the legal system—it also enables the reconstruction of the legal order.[23] My thesis adopts a reconstructive research approach as a central methodology. The unique characteristics of AI development have not been adequately addressed in the current GDPR framework. Therefore, the objective is twofold: to identify the issues within the current legal landscape and to determine how these challenges should be addressed through interpretation.

Husa has noted that legal academic work can incorporate elements from other disciplines, as long as the core issue remains legal.[24] While the framework of my thesis is legal under the GDPR, it also includes aspects from the field of information technology. The core of my thesis is legal-dogmatic, focusing on legal issues, but I have laid the groundwork for these by exploring methods and mechanisms of AI in business. This journey starts with fundamental concepts of personal data and data protection and leads to AI systems and their learning mechanisms. To interpret the GDPR specifically from the perspective of AI development, it is essential to understand the unique characteristics of AI systems in sufficient detail to compare them with other forms of data processing. This enables an appreciation of their specific legal requirements under the regulation. Moreover, in today's—and especially tomorrow's—work environment, a lawyer must have at least a foundational understanding of technology. This knowledge is crucial for assessing the legality of AI development processes in relation to the GDPR.

Husa defines the crucial role of legal dogmatics as addressing uncertainty regarding the content of the legal order.[25] The interpretive task requires the law to be understood within the prevailing

[23] Aarnio 2006, p. 238.
[24] See Husa–Mutanen–Pohjolainen 2008, p. 9.
[25] Husa–Mutanen–Pohjolainen 2008, p. 20.

framework at any given time. According to Myrsky, because the interpretive questions in a given case are not always clear, the identification of the interpretive issue itself is also part of legal research.[26] The aim of my thesis is to examine and clarify sections of the GDPR that require interpretation from the perspective of AI development using health data. Although my focus is on a specific area of AI development, I believe the findings of this thesis will provide insights into broader issues related to personal data and processes involving AI development.

1.3 Key terminology and concepts

1.3.1 Data Privacy and Personal Data in The Context of AI Development

Data protection is an independent fundamental right in the EU Charter of Fundamental Rights CFR). The European Court of Human Rights (ECtHR) has ruled that the right to privacy covers data protection, although the European Convention on Human Rights (ECHR) does not specifically mention data protection or the protection of personal data.[27] The concept of data privacy emerged with the rise of the internet and widespread adoption of computers and mobile phones in the late 20th century. Before this, privacy was limited to physical aspects such as individuals, homes, documents, and personal life. Privacy norms rely heavily on trust and fiduciary responsibility, with an expectation that shared data will not be disclosed without consent. While sharing personal information is often necessary, it is done within defined relationships and boundaries.[28] The widespread use of personal data, especially in business, is a part of today's modern world and has a crucial role in enhancing Europe's competitiveness in international markets. This kind of usage of personal data can be very beneficial for society, when it is managed in a way that ensures that personal data cannot be used for any purpose or transferred to third party without ensuring compliance with the GDPR.[29]

---

[26] Myrsky 2011, p. 181.
[27] Keller 2017, p. 79.
[28] Sharma et al. 2020, p. 5–6.
[29] Keller 2017, p. 79–80, 154.

The evolution of technology complicates the establishment of privacy boundaries. While laws can address explicit breaches like hacking, the use of personal data for research, advertising, or resale introduces challenges in assessing harm and assigning liability, especially for non-monetary damages. Data collected through browsing habits, purchases, or preferences further blurs these lines. Such practices have driven the evolution of data privacy principles, adapting traditional notions of privacy to a digital world. This modern framework seeks transparency and control over data use, reflecting a shift from physical to information-based privacy concerns.[30]

For centuries, as technology has slowly advanced, privacy has been an ongoing concern. However, it was not until the twentieth century, especially with the arrival of computers, that privacy became a major global issue. From the 1960s onward, the issue of privacy gained more and more attention and was increasingly examined. In many respects, this underlying concern has not significantly changed. As philosopher Thomas Nagel has observed, recent decades in the United States have witnessed "a disastrous erosion of the precious but fragile conventions of personal privacy."[31] As the usage of personal data grows exponentially, it is essential to ensure that personal data is being used according to law. Special attention should be given to European personal data by ensuring compliance with the GDPR, when the data is being transferred outside of Europe. With the advent of new technologies such as artificial intelligence and the continuous growth of social media presence, it can be observed that data protection issues are increasing despite new legislation.

Data protection challenges in the United States are also reflected in Europe, as many U.S. social media and technology companies have customers and business partners in Europe, to whom EU legislation applies. The complexity is further increased by the fact that these companies may store their cloud services in the United States, meaning that European personal data is also kept outside of Europe. AI companies from third countries may also be subject to GDPR regulations.

---

[30] Sharma, et al. 2020, p. 6–7.
[31] Solove 2008, p. 4–6.

It is especially important to carefully assess the situation regarding these companies based outside of EU developing AI, as they must strictly adhere to the GDPR if they are using European personal data in the development of their AI.

Article 4 of the GDPR defines "personal data" as any information relating to an identified or identifiable natural person, referred to as the "data subject." An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifiers, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. In the context of the GDPR, the term "natural person" primarily refers to the fact that data protection applies to individuals, regardless of their nationality or place of residence. The right to personal data protection is universal, and individuals' fundamental rights and freedoms must be respected, no matter their background.[32]

In this sense the concept of personal data is defined quite broadly in the GDPR. Personal data encompasses both direct and indirect identifiability. For example, a property identifier or an address qualifies as personal data because it can be "linked to a natural person by using additional information," and the means to identify the natural person are reasonably available. Personal data can be either confidential or public. For instance, personal data found on the internet must be processed in accordance with the requirements of the GDPR. Personal data does not necessarily refer to sensitive or intimate information; what is decisive for the concept of personal data is that the information relates to an identifiable person.[33] The definition of personal data is generally clear, though there are some exceptions. A key limitation is that in the context of the GDPR "natural person" only refers to living individual, unless a Member State has explicitly provided for it in its own data protection legislation.[34] As a result, GDPR applies only to the personal data of living people. However, data concerning deceased individuals can still relate to

[32] WP 136, Opinion 4/2007, p. 21.
[33] Korpisaari et al. 2022, p, 58,60–61.
[34] GDPR, Reticle 27.

living, identifiable people, and must be handled according to the GDPR. This effects legal entities as well. Legal entities, such as companies, are not protected under the GDPR for their "personal data." GDPR only applies to natural persons. Though, information about legal entities can sometimes be linked to identifiable individuals, such as company executives or owners, and in these cases, the data must be treated as personal data.[35]

Personal data does not have to be accurate or verified; it can also include incorrect information. Previous case law has determined that, for instance, personal identification numbers, fingerprints, vehicle registration numbers, photographs, customer cards, computer IP addresses, or even street addresses qualify as personal data if they can be linked to a specific natural person. These interpretative principles continue to apply.[36] Health data, as defined by the GDPR, refers to any personal information about an individual's physical or mental health. This can include details about past, current, or future health conditions, such as medical history, diagnoses, treatments, X-rays and different kinds of test results. It also covers identifiers like health insurance numbers or information from tests, genetic data, and biological samples. Essentially, it includes any data that provides insight into a person’s health, whether it comes from doctors, medical records, health devices, or diagnostic tests.[37]

1.3.2 The Parties Involved in the Processing of Personal Data

The GDPR identifies several key parties involved in the processing of personal data. These entities have different roles and responsibilities, which are crucial for ensuring compliance with data protection requirements and safeguarding the rights of data subjects. The primary roles defined under GDPR include the **controller**, **processor**, **recipient**, and **third party**, each playing a specific part in the processing lifecycle of personal data.

---

[35] WP 136, Opinion 4/2007, p. 22–24.
[36] Korpisaari et al. 2022, p 62–63; C-582/14, Breyer.
[37] GDPR, Reticle 35.

According to Article 4(7) of the GDPR, a controller is defined as the natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data. The data controller is determined by actual control over the use of personal data. The controller is the party that decides what data is collected, where it is stored and processed, its purpose, and how it is used. What matters is the actual control, not whether the data processing is legal or illegal, or whether the controller has direct access to the data being processed.[38] A data controller can be defined either by determining the purposes and means of data processing or by law. Under Article 26 of the GDPR, joint controllers are those who jointly decide on processing purposes and methods. They must have a transparent agreement outlining their responsibilities, which must be accessible to the data subject.[39]

According to the EDPB, the concepts of data controller, joint controller, and data processor are "functional concepts," as they aim to allocate responsibilities based on the actual tasks and independent roles of the parties involved. The legal status of the entity is determined by its actual activities, rather than by the role described in a contract.[40] Controllers are the primary decision-makers in the data processing chain, as they decide why and how personal data should be processed. In the still developing AI with medical data, the controller could be the hospital if it determines the purposes and means of processing the personal data. However, if the AI developer jointly decides with the hospital on how the data will be used, both parties may be considered joint controllers, and they must establish a clear agreement outlining their respective responsibilities under the GDPR.

It is essential to determine the controller, as the role of the controller carries significant responsibilities under the GDPR. As specified in Recital 78, controllers are required to implement measures that ensure compliance with the Regulation's principles, including lawfulness, fairness, transparency, data minimization, and accountability.[41] These responsibilities include e.g. obligations such as conducting in certain circumstances Data Protection Impact Assessments

[38] Korpisaari et al. 2022, p. 74.
[39] Korpisaari et al. 2022, p. 75; EDPB, Guidelines 07/2020.
[40] EDPB, Guidelines 07/2020, p. 3, 10.
[41] GDPR, Recital 78.

(DPIAs) under Article 35 and ensuring that any processors they engage adhere to GDPR requirements through binding agreements, as stipulated in Article 28.

A processor on the other hand has been defined in Article 4(8), as a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. Data controllers often outsource tasks that involve personal data processing to service providers. These providers act as processors on behalf of the controller, handling data under the controller's instructions. The main difference between a controller and a processor is that the processors act under the instructions of the controller and are prohibited from determining the purposes or methods of processing. Their role of processor is limited to operational aspects of data handling, such as storing, transmitting, or analyzing personal data as directed by the controller.[42] According to the EDPB, two basic conditions define a data processor: the processor must be a separate entity from the controller and must process personal data on behalf of the controller.[43]

The key factor drawing a line between a data controller and a processor acting on behalf of the controller is who determines the purpose and methods for data processing. A processor becomes a controller if it begins using the data for its own purposes, contrary to the controller's instructions.[44] The Data Protection Working Party has stated in their opinion that when determining the distinction between a data controller and a processor, factors such as the quality of the controller's prior instructions, and the level of control the controller has over the processor's actions should also be considered.[45]

Under GDPR, processors have strict obligations to ensure data security and compliance. For instance, article 28(3) requires that a processor and controller enter a binding contract that defines the scope and purpose of processing, as well as the processor's responsibilities. Processors must also implement appropriate technical and organizational measures to safeguard data, such

[42] Korpisaari et al. 2022, p. 75. European Commission 2009, Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries, p. 10–11.
[43] Korpisaari et al. 2022, p. 77; EDPB, Guidelines 07/2020.
[44] Korpisaari et al. 2022, p. 77.
[45] WP 169 Opinion 1/2010, p. 28.

as encryption or pseudonymization, to protect the confidentiality and integrity of personal data.[46] Processors are common in contexts where specialized data handling or storage services are outsourced.

A recipient refers to any natural or legal person, public authority, agency, or other body to whom personal data is disclosed, regardless of whether they are a third party. However, public authorities receiving data in the framework of a particular inquiry under Union or Member State law are not considered recipients, provided that their processing complies with applicable data protection rules.[47] It is important to understand the role of the recipient in the processing of personal data, as the term "recipient" is connected e.g. to a data subject's right to know how their information is being shared (as outlined in Articles 13–15 and 19 of the GDPR). The data subject must be informed about which parties may receive their personal data. Depending on the development process, this information can include both the data controller and the processor as potential recipients.[48] In the development of AI with data classified as personal data, the concept of a recipient refers to whom personal data is shared within and outside the organization. Recipients may include entities like subcontractors, healthcare partners, or external collaborators who handle the data for processing. The GDPR ensures that any data shared with these recipients is done so in a way that complies with privacy rules, especially when it involves transferring data to third-party organizations working on developing AI, ensuring data protection throughout the development.

A third party in the processing of data is a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and those authorized to process data under the direct authority of the controller or processor.[49] A third party is an entity that neither participates in processing personal data nor is directly affected by the processing. For example, according to Recital 54 of the GDPR, when processing an employee's health data, the employer,

[46] GDPR, Recital 78.
[47] GDPR, Article 4(9).
[48] Korpisaari et al. 2022, p. 78.
[49] GDPR, Article 4(10).

insurance company, or bank can be considered a third party.[50] Third parties are typically external entities or individuals who aren't directly involved in processing the data but may interact with it in certain situations, such as company anonymizing the personal data or other external service providers. Even though third parties are not directly parties involved in processing, they still need to comply with the GDPR to the extent that they interact with personal data under the direct authority of controller or processor. The GDPR ensures that third parties follow strict data protection standards. For example, Article 28(4) requires that any sub-processors hired by the main processor must have the same contractual obligations, creating a system of accountability. This kind of framework helps prevent unauthorized access to personal data and ensures data protection standards are upheld throughout the process, even in the situations where third parties are involved.

A data subject refers to an individual whose personal data is being processed, specifically a natural person. Company information is not classified as personal data, and businesses are not considered data subjects under the GDPR. However, individuals representing a company, such as contacts or other employees, are considered data subjects, and the processing of their personal data (e.g., name, address, phone number) is covered by the regulation.[51] In the development of AI a data subject refers to an individual whose personal data is being used in the development process. If the AI is being developed with health data this could include patients whose health information, such as X-rays, medical records, or diagnostic results, is used to train AI models. Even though legal entities such as companies themselves are not considered data subjects under the GDPR, individuals associated with these organizations are protected by the regulation if their employers data that includes their personal health data, is being used for AI development.

[50] Korpisaari et al. 2022, p. 79.
[51] Hanninen et al. 2017, p. 20.

1.3.3 Processing of Data

The GDPR defines processing in article 4(2) as any operation or set of operations performed on personal data or sets of personal data, whether by automated or manual means.[52] This definition encompasses a wide range of activities, including collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, dissemination, or otherwise making available, as well as alignment, combination, restriction, erasure, and destruction of personal data.[53] Since the definition of "processing" in the GDPR is principally the same as in the previous Data Protection Directive (DPD), as the Court of Justice of the European Union (CJEU) rulings on the meaning of "processing" under the DPD are still relevant for interpreting the term within the GDPR.[54] The CJEU has interpreted the definition of 'processing' under the DPD in several cases[55]. These cases demonstrate that the term 'processing' covers a broad range of activities.[56] For instance CJEU has ruled that such activities as the act of publishing a video recording, which, contains personal data and the transfer of personal data from an EU Member State to a third country is processing of personal data[57]. In this sense also transferring personal data inside the EU from one legal entity to another, should be seen as processing of personal data.

The definition of processing is undeniably quite broad, indicating that whenever personal data is used in any way or for any purpose, it is considered processing.[58] The CJEU has pointed out that "processing" can include a variety of actions, each corresponding to a different stage in handling personal data. Essentially, the term covers any activity involving personal data, regardless of how long it takes, how much data is processed, or whether the data is formally recorded. The Article 29 Data Protection Working Party (WP 29) shared this view in its Opinion 03/2015

---

[52] Article 4(2).
[53] GDPR, Article 4(2); Recital 26.
[54] Bygrave et al. 2020, p. 118; Case C- 40/ 17, Fashion ID (AG Opinion), para. 87.
[55] European Parliament and Council. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, L 281, 31–50.
[56] Bygrave et al. 2020, p. 118.
[57] Case C-345/17, *Sergejs Buivids*, para. 39; Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, para. 45.
[58] Hanninen et al. 2017, p. 20–21.

on data protection in criminal investigations, stating that even collecting data without storing or recording it still counts as processing.[59] The definition of processing should be interpreted in a way that preserves the high level of protection provided by the GDPR, as outlined in recitals 9-10.[60]

By using a broad definition of processing data, the GDPR makes sure that every stage of data handling, from collection to disposal, is covered by its rules. This approach highlights the Regulation's aim to provide strong protection for individuals, holding data controllers and processors accountable at every step of personal data's lifecycle. In medical AI development processing personal data means any action with the hospital's data, such as collecting, storing, using, or changing it. This kind of processing includes e.g. anonymizing data like X-rays and medical reports and using it to develop the algorithms of AI. Any handling of the data, from storage to use in AI development, is considered processing under the GDPR[61]. Therefore, the hospital and AI developer must both follow the GDPR regulations strictly at every stage of processing any data that might classify as personal data in the developing of AI.

1.3.4 Artificial Intelligence and Artificial Intelligence Systems

Artificial intelligence is a broad and multifaceted concept. Rather than being a single technology, it encompasses a range of methods, technologies, applications, and research directions. It can also be viewed as just one component within the broader framework of digitalization.[62] Therefore, it is not a surprise that arriving at a consensus on the definition of AI within the scientific community has proven challenging.[63] Although the AI Act is mainly excluded from the study it is notable that it defines artificial intelligence as a machine-based system designed

[59] Bygrave et al. 2020, p. 119; Case C- 40/ 17, Fashion ID, para. 72; WP 233, Opinion 03/2015, p. 7.
[60] Bygrave et al. 2020, p. 119.
[61] GDPR, Article 4(2).
[62] Ailisto et al. 2018, p. 6.
[63] Wang 2019, p. 1–2, 13–14.

to operate with varying levels of autonomy. These systems may exhibit adaptiveness after deployment and can infer how to generate outputs—such as predictions, content, recommendations, or decisions—from the input they receive. These outputs can influence both physical and virtual environments.[64]

It has been a longtime goal for computer science developers to program machines to simulate human intelligence by perceiving, reasoning, and acting autonomously. For AI to achieve this goal the computer science community has set it, it should have to be able to perform complex tasks that traditionally require human cognitive functions, including decision-making, problem-solving, and pattern recognition.[65] AI systems may not necessarily replace human doctors, but AI systems could still be a powerful help for health care. For example, in the medical field AI could fasten the work of doctors by pointing out signs of symptoms of patients, which could indicate some specific diseases. This could liberate doctors from doing the necessary manual work. This way doctors may just check whether the work from AI is correct and focus more on the side of health care which should not be given to the AI by law, making doctors a lot more efficient.

The concept of AI is in its nature multidisciplinary, connecting fields such as computer science, mathematics, and neuroscience.[66] It can be assumed that AI has been defined in the AI act and between professionals in different fields of science very broadly, due to it having such a multi-dimensional nature. As AI technology develops rapidly it is understandable that we need to assess the definition by the context it is being used in. In the light of data protection, it is not that important to have specific definition for AI, since the only thing that matters in the development of AI in the personal data protection perspective in this study, is that personal data is handled accordingly to the GDPR.

---

[64] AI act article 3(1).
[65] Günther, 2024, p. 59.
[66] Günther, 2024, p. 57; Ailisto et al. 2018, p. 6.

1.3.5 Machine Learning and Machine Learning Systems

Machine learning is a subset of artificial intelligence that automatically enables a machine or system to learn and improve from experience.[67] Machine learning is a complex concept. It is an umbrella-like term for many specific techniques that automatically learn from data to improve.[68] Machine learning is a branch of computer science that uses statistical methods to enable computers to learn from data and improve their performance on specific tasks without requiring explicit programming.[69] Machine learning is particularly useful in situations where humans either do not fully understand a phenomenon or where modeling it manually is nearly impossible due to the large amount of data involved. These problems can be extremely time-consuming or even unmanageable for humans. However, if enough data about the phenomenon is available, machine learning methods can be trained to analyze and solve the problem effectively.[70] Machine learning allows AI systems to learn patterns and make decisions with trained algorithm from data rather than relying on pre-defined instructions from the developer of the AI.[71] The process begins by training the system with a dataset, known as training data. During this phase, the algorithm adjusts its internal parameters to accurately classify the examples in the dataset or to make reliable predictions about a desired outcome based on the data provided.[72]

Training is the process where a learning algorithm is given a lot of different examples of inputs along with the desired outputs associated with those inputs. With this information, the algorithm learns to create a function that connects the inputs to the outputs. This way training helps the algorithm map a flexible function to the data. The result is often either a probability of a specific category or a numeric prediction.[73] In simplified terms the training data is made up of pairs, where each input (x) has a corresponding output (y). The goal is to make a prediction (y*) for a new input (x*) based on what the model has learned from the data.[74] For example to train a

---

[67] Crabtree, M. (2024, November 8). *What is machine learning?*. DataCamp. (https://www.datacamp.com/blog/what-is-machine-learning) (Accessed January 4, 2025).
[68] Günther 2024, p. 60.
[69] Ailisto et. al. 2019, p. 14.
[70] Ailisto et. al. 2019, p. 14; Mueller et. al 2016, p. 25.
[71] Mueller et. al. 2016, p. 30.
[72] Mueller et. al. 2016, p. 30; Ailisto et. al 2019, p. 14.
[73] Mueller et. al. 2016, p. 32.
[74] Jordan–Mitchell 2015, p. 257.

medical AI designed to assist radiologists in detecting possible cancers in X-rays, the AI must be trained with X-rays paired with their labels provided by radiologists as inputs[75]. These labels specify the desired output for each X-ray, such as whether cancer is present, where it is located, or any other relevant diagnostic information. AI learns from the inputs by analyzing the patterns in the labeled images, such as shapes, densities, or textures that are common in cancerous tissues. By training the algorithm learns to recognize these patterns and creates a function that predicts whether a new, unseen X-ray shows signs of cancer. After the training is completed, the AI can analyze new X-rays and provide probabilities or markers indicating areas that might need closer examination by the radiologist. This speeds up the process and helps ensure no potential signs are overlooked.

Machine learning is usually divided into three main approaches: supervised learning, reinforcement learning, and unsupervised learning. The most used method is supervised learning. In this method, the machine learns through supervision" or teaching.[76] Supervised learning is a method that has a goal of making connection from an input (e.g. X-ray) to an output decision (e.g. identifying a cancer). In this method the AI teaches itself human knowledge by developing its own way of connecting inputs and outputs that human supervisor says are correct.[77] Supervising does not need an actual teacher to make the outputs specifically for teaching AI, but the outputs must be made by human. The outputs can also be side products of real-life human activities, such as old patient records made by doctors. These input-output pairs help the system learn how to perform its task by recognizing patterns and making connections between the inputs and their corresponding correct responses.[78]

Reinforcement learning differs from supervised learning mainly from the feedback it receives from the learning process. As supervised learning training is based on output error data, rein-

[75] Labels as inputs are essentially the desired outputs that are paired with the inputs during the training process to teach AI.
[76] Sartor – Lagiola 2020, p. 10.
[77] Günther 2024, p. 61; Deo 2015, p. 1920.
[78] Sartor – Lagiola 2020, p. 10.

forcement learning focuses on acting and evaluating the outcomes based on rewards. In reinforcement learning the algorithm performs actions and receives feedback through a reward function that measures the success of those actions with a goal to build a model based on this process to maximize the reward. It is commonly used in robotics and game systems.[79] Reinforcement learning can be used to automate the process of preparing high-quality datasets by sorting through a large database of unorganized X-ray images and identify those most relevant for training a medical AI system at later stage with supervised learning. The key difference between supervised learning and reinforcement learning is that reinforcement learning gets its feedback as rewards and penalties based on action taken meanwhile supervised learning optimizes predictions through error minimizing.

Unsupervised learning on the other hand does not rely on labelling by humans. By this method the AI discovers its own ways of grouping data according to its own criteria without interpretation of a human observer. The main task for AI with learning of this kind, is to label data and reduce the data's complexity.[80] In this method the AI reduces the dimensionality of data by categorizing similar inputs into groups, which simplifies data by reducing the number of variables to analyze. Unsupervised learning is very valuable for data mining, it assists in preparing and labeling data, which can then be used in supervised learning models.[81] Unsupervised learning can be as efficient or even more efficient as reinforcement learning in preparing data for supervised learning depending on the quality of the AI system performing the learning, but as AI systems and AI overall is such a new phenomenon, it could be safer for AI developers to use reinforcement learning at the preparing stage to be more in control of the learning process.

[79] Singh et al. 2016, p. 7; Barto 2006, p. 98.
[80] Günther 2024, p. 61; Theodoridis 2015, p 12; Mechelli et al. 2019, p. 337.
[81] Singh et al. 2016, p. 7.

1.3.6 Algorithm

Machine learning is essentially built around algorithms. The term 'algorithm' is frequently used to describe AI applications, often in contexts such as "algorithmic decision-making," highlighting the role of algorithms as core components of AI systems processing data and generating outputs such as predictions, recommendations, or decisions.[82] In simple terms, algorithm is a procedure or formula for solving problems. It can be defined as a systematic set of operations to perform on a given data set. The goal is to produce a solution to a problem. In some cases, the algorithm is provided with inputs that help determine the result, but the primary focus is always on achieving the desired outcome. Algorithm uses immense datasets, known as big data[83], which is a dataset large enough for the algorithm to manage in a manner that allows for pattern recognition to make predictions.[84] Every AI system relies on an algorithm, with some of these algorithms specifically designed to handle tasks that are central to the system's AI-related functions, such as learning, reasoning, or decision-making.[85] Therefore, it is essential for this study to define algorithm. The role of algorithms is important to understand to assess the processing of personal data in the development of artificial intelligence, especially when the legal basis for processing personal data is the consent of the data subject.

An algorithm can also be understood as an abstract, formalized description of a computational procedure. Algorithms are expressed in programming languages and can vary significantly in complexity. Simpler algorithms may be used for tasks like alphabetizing word lists, while more complex algorithms are applied in areas such as speech recognition or generating predictions.[86] Algorithms can be categorized based on their characteristics or areas of application. For example, combinatorial algorithms focus on tasks such as counting and enumeration, numerical algorithms solve equations and provide numerical answers rather than symbolic ones, and probabilistic algorithms generate results that fall within specific levels of certainty.[87] Probabilistic

---

[82] Sartor – Lagiola 2020, p. 3–4.
[83] Big data source has a lot of detailed complex and depth data, that allows the user of data to solve problems. Mueller et.al 2016, p. 23.
[84] Mueller et.al 2016, p. 23, 30.
[85] Sartor – Lagiola 2020, p. 3–4.
[86] Sartor – Lagiola 2020, p. 3.
[87] Dourish 2016, p. 3.

algorithm is the most relevant algorithm for this study as most of the AI systems that are being developed the most with personal data and there may arise more security issues concerning personal data, though some combinatorial, numerical and probabilistic algorithms may also be developed such personal data that is numerical e.g. birth dates.

Some algorithms learn by themselves. Such algorithms may develop new problem-solving strategies, modify its internal data connections and weight, or even generate new algorithms in order to perform better its functions.[88] Even though whether an algorithm learns by itself or not is not relatively important in the context of this study, it is good to know that such algorithms also exist to fully comprehend what kind of legal problems might arise from different algorithms, as they are crucial part of machine learning.

1.3.7 Do AI Systems Store the Training Data?

There have been opposing opinions presented in legal literature, whether all AI systems retain data that can be classified as personal data. Veale, Binns, and Edwards (2018) argue that machine learning models may qualify as personal data due to their vulnerability to certain types of cybersecurity attacks, which can compromise data confidentiality. In their opinion they highlight the possibility of re-tracing the data from machine learning model back to the individual whose data has been used in the training of the model.[89] However, Leiser and Dechesne have criticized this view. In their opposing opinion they noted that unlike in the traditional decision-making systems[90], purely numerical representations of correlations can be found in the machine learning models, that it has learned from the training data by generating numerical outputs based on patterns. This means that unlike the training database, the model does not store the training

[88] Sartor – Lagiola 2020, p. 3–4.
[89] Veale et al. 2018 p. 6–9.
[90] In their opinion they also, viewed that even in the traditional decision or prediction systems the anonymized data as information is so abstract and generalized that it is "effectively meaningless for direct identification. Leiser–Dechense 2020, p. 191.

data. Even though the patterns learned from the training data may indicate whether certain specific data has been used as training data with enough context information, it does not mean that personal data could be located within the model.[91]

It indeed seems that machine learning models do not store data that could be classified as personal data, provided the patterns in the model are purely based on numerical representations of correlations. Even if one could get an output which might indicate to specific data, the model could only hint that similar data has been used for training as it only has patterns of such data, that may even be learned pattern from combination of similar data that has been used in the training. Some AI systems may even be designed on purpose to store all the data they learn from, although it may not be necessary for the AI systems to store the actual original data that may be considered as personal data. To avoid the obligations that may arise from the GDPR e.g. data subjects right to be forgotten, it is in the interest of the AI developers to develop AI systems that do not store the data that may be classified as personal data, as then there is no data in the core functions of the algorithms that are under the influence of the GDPR.

[91] Leiser–Dechense 2020, p. 191.

2 Normative Framework for Data processing in the Development of AI Systems

2.1 General Data Protection Regulation

Personal data protection is considered to be a fundamental right. As outlined in Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union (TFEU), all individuals are entitled to have their personal data protected.[92] 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) came into force on May 25, 2016, and its application began in the Member States on May 25, 2018. The GDPR was preceded by the Data Protection Directive, which aimed to implement the protection of private life and other fundamental rights safeguarding privacy when processing personal data, as well as ensuring the free movement of personal data between member states.

Achieving these two goals can sometimes require balancing. For example, in its judgment C-518/07 (Commission v. Germany), CJEU states that the role of the supervisory authority is "to achieve the right balance between privacy protection and the free movement of personal data."[93] These objectives present a challenge because they are inherently in tension with each other. The goals of protecting personal data and ensuring its free movement aim to achieve fundamentally different outcomes.[94] The tension arises from the fact that robust privacy protection often necessitates restrictive measures on data processing, which could limit the seamless flow of data. On the other hand, enabling the free movement of data requires a degree of flexibility in processing that may conflict with strict privacy safeguards. This duality creates a regulatory tightrope: overly stringent privacy measures could hinder innovation and cross-border data use, while excessive leniency might undermine individual rights. The supervisory authority's task,

[92] Korpisaari, et al 2022, p. 40.
[93] Korpisaari, et al 2022, p. 41; Case C-518/07, *European Commission v Federal Republic of Germany*.
[94] Lynskey 2015, p. 46.

therefore, is to navigate this delicate balance, ensuring that neither objective is disproportionately prioritized at the expense of the other.

Principles and rules concerning the processing of personal data must uphold the fundamental rights and freedoms of individuals, irrespective of their nationality or place of residence. The GDPR aims to establish a framework that supports the European Union's goals of freedom, security, justice, and economic union. It also seeks to foster economic and social progress by promoting the integration and convergence of economies within the EU's internal market, all while safeguarding the well-being of individuals.[95] This Regulation is designed not to obstruct the legitimate use of personal data in business but to define boundaries and responsibilities for its processing. By setting clear guidelines, it ensures that personal data can move freely across the EU without compromising data protection standards. This balance is essential to maintaining trust in digital and data-driven economies while enabling innovation and compliance within a unified regulatory framework.[96]

The GDPR is keeping the free movement of personal data in mind, intended to protect all natural persons within its scope, regardless of their nationality or place of residence. This means that the GDPR safeguards the personal data of an individual, even if they do not hold the nationality of an EU member state or have a permanent residence in an EU member state, as long as the GDPR applies to the processing of that person's personal data. For companies the GDPR may seem like an innovation killer, but the GDPR is not just restricting the use of personal data. It is instead, ensuring that the free movement of personal data happens in a manner that respects the fundamental rights of data subjects.

[95] GDPR, Article 1; GDPR, Recital 2.
[96] See Korpisaari et al. 2022, p. 42.

2.2 Material Scope

The GDPR is a general regulation governing the processing of personal data. The processing of personal data is also regulated by several hundred specific laws.[97] Although the GDPR as a regulation is directly binding on EU member states, they may impose stricter rules on the processing of personal data. It is noteworthy, however, that EU legislation cannot conflict with national legislation. In cases of conflict, EU law takes precedence over national law.[98] A regulation in European Union law has direct applicability within Member States if it does not require national legislative measures to be incorporated into domestic law[99]. This principle is clearly articulated in Article 288 of the TFEU, which states: "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States." Once treaties come into effect, they, along with regulations, become directly enforceable within the legal systems of the Member States. A natural or legal person can invoke a directly effective provision of European Union law in a national court. Direct effect applies only to specific articles that meet the necessary criteria, not to an entire regulation or directive as a whole.[100]

The limits of the European Union's legislative authority are defined in its founding treaties. Therefore, the GDPR cannot be applied to the processing of personal data carried out in connection with activities that fall outside the scope of EU legislation. Consequently, the GDPR does not cover matters related to the protection of fundamental rights and freedoms or the free movement of personal data that do not fall within the scope of EU law, such as activities concerning national security. Additionally, the GDPR does not apply to the processing of personal data by member states when carrying out actions related to the EU's common foreign and security policy.[101] The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing done by other than automated means of personal data which form part of a filing system or are intended to form part of a filing system.[102] The GDPR applies

---

[97] Korpisaari et al. 2022, p. 46.
[98] Raitio–Tuominen 2020, p. 234.
[99] As the GDPR is a regulation, it has direct legal effect. This means that a natural or legal person can invoke the GDPR in a national court as a directly effective source of European Union law.
[100] Raitio–Tuominen 2020, p. 241–242, 245.
[101] Korpisaari et al. 2022, p. 47.
[102] GDPR, Article 2(1).

to any activity involving the processing of personal data, including sensitive data such as health information, ensuring compliance with its principles across the EU. However, the regulation is not all-encompassing; its scope is limited to activities governed by EU law. For example, it does not apply to activities related to national security or to actions taken under the EU's common foreign and security policy.

In medical AI development, GDPR covers the processing of patient health data when it falls within the scope of EU legislation. Hospitals and AI developers operating in the EU must ensure their data processing activities comply with GDPR requirements, such as obtaining a lawful basis for processing, implementing appropriate security measures, and respecting data subject rights. The dual application of the GDPR and specific national laws adds complexity to the regulatory environment. For instance, while the GDPR provides a harmonized framework for personal data protection, member states may impose stricter rules on certain aspects, such as the secondary use of health data.

2.3 Territorial Scope

The territorial scope of the GDPR, as defined in Article 3, is quite broad. The regulation applies to the processing of personal data if 1) the controller or processor is established within the EU, or 2) the data of individuals located within the EU is processed in connection with the offering of goods or services, or 3) the behavior of individuals within the EU is monitored, or 4) the controller is established in a location where the law of a Member State applies under international public law. Article 3 is one of the most important provisions of the GDPR, as it defines whether, the GDPR applies or not. The rest of the Articles have no relevance, if the criteria set out in Article 3 are not met.[103] This applies to the processing of personal data carried out by a controller or processor established in the Union, even if the processing itself does not take place within the Union and the personal data concerns individuals located outside the Union. Estab-

[103] See Brygare et al. 2020, p. 81.

lishment requires actual operations and stable arrangements. The legal form of the establishment—whether it is a branch or a subsidiary with legal personality—is not decisive in this regard.[104]

The GDPR applies to data controllers and data processors with an establishment in the EU, or with an establishment outside the EU that targets individuals in the EU by offering goods and services (irrespective of whether a payment is required) or that monitor the behavior of individuals in the EU (where that behavior takes place in the EU). Factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union. Data controllers and/or data processors not established in the EU, but whose activities fall within the scope of the GDPR, will generally (some exceptions apply) have to appoint a representative established in an EU member state. The representative is the point of contact for all Data Protection Authorities (DPAs) and individuals in the EU on all issues related to data processing (Article 27).[105]

The territorial scope of the GDPR, as defined in Article 3, has significant implications for medical AI development involving hospitals, AI developers, and the use of patient health data. Whether the GDPR applies depends on the location and operations of the hospital and the AI developer, as well as the geographical origin of the patient data being processed. If the hospital or AI developer is established within the European Union, the GDPR applies to their processing of patient health data, even if the data subjects are outside the EU or the processing itself occurs outside the Union. Establishment requires actual operations and stable arrangements, but the legal form of the entity—whether it is a branch or a subsidiary—is not determinative. Similarly, if the AI developer or hospital is based outside the EU but targets individuals within the Union by offering goods or services or by monitoring behavior occurring within the EU, the GDPR

[104] Korpisaari et al. 2022, p. 54.
[105] Korpisaari et al. 2022, p. 54–56.

also applies. Indicators of targeting include the use of languages, currencies, or references to customers within the EU.

For entities not established in the EU but whose activities fall under the GDPR, Article 27 requires the appointment of a representative in an EU Member State. This representative acts as the point of contact for DPAs and data subjects concerning all GDPR-related matters. In medical AI development, this requirement ensures accountability and regulatory compliance even for entities operating beyond EU borders. The broad territorial reach of the GDPR thus ensures that the processing of patient health data for AI development adheres to EU data protection standards, regardless of where the entities or processing activities are located, provided the conditions of Article 3 are met.

3 General Grounds for The Development of AI With Personal Data

3.1. Protecting Data Through Guiding Principles

3.1.1 The Data Protection Principles

At the core of the GDPR lies Article 5, which outlines the key principles governing the processing of personal data, known as the data protection principles.[106] These principles are designed to protect individuals' rights and freedoms while enabling lawful data processing. They also serve as the foundation upon which all other GDPR obligations are built. The data controller must ensure compliance with these principles at every stage of personal data processing. A new key aspect in the regulation of data protection principles is the accountability requirement in Article 5(2) of the GDPR. This means it is not enough to simply follow the principles; the data controller must also be able to always demonstrate ongoing compliance. This requirement is known as the accountability obligation. These principles largely align with those found in Article 6 of the previous Data Protection Directive.[107]

The key principles outlined in Article 5 of the GDPR are:

1) The principle of lawfulness, fairness, and transparency in processing
2) The principle of purpose limitation
3) The principle of data minimization
4) The principle of accuracy
5) The principle of storage limitation
6) The principle of integrity and confidentiality
7) The accountability principle of the data controller

A violation of the principles outlined above may result in an administrative fine under Article 83(5) of the GDPR, which can be as high as €20 million, or for companies 4% of their total global annual turnover from the previous financial year, whichever is higher.

---

[106] Korpisaari et al. 2022, p. 99; Voigt – Von dem Bussche 2017, p. 87.
[107] Korpisaari et al. 2022, p. 99.

The principle of **lawfulness, fairness and transparency**, as set out in Article 5(1)(a), requires that personal data must be processed in a manner that complies with the legal grounds specified in GDPR Article 6 or where applicable, Article 9 for special categories of personal data. Under the GDPR, the basic rule is that personal data cannot be processed unless there is a valid legal basis for doing so.[108] Personal data processing must first and foremost be lawful, meaning there must be a legal basis for it. The lawful grounds for processing personal data are outlined in Articles 6 and 9–11 of the GDPR, as well as in various national laws. The lawful bases include such basis as consent, the performance of a contract, compliance with a legal obligation, protection of vital interests, performing a task in the public interest or exercising public authority and the legitimate interests pursued by the data controller. Processing based on a contract is also considered lawful, even if the contract is not explicitly stated in law.[109] The regulation generally prohibits the processing of special categories of personal data. However, such data can be processed if it has a specific legal basis, as outlined in Article 9 of the GDPR or in national laws of the member states. There are numerous such legal grounds, but it is important to note that these exceptions must be interpreted narrowly.[110]

Fairness involves treating individuals and their expectations with respect when their data is processed. It also requires that data is not misused. This principle protects people from undisclosed data gathering or other hidden processing and ensures they understand the nature and purpose of data use. In addition, fairness links to the principle of purpose limitation by restricting how data collected for one purpose may be used for another.[111] CJEU has emphasized that fairness means informing individuals about how their personal data is being used.[112] Fairness ensures that individuals are treated ethically and are neither deceived nor exploited. Transparency requires that individuals are adequately informed about the purposes and methods of data processing, typically through clear and accessible privacy notices.

---

[108] Voigt–Von dem Bussche 2017, p. 87.
[109] Korpisaari et al. 2022, p. 99–100; Feiler et al. 2018, p. 74.
[110] Korpisaari et al. 2022, p. 99–100; Feiler et al. 2018, p. 74.
[111] Korpisaari et al. 2022, p. 101.
[112] Case C-496/17, Deutsche Post AG v Hauptzollamt Köln, paragraph 59.

Transparency is an essential part of the first principle because data processing often occurs behind the scenes, and its effects might not be immediately visible to individuals. There is often an information gap between data controllers and individuals, with controllers knowing more about what data is collected, how it's used, and any new information derived from it. Meanwhile, the individuals concerned might not even know what data has been collected about them. This makes data processing difficult to understand and largely invisible to those affected.[113] Transparency along with GDPR Articles 13 and 14, ensure that people are aware of how their personal data is collected, used and shared. This prevents situations where the consequences of data processing only become clear later, such as when a decision that affects a data subject negatively is made about someone or when they discover their data is being used in ways they didn't expect.[114] Transparency means that individuals shouldn't have to search hard to find the information they need; it should be readily available on the same website where they provide their data.[115]

To maintain transparency, organizations must clearly inform individuals on how their personal data is handled. This information should be easily accessible and written in simple, straightforward language, as highlighted in Recital 39 of the GDPR. It should include details on who is processing the data, the purposes of processing and any relevant safeguards. Individuals also have the right to receive confirmation and notifications about how their data is being processed, including information on risks, rules, protections and their rights, along with instructions on how to exercise those rights. The obligation to provide information as part of transparency supports fulfilling the accountability requirement specified in Article 5(2) of the GDPR.[116] Being transparent and providing clear information not only ensures compliance with the law but also builds trust between data controllers and individuals. It encourages a trustworthy environment

[113] Korpisaari et al. 2022, p. 101; Hildebrand 2008, p. 308.
[114] Korpisaari et al. 2022, p. 101; De Hert et al. 2013, p. 139-140.
[115] WP 260 rev.01, Guidelines 2017, p. 8.
[116] Korpisaari et al. 2022, p. 102; WP 260 rev.01, Guidelines 2017, p. 5–6.

where data protection practices are regularly reviewed and improved, ensuring that personal data is handled responsibly throughout its entire lifecycle.[117]

When a hospital shares personal health data for AI development, it acts as the data controller, while the AI developer processes the data on its behalf. The hospital must adhere to GDPR principles of lawfulness, fairness and transparency. This means that they must have a legal basis for the processing of patient data, such as consent or legitimate interest. Patients should also be informed fairly and transparently, meaning that the patients should be able to clearly understand how their data is collected, who is handling it and the reasons for its use—whether for creating AI applications or anonymizing data for future projects. Both the hospital and the AI developer are responsible for ensuring that data processing is conducted legally and fairly, maintaining transparency throughout the entire process.

The **purpose limitation** principle, under Article 5(1)(b), dictates that personal data must be collected for specified, explicit, and legitimate purposes. Further processing of the data must not be incompatible with these original purposes, except where exceptions are provided, such as for scientific research, historical research, or statistical purposes, as outlined in Article 89(1). Purpose limitation restricts how a data controller can use the information collected on individuals. This principle encompasses two main aspects: first, personal data must be gathered for specific, explicit and legitimate purposes (purpose specification); second, the data cannot be processed in ways that are incompatible with those original purposes (compatible use).[118]

Purpose limitation allows data collected for one specific reason to be used for another, provided the new use is compatible with the original intent. This principle has two main objectives: firstly, it protects individuals' reasonable expectations on how their personal data is handled, and secondly, it enables the secondary use of personal data within certain boundaries.[119] In this sense, processing personal data for purposes other than those initially intended does not automatically

[117] Korpisaari et al. 2022, p. 102; De Hert 2013, p. 139.
[118] WP 203 Opinion 03/2013, p. 3.
[119] Korpisaari et al. 2022, p. 103.

mean that the new use is incompatible with the original purpose. Instead, each case should be individually assessed to determine whether the purposes are compatible.[120] Incompatible uses do not include activities such as archiving for the public interest, conducting scientific or historical research or performing statistical analyses, as outlined in Article 89 of the GDPR. The principle of purpose limitation allows for specific regulations regarding the processing bases mentioned in Article 6(1)(c) and (e) of the GDPR. These bases involve fulfilling the data controller's legal obligations and carrying out tasks in the public interest or exercising public authority. Additionally, Article 6(4) of the GDPR details the factors that must be considered when processing personal data for purposes different from those for which it was originally collected.[121]

Before the regulation was established, the Data Protection Working Party outlined key considerations for using personal data for purposes different from those for which it was originally collected. These considerations include:

1) **Alignment with Original Purpose**: Assessing how the new intended use relates to the initial lawful purpose for which the data was collected.
2) **Collection Context and Expectations:** Understanding the circumstances under which the personal data was gathered and the reasonable expectations of the data subject regarding its use.
3) **Nature and Impact of the Data**: Evaluating the type of data being processed and the potential effects of its processing on the individual.
4) **Ensuring Fair and Lawful Processing**: Ensuring that the data controller maintains fair and lawful handling of the data and prevents any excessive impacts on the data subject.[122]

[120] WP 203, Opinion 03/2013, p. 3.
[121] Korpisaari et al. 2022, p. 103.
[122] Korpisaari et al. 2022, p. 103; WP 203, Opinion 03/2013, p. 3.

In addition to the list, the data controller must consider the information initially provided to the data subject.[123] If additional data processing is considered feasible, the data controller must inform the individual about this further processing. Moreover, the controller needs to provide more details regarding the additional processing to ensure compliance with the principle of lawfulness, fairness and transparency.

This principle ensures that the scope of data processing remains clear and justified. However, it raises challenges in AI development, where data originally collected for one purpose might be repurposed for model training or further development of AI systems. In developing medical AI, the purpose limitation principle ensures that personal data collected by hospitals for specific healthcare purposes is used appropriately. When a hospital shares anonymized health data with an AI developer, this secondary use must align with the original reasons for data collection. Additionally, the hospital must inform patients about how their data is being anonymized and used for AI development, adhering to the principles of lawfulness, fairness and transparency. This approach protects patients' rights while allowing the advancement of medical AI within the regulatory framework.

The principle of **data minimization**, articulated in Article 5(1)(c), requires that personal data be adequate, relevant and limited to what is strictly necessary for the purposes for which it is processed. The wording of the article illustrates the close relationship between the principles of data minimization and purpose limitation. Both principles emphasize that there must be a clearly defined and justified need before collecting any data. Personal data processing should be limited to what is essential for the specific purpose defined. Data is only considered necessary if it is relevant and appropriate and not excessively broad in relation to the intended use. Data controllers should collect only the amount of data required to achieve their goals and ensure that the purpose cannot be reasonably fulfilled by other means. Additionally, the collected data must be directly related to its intended purpose.[124]

---

[123] WP 251, Opinion 1/2022, p. 12.
[124] Korpisaari et al. 2022, p. 104–105.

The principle of data minimization also requires that data must be deleted from records once it is no longer needed. In practice, this means collecting the least amount of personal data possible in each situation and removing any redundant or unnecessary information. Data controllers should avoid gathering data that might be needed in the future.[125] It is important to clearly define the necessity of data at the time of collection. While personal data can be collected and processed with the individual's consent, it must be ensured that consent does not grant the right to collect unlimited data or process personal information unnecessarily.[126] Data controllers must refrain from collecting excessive data, thereby minimizing risks associated with breaches or unauthorized access. In the context of AI development, compliance with this principle can be challenging due to the large datasets typically required for training algorithms.

While AI development often benefits from extensive data collection, controllers must strike a balance between data utility and compliance. Under GDPR, even for innovative or secondary purposes, personal data processing must be justified, and developers must explore ways to minimize data volumes. Techniques such as pseudonymization and anonymization, explicitly encouraged under the GDPR, can further support compliance with data minimization while preserving data usability. For AI developers and other data controllers, implementing this principle requires careful planning, strict adherence to necessity and the use of safeguards to minimize risks while achieving their objectives.

The **accuracy** principle, detailed in Article 5(1)(d), mandates that personal data must be accurate and kept up to date where necessary. Inaccurate or outdated data must be corrected or erased without undue delay. Personal data must always be accurate and kept up to date when necessary. To ensure accuracy, data controllers need to take reasonable steps to promptly correct or remove any inaccurate or incomplete information related to the purpose of processing. For example, if a data controller discovers that a person’s contact information is no longer valid, they should update it immediately. This might involve updating contact details from official records and assessing whether the customer relationship and the associated rights to process data should

[125] Korpisaari et al. 2022, p. 105; Voigt – Von dem Bussche 2017, p. 90–91.
[126] Hanninen et al. 2017, p. 49.

continue.[127] In AI development, the accuracy requirement involves assessing whether personal data is still necessary for its original purpose. This means evaluating if personal data remains needed in any form for developing the AI. For example, if personal data is anonymized and only the anonymized data is used for development, the original personal data is no longer required. However, if the AI is being developed using pseudonymized data, the personal data may still be needed for the development process.

The principle of **storage limitation** requires that personal data is retained only for as long as necessary for the purposes of processing. Personal data should be kept only for as long as necessary. In some cases, the retention period may be extended if the reasons for processing the data continue to apply. Additionally, certain situations legally require data controllers to retain information for a specific duration. For instance, employers must keep employee personal data even after employment ends to issue work certificates.[128] Health data used for developing AI is particularly unique because national laws often require very long retention periods for such information. For example, in Finland, prescription and patient records must be kept for 12 years after a patient's death or up to 120 years from the patient's birth if the date of death is unknown. Additionally, prescription delivery notes are retained for 12 years after the prescription expires[129]. However, the obligation to delete data can specifically apply to pseudonymized health data stored for training AI models. Even so, if pseudonymized health data is deleted, it can always be regenerated from the original health data.

According to Article 13 of the GDPR, data controllers must inform individuals about how long their data will be stored when collecting it. This means that when planning data processing activities, controllers must also determine and specify the data retention periods. To ensure compliance, data controllers should regularly review their data retention practices to make sure that personal data is not held longer than needed. Any personal data that is no longer necessary must be deleted or anonymized.[130]

---

[127] Korpisaari et al. 2022, p. 107; Hanninen et al. 2017, p. 50.
[128] Korpisaari et al. 2022, p. 107.
[129] See Act on the Processing of Client Data in Social and Health Care (703/2023).
[130] Korpisaari et al. 2022, p. 107.

The principle of **integrity and confidentiality**, set out in Article 5(1)(f), requires data controllers to implement appropriate technical and organizational measures to safeguard personal data against unauthorized access, loss, or destruction. Personal data must be handled to ensure its integrity and confidentiality, preventing unauthorized access. Integrity means that data is not altered without the data controller's consent. To protect data from unlawful processing and accidental loss, destruction, or damage, appropriate technical and organizational measures must be put in place. This approach aligns with the regulation's risk-based strategy.[131]

Technical measures include using strong passwords, shutting down systems after periods of inactivity and securing employees' personal computers and mobile devices with passwords. Access to high-risk data should be strictly controlled and guidelines should prevent the transport of data-containing devices like USB drives offsite. Special categories of personal data require even stricter protection, such as specific login restrictions, pseudonymization and logging systems to monitor who accesses the data and for what purpose.[132]

Organizational measures involve limiting data access to only those employees who genuinely need it for their roles. Organizations should regularly review job functions to determine the necessary level of data access required to perform each task effectively and securely. By implementing these measures, organizations ensure that personal data is protected throughout its lifecycle, maintaining trust and compliance with data protection regulations.[133] In the AI development encryption, pseudonymization and access controls between controllers, recipients and third parties are essential safeguard methods, which are particularly relevant when processing sensitive data.

Finally, Article 5(2) introduces the principle of **accountability**, which places the burden of demonstrating compliance on data controllers. Article 5(2) of the GDPR mandates that data

[131] Korpisaari et al. 2022, p. 107–108.
[132] Korpisaari et al. 2022, p. 108.
[133] Ibid.

controllers must do more than merely comply with data protection principles; they must also be able to continuously demonstrate their adherence to these principles. The responsibility for ensuring compliance lies solely with the data controller, who must uphold data protection standards at every stage of personal data processing.[134] This accountability remains with the data controller even when the roles of controller and processor are fulfilled by separate entities. Therefore, the data controller must provide evidence of compliance not only for their own data processing activities but also for those carried out by any engaged data processors. Ensuring accountability is essential in the development of artificial intelligence, particularly because the process may involve not only the data controller (e.g., the hospital) and the AI developer (the recipient) but also third parties acting as intermediaries. These intermediaries might include entities responsible for anonymizing health data or consultants ensuring compliance with GDPR requirements. Assigning accountability to a single entity requires clearly designating one party as the data controller through both contractual agreements and the definition of roles and actual activities within the process.

3.1.1 Integrating Data Protection Principles into AI Development

To ensure that data protection principles are properly implemented, they should be considered already during the planning phase of personal data usage. In the context of this research, this means that data protection issues must be addressed at the very beginning of the AI development process. This applies not only to the development process itself but also to how personal data might be at risk due to the AI system being developed, both during and after its creation.

Built-in and default data protection, commonly referred to as Privacy by Design and Privacy by Default, is a foundational approach in data protection that ensures privacy considerations are embedded directly into the system design and maintained throughout the entire data lifecycle. These principles aim to proactively address data protection risks, ensuring compliance and safe-

[134] Korpisaari et al. 2022, p. 99.

guarding personal data from the outset. Importantly, the responsibility for integrating these requirements extends beyond data protection officers to include all stakeholders involved in system design and data processing.[135]

Ann Cavoukian, who pioneered these concepts, outlined seven guiding principles to ensure a proactive and holistic implementation of privacy:

1. **Proactivity**: Privacy risks are identified and mitigated in advance, rather than corrected after problems arise.
2. **Privacy by Default**: User privacy is automatically protected, requiring no additional actions from the individual.
3. **Privacy Embedded in Design**: Privacy is a core component of the system, integrated without compromising functionality.
4. **Full Functionality**: Privacy and other objectives (e.g., security, usability) are achieved without unnecessary trade-offs.
5. **End-to-End Security**: Data security is ensured throughout the entire lifecycle, from initial collection to final destruction.
6. **Transparency**: Privacy practices and processes are documented and made accessible to relevant stakeholders.
7. **User-Centricity**: Privacy measures prioritize the user, offering clear options and information to empower individuals.[136]

Building on the principles of Privacy by Design and Privacy by Default, the risk-based approach provides a framework for proactively assessing and managing risks associated with the processing of personal data. Highlighted in key provisions of the GDPR, including Articles 24, 32, and 35, this approach emphasizes the need for appropriate technical and organizational measures to safeguard individual rights and personal data while ensuring compliance with regulatory requirements. Central to the risk-based approach is risk analysis, which requires data controllers to identify potential risks to individuals' rights arising from personal data processing. These risks

---

[135] See korpisaari et al. 2022, p. 311.
[136] Korpisaari et al. 2022, p. 311–312; Cavoukian 2011, p. 2.

must then be assessed in terms of their likelihood and severity, enabling the implementation of targeted measures to mitigate them effectively. Such measures must be tailored to the specific context, avoiding both underestimation and over-engineering of safeguards. By addressing data protection requirements early in the development process, organizations can prevent costly adjustments to existing systems and decisions, ensuring privacy is seamlessly integrated into the foundation of AI development.[137]

3.2 Legal Basis for the Processing of Personal Data in AI Development

The GDPR emphasizes that the processing of personal data is permissible only when it meets specific legal grounds as outlined in Article 6. These lawful bases define the specific conditions under which personal data processing is considered lawful. According to the GDPR, processing personal data is prohibited unless it is explicitly authorized by one of these legal bases.[138] Therefore, every instance of personal data processing must have a legitimate legal justification.

Under Article 6 of the GDPR, personal data can only be processed if at least one of the following lawful bases, each reflecting distinct circumstances under which personal data may be handled, is satisfied:

1. **Consent of the Data Subject:** The individual has given clear and informed consent for their personal data to be processed for a specific purpose.[139]
2. **Performance of a Contract:** Processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before entering a contract.[140]

---

[137] See Korpisaari et al. 2022, p. 316.
[138] Article 6(1) of the GDPR requires that data processing is lawful only if, and to the extent that, at least one of the legal bases outlined in points (a)–(f) of the article is fulfilled.
[139] GDPR Article 6(1)(a).
[140] GDPR Article 6(1)(b).

3. **Legal Obligation:** Processing is required to comply with a legal obligation to which the data controller is subject.[141]
4. **Vital Interests:** Processing is necessary to protect the vital interests of the data subject or another person, such as in life-threatening situations.[142]
5. **Public Interest:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.[143]
6. **Legitimate Interests:** Processing is necessary for the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.[144]

To ensure the legality of data processing, data controllers must be able to demonstrate that their processing activities are based on one of these lawful grounds.[145] This requirement emphasizes the accountability of data controllers to uphold the principles of lawfulness, fairness and transparency as outlined in Article 5(1)(a) of the GDPR. Articles 6(2) and 6(3) provide member states the authority to maintain or introduce more detailed regulations to adapt the application of GDPR rules for data processing activities conducted under Article 6(1)(c) (legal obligations) and Article 6(1)(e) (public interest or exercise of official authority). This provision allows countries to customize GDPR compliance to meet specific national requirements, particularly in sectors such as healthcare where legal and public interest considerations are essential. However, for the other lawful bases of data processing outlined in Article 6, member states do not have the flexibility to introduce additional regulations, ensuring a consistent application of GDPR standards across all types of data processing activities.[146]

Besides consent, two other legal bases for lawful processing are particularly relevant to medical AI development. The first is when processing is necessary for performing a task carried out in

[141] GDPR Article 6(1)(c).
[142] GDPR Article 6(1)(d).
[143] GDPR Article 6(1)(e).
[144] GDPR Article 6(1)(f).
[145] Korpisaari et al. 2022, p. 115.
[146] Korpisaari et al. 2022, p. 115.

the public interest. The WP29 has confirmed that health research can qualify as a public interest task, even if conducted by private or commercial entities. However, it should be noted that the development purposes must align with the public interest. The second legal basis is when processing is necessary for the legitimate interests pursued by the data controller or a third party. This basis is limited by Article 6(1)(f) of the GDPR, which states that such interests can be overridden by the data subject's fundamental rights and freedoms. The WP29 has indicated that applying the legitimate interests condition requires a balancing test[147], where the controller's or third party's legitimate interests must be weighed against the data subject's rights and interests.[148] In developing medical AI, it would be easiest to rely on the task carried out in the public interest as the developers are usually trying to create AI innovations to enhance the health care. However, each of these bases comes with its own set of challenges.

3.3 Processing of special categories of personal data such as Health Data

Article 9 of the GDPR imposes a general prohibition on the processing of special categories of personal data, that are considered particularly sensitive due to their potential to infringe upon the rights and freedoms of data subjects. Special categories of data include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a person, health data, and data concerning a natural person's sex life or sexual orientation.

Given its sensitive nature, the processing of such data is prohibited unless specific legal exceptions, as provided in Article 9(2), apply. In the health and medical sectors, personal data often includes sensitive health-related information, which is categorized into the special categories of data. Consequently, data controllers, either the hospital or the AI developer depending on their

[147] Legitimate interest assessments, often called "balancing exercises," involve evaluating the opposing rights and interests in a particular situation. On one side are the data subjects' interests, fundamental rights, and freedoms, while on the other are the interests of the controller or a third party. To establish legitimate interest as a valid legal basis for processing, it is essential to consider the specific circumstances of each case and demonstrate that these interests legitimately outweigh the potential impact on data subjects. EDPB, 2024, Opinion 2024/28, p. 23.
[148] Donelly–McDonagh 2019, p. 112–113.

roles in the processing of data, must obtain exemptions from the GDPR's prohibition on processing special categories of personal data, as detailed in Articles 9(1) and 9(2). This ensures that the processing of such sensitive data is legally permissible under the regulation.[149]

3.4 The Secondary Use of Health Data

3.4.1 Scientific Research Purposes in the Context of Machine Learning

In addition to establishing a legal basis for processing, it is essential to evaluate whether further processing occurs. This consideration is particularly important when handling data that was previously collected, potentially for a different purpose and by another controller.[150] This scenario is common in the development of medical AI, where data is typically gathered by hospitals and subsequently processed for AI development by another entity. This kind of secondary use of health data holds significant potential for advancing health research. Technological advancements, particularly in artificial intelligence, have enhanced the ability to reuse datasets. However, the GDPR and ethical guidelines often limit the reuse of personal data unless the data subject has provided informed or explicit consent.[151] According to Article 5(1)(b) of the GDPR, the continued processing of personal data for scientific research purposes that serve the public interest is considered compatible with the original purpose for which the data was collected. This compatibility is contingent upon the implementation of appropriate safeguards to protect the rights and freedoms of the data subjects, as detailed in Article 89(1). As a result, the GDPR assumes that secondary use of personal data for such research purposes aligns with the initial data processing objectives, provided that the necessary protections are in place.[152]

Article 9(2)(j) of the GDPR, has a so called "research exemption," which permits the processing of special categories of personal data for scientific research purposes, even though such processing is generally prohibited. However, this exemption is only valid if the processing adheres

[149] Anwana et al. 2024, p. 100.
[150] Anwana et al. 2024, p. 112.
[151] Anwana et al. 2024, p. 99.
[152] See GDPR, Recital 50.

to Article 89(1). This means that the research must be based on Union or member state law, be proportionate to the research goals, respect the fundamental principles of data protection, in addition to including appropriate and specific measures to protect the rights and interests of the data subjects. This exemption allows researchers to use sensitive personal data for important scientific advancements while ensuring that individuals' privacy and rights are thoroughly protected through stringent legal and technical safeguards.[153] To use this exemption it should be kept in mind that Article 9(2)(j) should be considered together with the lawful processing standards outlined in Article 6(1) of the GDPR.[154]

In the context of the GDPR, "scientific research purposes" are broadly understood to encompass technology development and demonstration, foundational research, applied research, and privately funded studies.[155] Scientific research is defined as activities aimed at generating new knowledge and advancing a particular field to a high level.[156] Consequently, conducting scientific research is not limited to academic researchers alone but can also be undertaken by non-profit organizations, governmental institutions, and private companies aiming for profit. Digitization has made the generation and dissemination of personal data easier and more cost-effective than ever, fundamentally transforming how research is conducted. The distinction between private sector research and traditional academic research has become increasingly blurred, making it more challenging to differentiate research that provides generalizable benefits to society from research that primarily serves private interests.[157] Therefore, it remains unclear to what extent experimental development activities aimed at improving services or introducing new offerings by for-profit companies can be classified as scientific research.[158] The Data Protection Working Group, in its guidelines on consent, defines scientific research as a research project that adheres to relevant sector-specific methodological and ethical standards, as well as best practices. The group emphasizes that the definition should not be extended beyond its general

[153] Anwana et al. 2024, p. 105.
[154] Donelly–McDonagh 2019, p. 112.
[155] GDPR, Recital 159.
[156] Ducato 2020, p. 3.
[157] EDPS, Preliminary Opinion 2020, p. 12.
[158] See Kindt 2016, p. 73.

meaning.[159] Conversely, the European Data Protection Supervisor (EDPS) adopts a broader interpretation of scientific research, viewing it as an endeavor that leverages society as a whole and generates knowledge that supports the public interest.[160]

The regulation's wording initially suggests that further processing of personal data for scientific research purposes is permissible, provided that appropriate safeguards are implemented. However, the Data Protection Working Group has also been skeptical about further processing as they have stated that the compatibility assumption should not be interpreted as a universal exception allowing further processing in all cases of scientific research.[161] Similarly, the EDPS has stated that the lawfulness of processing must be evaluated on an individual basis, especially when applying Articles 9 and 6 of the GDPR.[162]

The application of the compatibility assumption in commercial AI research has generally been met with considerable criticism. This is because commercial research may not follow the same high standards and inspection methods as academic research. Additionally, the concealed nature of algorithms and the protection of business secrets can make oversight challenging.[163] However, Stalla–Bourdillon, and Knight have argued, that from a modern perspective, the absence of prior ethical approval does not necessarily prevent an activity from being classified as scientific research, provided that the research conducted by data scientists does not result in actions or decisions affecting individuals. They suggest that even though developing various data analytics applications might not fit the traditional definition of scientific research, the compatibility assumption can still be applied in certain situations involving the training of machine learning systems. This is because AI research is considered part of the broader research activities carried out by data scientists.[164]

---

[159] WP 259 rev.01, Guidelines 2017, p. 27–28.
[160] EDPS, Preliminary opinion 2020, p. 12.
[161] WP 203, Opinion 03/2013, p. 28.
[162] EDPB, Guidelines 03/2020, margin number 17, 18, 91.
[163] Mezaros–Ho 2021, p. 1, 9.
[164] Stalla-Bourdillon – Knight 2018 p. 17, 264–265; Mezaros–Ho 2021, p. 8–9.

3.4.2 Further Processing of Health Data for AI Development on Public Interest Grounds under the AI Act

The AI Regulation also addresses the further processing of personal data. Article 59 of the AI Regulation supports the view that the further processing of health data is permissible based on public interest. Further processing of personal data for developing certain AI systems in the public interest is allowed under Article 59 of the AI Act, provided it occurs within the framework of the AI regulatory sandbox[165] and meets specific criteria to protect individuals' rights and ensure compliance with Union data protection laws. The regulatory sandbox permits personal data originally collected for other purposes to be processed for developing, training, and testing AI systems. However, this is only allowed when the AI systems are designed to serve substantial public interest and address specific areas such as public health and safety (e.g., improving healthcare systems or disease prevention), environmental protection, climate change mitigation, energy sustainability, resilient transportation and enhancing the efficiency of public services.[166]

Crucially, the processing must be necessary to achieve these objectives and cannot be effectively accomplished using anonymized, synthetic or non-personal data.[167] Additionally, stringent safeguards must be in place. Effective monitoring mechanisms are required to identify and mitigate high risks to individuals' rights and freedoms during the experimentation phase.[168] If risks are deemed too significant, processing must be halted immediately. The sandbox environment must also ensure that personal data is stored in a secure, isolated system accessible only to authorized individuals.[169] Data created during the sandbox experimentation cannot be shared outside the sandbox and any sharing of original data must comply with Union data protection laws.[170] Furthermore, personal data processing in the sandbox must not result in decisions or measures that

---

[165] A regulatory sandbox is generally a tool that allows companies to verify that new technologies and products will meet all regulatory requirements. See: European Comission-Projects-Digital regulatory sandbox.
[166] AI act, Article 59(1)(a).
[167] AI act, Article 59(1)(b).
[168] AI act, Article 59(1)(c).
[169] Ai act, Article 59(1)(d).
[170] Ai act, Article 59(1)(e).

affect data subjects' rights.[171] To uphold transparency and accountability, logs of data processing must be maintained during the sandbox activities,[172] and personal data must be deleted once the project concludes or the retention period ends.[173] Detailed documentation of the processes, including the rationale and testing results, must be preserved, while a summary of the project's objectives and expected outcomes should be publicly available, barring sensitive cases such as law enforcement operations.[174]

3.5 Withdrawal of Consent, the Right to Be Forgotten and Right to object

Article 17 of the GDPR defines the data subjects´ right to erasure ("Right to be forgotten"). According to the article the data subject has the right to request the controller to delete their personal data without undue delay. The controller is obligated to erase the personal data without undue delay, provided that at least one of the following conditions is met:

a) The personal data is no longer necessary for the purposes for which it was originally collected or otherwise processed.
b) The data subject withdraws their consent, on which the processing is based according to Article 6(1)(a) or Article 9(2)(a) and there is no other legal basis for the processing.
c) The data subject objects to the processing under Article 21(1) and there is no legitimate reason for the processing, or the data subject objects to the processing under Article 21(2).

Since this pertains to the data subject's personal rights, they must demonstrate a valid reason for requesting the deletion of their data.[175] In the development of medical AI based on consent, the basis for processing their health data lies in the individual's agreement. If the data subject

[171] Ai act, Article 59(1)(f).
[172] Ai act, Article 59(1)(h).
[173] Ai act, Article 59(1)(g).
[174] Ai act, Article 59(1)(i)–(j).
[175] Korpisaari et al. 2022, p. 247.

chooses to withdraw their consent, it serves as the foundation for their request to have their data deleted.

Under Article 21(1) of the GDPR, the data subject has the right to object at any time to the processing of their personal data based on Article 6(1)(e) or (f) of the GDPR, such as profiling under these provisions. The data controller must cease processing the personal data unless they can demonstrate that there are compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or if the processing is necessary for the establishment, exercise, or defense of legal claims. Furthermore, according to Article 21(2) of the GDPR, when personal data is processed for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), the data subject retains the right to object to the processing based on their personal and specific situation. This right can only be overridden if the processing is necessary for performing a task carried out in the public interest. Article 21 makes the use of legitimate interest a less favorable option for AI developers, as it strengthens the data subject's rights to restrict the use of their personal data in AI development. In contrast, using public interest as the legal basis provides robust protection for the data subject’s rights, provided that the AI developer can justify the public interest rationale. This approach, in my view, supports the development of innovative medical AI technologies that enhance healthcare by reducing the workload of healthcare professionals and improving the quality of care.

Under the GDPR, personal data must be deleted when the data subject withdraws the consent that justified its processing, provided there is no other legal basis for the processing. As previously mentioned in relation to Article 7, individuals have the right to revoke their consent for the processing of their personal data at any time. If consent is the only legal justification for processing, the data must be removed once consent is withdrawn. The GDPR does not provide a specific definition of what constitutes data deletion. Merely transferring data to a "trash bin" from which it can be easily recovered does not meet the requirements. Data must be erased in a manner that ensures the data controller, processor, or any third party can no longer access it.

The GDPR does not prescribe the exact methods for data deletion.[176] When developing artificial intelligence, a fundamental issue arises in determining when personal data remains classified as personal data, specifically, when it can be considered sufficiently anonymized. Additionally, problems emerge if the AI is required to retain data that could potentially be linked back to the individual, raising important questions about the appropriate methods for data deletion. The criteria for achieving an adequate level of anonymization are thoroughly examined in Section 5.

[176] Korpisaari et al. 2022, p. 247–248.

4 Consent and Its Legal Implications in AI Development

4.1 Defining Consent: A Theoretical Approach to Individual Autonomy, Control, and Ethical Dimensions

Consent is often perceived as an intuitive and straightforward concept within legal contexts, primarily because it serves as a foundational principle across numerous areas of law. Many legal doctrines depend heavily on the notion of consent, and it is uncommon for lawyers to express significant uncertainty about its practical application.[177] When the legal system acknowledges an individual's right to self-determination, it empowers individuals to structure their legal relationships with others according to their own preferences. One method to achieve this is through the expression of will. By expressing their intentions, individuals establish norms that, while considering the mutual relationships between parties, should be equated with legal provisions (lex inter partes). The legal effect arises because the individual so desires. However, the person expressing their will may, due to erroneous or incomplete communication, convey an impression that does not accurately reflect their true intentions. This situation raises the issue of interpreting the expression of will. The role of interpretation is to ascertain the meaning that should be attributed to the expression as a legal norm.[178] Since data protection primarily involves the safeguarding of individuals' personal data, it is my view that interpretations should be approached from the perspective of the person providing the expression.

The principle of consent underpins much of the legal doctrine, particularly where voluntary obligations are concerned. This idea forms the basis of doctrines such as the freedom of contract and sanctity of contract, which posit that agreements entered voluntarily are inherently fair. Similarly, in international law, this principle manifests in the doctrine of pacta sunt servanda, which asserts that agreements must be honored. However, determining whether consent has been given freely involves two layers of complexity. First, a robust and defensible definition of "voluntary" action must be established. Second, using this framework, actions must be interpreted reliably to determine whether they were, in fact, voluntarily undertaken. While there is a

[177] BeyLeveld, – Brownsword 2007, p. 4.
[178] Telaranta 1990, p. 90.

general agreement that obvious forms of coercion, undue pressure and influence invalidate free consent, subtler nuances in these dynamics continue to present challenges in legal analysis.[179]

When discussing free consent, most agree that true voluntariness cannot exist if there is extreme coercion, pressure or influence involved. Additionally, although not everyone concurs, some believe that incentives and inducements can also diminish the authenticity of free consent. Beyond these points of agreement, the concept of voluntariness becomes increasingly debated.[180] In legal literature, the issue has been explored through two distinct approaches: will theory and expression theory. The choice between these approaches depends on whether more emphasis is placed on the individual's intent (will) or the manner in which the will is expressed (expression). According to will theory, the expression of will is binding solely based on its content as intended by the individual making the expression. This means that if an error occurs during the expression of will, the recipient of the expression bears the associated risks. Conversely, expression theory holds that the expression of will is binding only to the extent that it is understood by an external party who objectively evaluates and considers the surrounding circumstances.[181]

Duncan Kennedy has argued that voluntariness is inherently adaptable, can be shaped by ideological factors and lacks consistent stability. He highlights that in legal contexts, the definition of voluntariness can vary significantly. On one end, protections against fraud and coercion might be nearly eliminated to promote individualism and self-reliance. On the other end, individuals with slightly more knowledge or power might be forced to relinquish all their advantages, potentially weakening the enforceability of laws within capitalist economies. If this analysis is accepted, two possible responses arise, neither of which are entirely satisfactory. The first option is to recognize that the concept of free dealing does not have a fixed definition and is inherently open to some degree of uncertainty. The second option is to define free dealing in a specific and

[179] BeyLeveld, – Brownsword 2007, p. 8.
[180] BeyLeveld, – Brownsword 2007, p. 8, 12–13.
[181] Telaranta 1990, p. 90–92.

strict manner within the range of voluntariness, although this might lead to arbitrary applications. Neither approach completely addresses the issues caused by the unclear nature of free consent.[182]

For consent to be considered genuine, it must be freely given and based on sufficient information, regardless of how these requirements are interpreted. An individual's ability—or competence—to give consent must align with these conditions. A person capable of consenting must first have the ability to make their own judgments and decisions independently, without external influence or pressure. Additionally, they must be able to understand and use the information that is important for making their decision.[183] The definitions and interpretations of consent significantly influence the practical implementation of consent forms in medical AI development. To ensure that consent is both valid and compliant with GDPR, consent forms must be meticulously designed to guarantee that individuals freely and knowingly agree to the use of their personal data. This involves providing clear and comprehensive information about the specific purposes for which the data will be used, the types of data being collected, and how the data will contribute to the training and improvement of AI models. Medical AI consent forms should avoid technical jargon, instead using plain language that is easily understandable to individuals with varying levels of expertise[184]. Additionally, these forms must explicitly outline the individual's rights, including the ability to withdraw consent at any time without facing any negative repercussions. Facilitating straightforward and accessible withdrawal processes is essential to uphold the principle of voluntariness.

Moreover, consent forms should address the distinctions between anonymization and pseudonymization, explaining how each process affects the individual's data privacy and the legal implications thereof. When data is anonymized, consent may no longer be necessary, but this must be clearly communicated to ensure transparency. In cases where pseudonymized data is shared with third parties, consent forms must specify the safeguards in place to prevent re-identification

---

[182] BeyLeveld, – Brownsword 2007, p. 8, 12–13.
[183] BeyLeveld, – Brownsword 2007, p. 12–13.
[184] See Korpisaari et al. 2022, p. 150.

and clarify the limited scope of data use. To ensure that the autonomy of the individual completing the consent form in deciding on their consent, as well as their control over their personal data, is sufficient for valid consent, the completion of the consent form should be entirely separate from other procedures, such as healthcare treatment. The individual filling out the form should be fully aware that providing consent is not mandatory and that withholding consent will not result in any personally negative consequences. By incorporating these detailed and transparent elements, medical AI developers can foster trust and ensure that consent is both informed and voluntary. This comprehensive approach not only aligns with GDPR requirements but also promotes ethical standards in the use of personal data, thereby facilitating the responsible advancement of AI technologies in healthcare.

4.2 Consent as the Basis for the Processing of Health Data

The possibility of progressing AI with health data or reusing already existing health data for the development purposes has grown substantially, largely due to rapid evolvement in technology. These new AI developing tool innovations have significantly expanded the potential for repurposing existing datasets. However, the GDPR and various ethical frameworks often impose strict limitations on further utilizing personal information without a clear and informed consent of the individuals involved.[185] Article 7 of the GDPR sets out the conditions under which consent, as a legal basis for processing personal data, can be considered valid. Given that consent is one of the most commonly relied-upon grounds for lawful data processing under Article 6(1)(a), Article 7 provides essential safeguards to ensure that the data subject's consent is not only obtained but also demonstrable, revocable and freely given.[186]

Consent in data protection law signifies genuine choice and control for the data subject. When consent is obtained with prior awareness and control over data processing, it serves as the most autonomous legal basis among those outlined in Article 6(1) of the GDPR. Explicit consent

[185] See e.g. Anwana et al. 2024, p. 99.
[186] GDPR, Recital 32; See also Korpisaari et al. 2022, p. 145–146.

ensures transparency and grants data subjects significant autonomy, enabling them to maintain control over their personal information.[187] For consent to be valid, it must be given freely and for specific, explicit purposes. Consent must cover all processing activities carried out for the same or related purposes. It is permissible to obtain consent for multiple purposes simultaneously, provided that the data subject is fully aware of each purpose they are consenting to and genuinely has the option to choose. Consent is not considered freely given if the data subject cannot provide separate consent for different processing activities involving their personal data. There is no strict format for consent; it can be provided verbally, in writing, on paper, or electronically. However, data controllers must be able to demonstrate that consent has been obtained, making documented consent highly advisable.[188]

When obtaining legal consent, it is essential to consider the conditions under which consent is given and whether these conditions provide the data subject with adequate freedom to make an informed choice. Consent must be specific, meaning that the data subject clearly indicates their agreement to a particular processing activity, and it should not be assumed that consent for one purpose extends to other, unrelated purposes. Informed consent requires that the data subject can easily understand the implications of their consent, with the reasons for data processing being clearly and thoroughly explained.[189]

A notable example is the Planet49 case, where the CJEU determined that consent was not valid when users were required to accept data storage or the use of cookies through pre-ticked boxes. The court emphasized that consent must involve a clear affirmative action, meaning that users must actively opt-in rather than passively accept by default. This ruling reinforces the necessity for data controllers to obtain explicit and unambiguous consent, ensuring that individuals retain control over their personal data and that consent is genuinely informed and voluntary.[190]

---

[187] Anwana et al. 2024, p. 100; See EDPB, Guidelines 05/2020.
[188] Korpisaari et al. 2022, p. 116–117, 148.
[189] Anwana et al. 2024, p. 107.
[190] Korpisaari et al. 2022, p. 117.

The first condition under Article 7(1) places the burden on the data controller to demonstrate that valid consent has been given by the data subject. Consent must be provable through records or documentation, which are necessary for demonstrating compliance with GDPR principles, such as accountability under Article 5(2). For AI development and other large-scale data processing activities, this requirement often translates into robust consent management systems that record when, how and for what purposes consent was obtained. Without such systems, controllers risk non-compliance, particularly if disputes arise regarding the validity of consent.

Article 7(2) addresses the issue of consent obtained in conjunction with other matters in a written declaration. The GDPR requires that any request for consent must be clearly distinguishable, intelligible and presented in an accessible form, using clear and plain language.[191] The European Data Protection Board (EDPB) has aligned that when obtaining consent for processing health data, all conditions for explicit consent under the GDPR must be met. These conditions are outlined in **Article 4(11), Article 6(1)(a), Article 7, and Article 9(2)(a).** Specifically, consent must be freely given, specific, informed and unambiguous, and it must be expressed through a statement or clear affirmative action.[192] Explicit consent is necessary in situations involving significant data protection risks, where ensuring a high degree of individual control over personal data is considered essential.[193] Explicit consent ensures that individuals are not misled or coerced into providing consent, particularly when it is embedded within lengthy or complex documents, such as 50-page agreements with multiple condition paragraphs. If a declaration fails to meet these requirements or contains terms that infringe upon GDPR principles, such provisions are rendered non-binding. This safeguard protects individuals from "consent fatigue" or from being unaware that they have consented to some unknown personal data processing.

The right to withdraw consent at any time is enshrined in Article 7(3) and represents a crucial component of GDPR's focus on empowering data subjects. Consent is only meaningful if it can be revoked as easily as it was given, ensuring that individuals retain control over their personal

---

[191] GDPR, Article 7(3).
[192] EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, margin number 18.
[193] EDPB, Guidelines 05/2020, margin number 91.

data. Data subjects are entitled to withdraw their consent at any time.[194] Consent is only considered voluntarily given if the data subject is genuinely able to make an independent choice and can later refuse or withdraw consent without facing any adverse consequences. The data controller must demonstrate that it is possible to decline or revoke consent at a later stage without causing harm, such as incurring additional costs. Additionally, data subjects must not be coerced or threatened with negative repercussions if they choose not to consent to the processing of their personal data. This ensures that consent remains voluntary and that individuals retain control over their personal information throughout the data processing lifecycle.[195]

Finally, Article 7(4) reinforces the principle that consent must be freely given by scrutinizing situations where consent might be conditional. It requires controllers to assess whether the performance of a contract, including the provision of a service, is made contingent on the data subject's consent to the processing of personal data that is not strictly necessary for the performance of that contract.[196] This provision ensures that consent is not coerced or "bundled" with unrelated processing activities, thus safeguarding the voluntariness of consent. In practical terms, this means that individuals must not be denied a service merely because they refuse to consent to unnecessary data processing. This protection is especially relevant in the digital economy, where services are frequently tied to data collection and analysis for purposes unrelated to the provision of the primary service.

4.3 Criteria for Valid Consent in Medical AI Development

The EDPB considers that obtaining valid consent requires providing the data subject with at least the following information:

- **Identity of the Data Controller:** Clearly identify who is responsible for processing the data.

[194] Sharma 2020, p. 245.
[195] Korpisaari et al. 2022, p. 147–148.
[196] GDPR, Recital 43.

- **Purpose of Each Processing Activity:** Specify the reasons for which consent is being requested for each particular data processing operation.
- **Types of Data Collected and Used:** Describe what kinds of personal data are being gathered and how they will be utilized.
- **Right to Withdraw Consent:** Inform the data subject of their ability to withdraw consent at any time.
- **Risks Associated with Data Transfers:** Explain any potential risks involved in data transfers, particularly those arising from insufficient data protection measures as determined by adequacy decisions and the absence of appropriate safeguards under Article 46 of the GDPR.[197]

Among the exceptions listed in Article 9(2), explicit consent of the data subject under Article 9(2)(a) is one of the most significant and widely relied-upon legal grounds. This basis allows the processing of special categories of personal data provided that the data subject has given explicit consent for one or more specified purposes. Explicit consent imposes a stricter standard than regular consent under Article 6(1)(a), requiring a clear, unambiguous and affirmative statement that leaves no room for doubt regarding the data subject's intention to consent.[198] Information of the processing of data subjects data given to the data subject must be clearly comprehensible and sufficiently detailed.[199] The data subjects consent must indicate their wish to have certain data used in a particular processing operation. The data subject should also be able to easily determine the consequences of their consent.[200] Depending on the case and circumstances, additional information may be necessary for the data subject to fully understand the processing of their data and its purpose. There is no prescribed format for providing this information; it may be conveyed orally, in writing, or even through an audio or video message. However, the message must be presented in a manner that an average person can comprehend. Consequently,

---

[197] See Korpisaari et al. 2022, p. 149–150; EDPB, Guidelines 05/2020, p. 16–17.
[198] See Korpisaari et al. 2022, p. 167; GDPR, Recital 52.
[199] Case C-673/17, *Planet49 GmbH*, paragraph 74. See also Anwana et al. 2024, p. 107.
[200] Case C-61/19, *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal,* paragrapgh 38. See also Anwana et al. 2024, p. 107.

when obtaining consent, lengthy legal jargon or complex privacy clauses that only a lawyer could understand should be avoided.[201]

Ensuring these elements can be challenging in scenarios where research data is intended for future, undefined studies. In such cases, some aspects of consent, such as the final purpose of data use, may not be known at the time consent is obtained. This uncertainty makes it difficult to fully meet the requirements of specificity and informed consent, as the data subject cannot be fully informed about all potential future uses of their data.[202] The situation is further complicated by Article 5(1)(b), which mandates that the new purpose must be compatible with the original purpose for which the data was collected, as EDPB has clarified that the GDPR must not be interpreted in a way that allows data controllers to circumvent specifying the purpose when obtaining consent from data subjects.[203] Valid consent requires a clear affirmative action by the data subject, such as ticking a box or signing a form and pre-ticked boxes or implied consent are explicitly prohibited.[204] In the context of AI development, obtaining valid consent can be challenging due to the often complex and evolving nature of processing operations. For instance, data subjects may struggle to fully understand how their personal data will be used for model training, further exacerbating issues of transparency, which also leads into a situation where it is uncertain whether the data subject has fully understood what has he or she consented to.

To ensure that consent is adequate, researchers should obtain clear and explicit permission from participants at the beginning of the AI development process, even before anonymizing their data. This consent must specifically allow the use of their data for all the intended health research purposes, like in this case AI development. Participants need to be fully informed about the goals of the AI development, whether it focuses on a particular area of health or a broader related field. By securing explicit consent for these specific purposes, the parties in the AI development comply with GDPR requirements and respect the participants' right to make informed

---

[201] Korpisaari et al. 2022, p. 150; WP 259 rev.01, Guidelines 2017, p. 14.
[202] Anwana et al. 2024, p. 107.
[203] Ibid; EDPB, Document on Response to the Request from the European Comission for Clarifications on the Consistent Application of the GDPR, Focusing on Health Research, February 2, 2021.
[204] GDPR, Recital 32.

decisions about their personal data. This approach not only protects individuals' rights but also enhances the transparency and legitimacy of the research process, which in this case would be medical AI development.[205]

[205] See e.g. Clarke et al. 2019, p. 1132.

5 Anonymization and Pseudonymization under the GDPR

5.1 Anonymization and Its Legal Implications

Under the GDPR, anonymization refers to the process of irreversibly modifying personal data in a way that individuals can no longer be identified, either directly or indirectly. Recital 26 of the GDPR clarifies that data which has been properly anonymized falls outside the scope of the Regulation because it no longer qualifies as personal data. Thus, the GDPR does not apply if anonymous data is used as training data for a machine learning system. By anonymizing personal data, AI developers can process large datasets without being subject to the GDPR's requirements, such as obtaining consent, performing data protection impact assessments (DPIAs), or adhering to strict storage limitations. This exemption creates a legal advantage, particularly in AI contexts where processing vast amounts of data may otherwise impose significant regulatory burdens.

Anonymization is also classified as further processing, as personal data to be anonymized, such as X-ray images, were originally collected for healthcare purposes, not for anonymization or AI development. Therefore, it must meet the compatibility requirement set by the purpose limitation principle or there needs to be other legal basis for processing e.g. new consent from the data subject. According to the data protection group's view, anonymization can be considered compatible with the original purpose without new legal basis for the processing of the original data, if the anonymization process reliably produces anonymized data.[206]

When evaluating the identifiability of personal data in the context of data anonymization, special attention should be given to three distinct methods of identifiability. First, it is necessary to assess whether specific records can be isolated in a way that makes it possible to identify an individual, either directly or indirectly. Secondly, consideration should be given to whether it is feasible to link two or more pieces of information about the same person or group, even if the individuals themselves cannot be directly identified. This could involve connections made

[206] WP 216, Opinion 05/2014, p. 7.

through common characteristics or shared data points. Lastly, it is important to evaluate the risk of deducing sensitive or private information about individuals with a high degree of accuracy based on patterns or trends observable within the data.[207] From a technical perspective, identifiability can also be simply categorized into two meanings: the revelation of identity and the revelation of a characteristic in context. In the first case, specific data can be linked to a particular identified person, while in the latter, new information is revealed about an unidentified person.[208] Anonymization can be considered successful if the revelation of identity is prevented. In practice, the only way to ensure with complete certainty that identity is not revealed is to refrain entirely from publishing the data. Therefore, anonymization is about achieving a sufficiently low level of identifiability.[209]

However, even if all identifiable information that could link a specific individual to e.g. an X-ray image was to be removed before using it for AI development purposes, the X-ray could not necessarily be considered fully anonymous.[210] Healthcare institutions that provide X-ray images often retain archives containing those images along with metadata that includes patient identities. As a result, data controllers or individuals with access to the original database could perform an image search to link the dataset images back to the metadata, thereby identifying the patient. To mitigate this risk, artificial noise can be added to the images to make such linkage more difficult. This kind of approach has significant drawbacks, as the added noise typically compromises the image's utility for practical applications, including medical research, by obscuring even basic anatomical details.[211] Aiming for full anonymization may also be impractical in some AI applications, as anonymization often reduces the quality of data, which may create difficulties to AI development. Developing an accurate and high-quality AI solution requires a lot of high-quality data. Typically, the more strongly the identifiability of individuals is removed from the data, the less useful the data becomes.[212]

---

[207] WP 216, Opinion 05/2014, p. 11–12.
[208] Holzel 2019, p. 186.
[209] Holzel 2019, p. 187; Duncan – Lambert 1989, p. 207.
[210] See Weitzenboeck et al. 2022, p. 199–200; Finck–Pallas 2020, p. 15; WP 216, Opinion 05/2014, p. 11–12, 23–25.
[211] Weitzenboeck et al. 2022, p. 199–200.
[212] Hintze 2019, p. 114; Holzel 2019, p. 187;. Lee et al. 2017, p. 1–2.

In its guidelines, the WP29 concludes that anonymization is a process applied to personal data to achieve irreversible de-identification. For data to be considered truly anonymized, the erasure must be permanent, ensuring that re-identification is no longer possible. If the original raw dataset still exists and can be linked back to the anonymized data, the data is considered pseudonymized rather than fully anonymized.[213] This distinction highlights the importance of destroying the raw data to achieve true anonymization. This perspective has been criticized, because in many cases, hospitals wishing to share anonymized data for scientific research may need to retain the original data sources for medical care purposes. Additionally, there have been arguments in legal literature that this approach conflicts with Recital 26 of the GDPR. Recital 26 adopts a risk-based approach to determining whether data qualifies as personal data. If there is a reasonable risk that an individual could be identified, the data should be treated as personal. However, if the risk of identification is negligible, the data can be treated as non-personal, even though absolute certainty of non-identification is not required. [214] This, however, leaves room for interpretation regarding the level of risk required for data to be considered personal data.

5.2 Pseudonymization as a Safeguard for Data Privacy

While fully anonymized data is not subject to the GDPR, pseudonymized data remains regulated because it can still be linked back to an individual using additional information. Pseudonymization, as defined in Article 4(5) of the GDPR, involves processing personal data in a way that it can no longer be linked to a specific individual without the use of additional information. This additional information must be stored separately and protected through technical and organizational measures to prevent the identification of an individual. Attributing data to an identified person means demonstrating that the data is related to that person. Attributing data to an identifiable person, on the other hand, refers to linking the data to other information through which the individual could be identified. This connection may rely on one or more identifiers or identifiable attributes.[215]

---

[213] Weitzenboeck et al. 2022, p. 200; Finck–Pallas 2020, p. 15; WP 216, Opinion 05/2014, p. 11–12, 23–25.
[214] Finck–Pallas 2020, p. 15.
[215] EDPB, Guidelines 2025/01, p. 9.

The GDPR does not specifically define pseudonymous data. Under the regulation, data is classified as either personal data or non-personal data. Pseudonymized data falls under the category of personal data because pseudonymization is considered a method of processing data rather than a separate data classification.[216] Pseudonymization occupies a grey area between personal data and anonymized data. As a concept pseudonymization is relatively old. The Data Protection Working Party has assessed pseudonymized data from the perspective of the personal data concept as early as 2007, concluding that individuals could be indirectly identified from pseudonymized data.[217]

The definition of pseudonymization can be understood as comprising three elements. First, pseudonymization involves the processing of personal data, which is subject to the GDPR. Second, pseudonymization ensures that personal data can no longer be attributed to a specific data subject without additional information. The re-identification of pseudonymized data can occur, for example, through the original data set or an encryption key, provided that such additional information is specified under Article 4(5) of the GDPR. Third, it is required that additional information is stored separately from the pseudonymized data, and that technical and organizational measures are implemented to ensure that the data cannot be linked back to an identified or identifiable individual.[218]

Pseudonymization is a valuable alternative for data anonymization for AI developers, since the data quality is a lot better than in the anonymized data. This is due to the fact that it has a lot more of the original data in it. For example, X-rays that do not link directly to the patient include still the original X-ray image, since the anonymized version would have a lot of the required detailed data deleted in the anonymization process. If this data was to be made anonymous, even the hospital that has the original image should not be able to identify the patient from the anonymized X-ray. Using pseudonymized data in AI development presents several challenges. AI

[216] Tarhonen 2017, p. 11.
[217] Tarhonen 2017, p. 15. WP 136, Opinion 4/2007, p. 18–20.
[218] Tarhonen 2017, p. 11.

developers must navigate and comply with a variety of GDPR requirements, which can complicate the development process. Additionally, the rights of data subjects may slow down the progress of AI projects and potentially impact the quality of the outcomes.

5.4 Sufficient Anonymization from the Perspective of an AI Developer

The EDPB emphasizes that AI models typically require a detailed assessment to determine whether personal data can be re-identified, either directly or through probabilistic methods. This assessment goes beyond the data controller's own abilities and should consider other parties—potentially including unauthorized third parties—who might gain access to the model or its results. In particular, supervisory authorities should consider:

1. **Characteristics of the training data, the AI model, and the training procedure**: The nature of the dataset, the model's design, and its training process can influence the likelihood of re-identification.
2. **Context of release and processing**: Where and how the model is deployed affects who might access it, as well as what additional data or tools could be used for re-identification.
3. **Additional information available**: Other data sources, whether publicly accessible or privately controlled, could be combined with the model's outputs to reveal personal details.
4. **Costs and time needed for re-identification**: The feasibility of re-identification depends on the resources required. If it is relatively simple or inexpensive, the risk of re-identification increases[219].
5. **Current technology and future developments**: Re-identification techniques evolve, so the assessment must account for both existing methods and potential technological advancements[220].[221]

---

[219] Case C-479/22 P, *OC v European Commission*, paragraph 50.
[220] Case C-479/22 P, *OC v European Commission*, paragraph 50.
[221] EDPB, Opinion 2024/28, p. 15–16.

According to WP29 and EDPB guidance, an AI model may be deemed anonymous only if it is impossible to single out, link, or infer personal data from its parameters or outputs.[222] In practical terms, two main criteria must be met: (1) personal data used during training cannot be directly or indirectly retrieved, and (2) any queries made to the model must not reveal personal information about the data subjects. Given the complexity of modern AI systems, supervisory authorities are encouraged to start with the presumption that re-identification risk is significant, necessitating a thorough, case-by-case examination before concluding that a model is truly anonymous.[223]

As explained above, pseudonymization involves processing personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, which must be kept separately and protected through appropriate technical and organizational measures.[224] Unlike anonymized data, pseudonymized data remains subject to the GDPR, if the data can be linked to a natural person by feasible methods using additional information. In 2016, the CJEU issued a landmark decision in the case of Patrick Breyer v Bundesrepublik Deutschland, which addressed the issue of anonymization. This case questioned whether IP addresses should be classified as personal data. The court clarified that data cannot be feasibly identified if doing so is legally prohibited or would require an unreasonable amount of time, cost and effort.[225] In 2023, the General Court of the European Union (SRB v EDPS) provided further clarification on when pseudonymized data should be considered personal data. The court emphasized the importance of evaluating the situation from the perspective of the data receiver. Specifically, if the recipient of the pseudonymized data does not possess any additional information that would allow them to re-identify individuals and lacks the legal means to obtain such information, the data can be considered anonymized and thus not fall under the category of

[222] WP 216, Opinion 05/2014, p .24; EDPB, Opinion 2024/28, p. 15.
[223] EDPB, Opinion 2024/28, p. 16.
[224] GDPR, Article 4(5). See 5.2 Pseudonymization.
[225] Case C-582/14, Breyer v Bundesrepublik Deutschland.

personal data. Importantly, the court noted that just because the data sender can re-identify the data does not automatically make the data personal for the receiver.[226]

This 2023 ruling opens new avenues for anonymization practices and brings much-needed legal clarity. It highlights that the classification of data as personal or anonymous can depend on the capabilities and context of the data receiver. Consequently, the same piece of information might be deemed personal data for one party who can identify individuals, while it remains anonymous to another party without such abilities. This distinction is crucial for the development of medical AI, where handling and processing health data must comply with GDPR regulations while enabling technological advancements.

The reason why, the SRB v EDPS ruling is highly significant for developers of medical AI, is that if AI developer does not have access to pseudonymized health data—such as patient names and other identifying details in X-ray images—this data is considered anonymous from the developer's perspective. Consequently, the AI developer is not required to comply with GDPR obligations, as such health data is not classified as personal data under the regulation. This allows for the use of high-quality health data essential for AI development without the constraints of GDPR. Although, in theory, individuals could be identified through extensive and costly research using detailed health information, such methods are not deemed reasonable means to reclassify health data as personal data. This ruling thus supports the advancement of medical AI while ensuring that data protection standards are appropriately maintained.

5.5 Assessing Whether and How Anonymization or Pseudonymization Can Mitigate Consent Requirements.

When processing personal data for anonymization, consent is required up to the point of anonymization. Once data is anonymized, it is no longer subject to GDPR regulations. However, there remains ambiguity regarding what precisely qualifies as anonymized data and where the

[226] Case T-557/20, SRB v EDPS.

border lies. If a third party is responsible of anonymizing the data, to whom personal information must be transferred, consent is also necessary for this transfer. In such cases, it should be clearly communicated to the individual that they can exercise their rights up until their data is anonymized. After anonymization, the data is no longer classified as personal data, and the individual no longer holds rights over it.

For pseudonymized data, consent obtained by the data controller—such as a hospital—maintains GDPR obligations because pseudonymized data is still considered personal data. Transferring pseudonymized data to a third party also requires consent. If the AI is developed by the hospital or under its authority, the training data must be treated as personal data. Therefore, when obtaining consent, detailed information must be provided about the types of AI being developed, how the AI learns from personal data, and whether any data derived from personal information is retained. Additionally, it must be clearly explained how the data subject can withdraw their consent, including the extent and timeframe for such withdrawal.

In these scenarios, the conditions for valid consent necessitate comprehensive information for the data subject, as personal data grants extensive rights to the individual throughout the entire AI development process. Conversely, if the hospital acts as the data controller and pseudonymizes the data, the AI developer is an entirely external third party operating independently without being under the hospital's direction or acting on its behalf and the AI developer only has access to the pseudonymized data, the AI developer does not need to comply with GDPR obligations for that data, as it is considered anonymous. In this case, the hospital remains the sole party responsible for ensuring GDPR compliance.

When obtaining consent from the data subject, it must be clearly indicated that pseudonymized data is being sent to a third party for AI development—data from which identifying information has been removed but is still classified as personal data. It is likely sufficient to inform the data subject before obtaining consent that AI development is being conducted and clarify that their data cannot be used to identify them. The information duty in this case includes informing the data subject that they can withdraw their consent up until the pseudonymized data is transferred

to the third party. As technology advances, it may become possible to identify individuals from pseudonymized data using reasonable methods. To prevent this, the hospital can license pseudonymized data or use agreements to ensure that the AI developer does not retain pseudonymized personal data for future use.

However, it is vital to ensure the legality of the anonymization process, as supervisory authorities (SAs) have the power to impose corrective measures if an AI model is developed through unlawful processing of personal data. Such measures may include fines, temporary restrictions on processing, or orders to delete all or part of the dataset—or even the AI model itself—depending on the severity of the infringement and the potential harm to data subjects. Controllers must therefore ensure the lawfulness of the initial data processing before pursuing anonymization.[227]

If a model can be shown to be genuinely anonymized and no longer involves personal data, the GDPR typically will not apply to its subsequent use. However, simply asserting that a model is anonymous does not automatically exempt it from GDPR. SAs must independently verify that re-identification risks are negligible, based on the case-specific details provided by the controller. If anonymization is inadequate or the model still reveals personal data, the GDPR remains in effect and additional remedial steps may be required—such as re-training the model after lawful data collection or erasing unlawfully obtained data. In selecting the most appropriate and proportionate measures, SAs assess factors like the volume and sensitivity of the data, the gravity of the unlawful processing, the available technical solutions and the risks posed to individuals. Demonstrating a robust and legitimate foundation for anonymization protects data subjects' rights and provides a clearer path for AI models to operate without infringing on privacy regulations.[228]

[227] EDPB, Opinion 2024/28, p. 32, 34–35.
[228] EDPB, Opinion 2024/28, p. 32, 34–35.

6 Conclusions

6.1 The Impact of the Parties' Roles on Data Processing Requirements

The roles assumed by parties in the context of data processing play a critical role in determining their respective obligations under the GDPR. These roles, particularly the distinctions between data controllers, processors, and third-party entities, directly shape the legal and operational frameworks governing data processing activities. This chapter explores the implications of these roles, focusing on scenarios where data is pseudonymized or anonymized for purposes such as AI development and the resultant requirements for compliance under GDPR.

Under GDPR, the assignment of roles begins with identifying the data controller, which is the entity that determines the purposes and means of data processing. In contrast, a data processor acts on behalf of the controller and follows its instructions. This distinction has significant implications for the contractual obligations between parties, as controllers must ensure that processors adhere to the requirements of Article 28 GDPR through data processing agreements. The requirement for such agreements underscores the GDPR's emphasis on accountability and the proper delegation of responsibilities.

A particularly nuanced situation arises when health data is shared with a third party, such as an AI developer. Pseudonymization, while a robust data protection measure, does not necessarily render data anonymous under GDPR, as the original data controller retains the means to re-identify individuals, which indicates that the data subject could be linked to the data and the data may not be completely anonymized. Consequently, the sharing of pseudonymized data typically necessitates a valid legal basis under Article 6 GDPR, such as consent, legitimate interests, or a public interest exemption. In this scenario, if the AI developer acts solely on the hospital's instructions and for its benefit, it may be considered a data processor. However, if the AI developer processes the data for its own purposes, such as training an AI model for independent research, it assumes the role of a data controller, bringing additional legal responsibilities.

The question of legal basis becomes more complex, if the AI developer acts in any other role than recipient and the data provided to the AI developer is pseudonymized. According to GDPR Recital 26, truly anonymous data falls outside the regulation's scope as it can no longer be linked to an identifiable individual. However, the determination of whether data is truly anonymous depends on whether any party, including the data provider, retains the means to re-identify the data.[229] If the hospital ensures that the data is sufficiently anonymized before transfer, it no longer acts as a controller in relation to the AI developer's processing activities, as the GDPR does not regulate the processing of non-personal data. However, if the health data is only pseudonymized from the perspective of the hospital, it still hast to have a legal basis for the transfer of the pseudonymized data to the AI developer.

After the transfer of the pseudonymized data with sufficient legal basis, the hospital is no longer obligated to make sure that the AI developer follows the GDPR, as the pseudonymized data is classified as anonymized data for the AI developer. Nevertheless, ethical and contractual considerations may still necessitate a clear agreement governing the use of the data, especially in sensitive sectors such as healthcare. Even in cases where data is anonymized, the hospital's role as the originator of the data introduces reputational and ethical obligations. Licensing agreements[230] or black-box access systems, where the AI developer operates within controlled environments, provide mechanisms to limit risks and maintain oversight. These contractual arrangements serve to ensure compliance with ethical standards and safeguard against potential misuse or re-identification attempts, even if the data itself is no longer subject to GDPR.

In conclusion, the roles of parties involved in data processing activities—whether as controllers, processors, or independent entities—significantly influence their obligations under GDPR.

---

[229] WP29 Opinion 05/2014, p. 9.

[230] Licensing is a legal agreement where the owner of a product, work, or intellectual property (the licensor) gives permission to another party (the licensee) to use, modify, or distribute it under specific terms and conditions. Licensing is commonly used in areas like software, patents, trademarks, and creative content. It allows the licensee to use the item legally without transferring ownership rights. Licensing International. (https://licensinginternational.org/education/what-is-licensing/) (Accessed January 9, 2025).

These roles determine not only the applicability of specific legal bases for processing but also the extent of contractual and ethical considerations required to ensure compliance. The interplay between pseudonymization, anonymization and the roles of data providers and recipients highlights the nuanced and context-dependent nature of data protection law. By clearly delineating responsibilities and adhering to GDPR principles, organizations can navigate these complexities and foster trust in the ethical use of personal data

6.2 Lawful Grounds for Processing the Training Data Without Explicit Consent

Under the GDPR, fully anonymized data is no longer considered personal data and therefore falls outside the scope of the regulation. This allows anonymized data to be used without restrictions, including for AI development. In contrast, pseudonymized data remains within the GDPR's scope because it retains the potential for re-identification. However, when pseudonymized data is transferred to a third party, such as an AI developer, who lacks the means or legal authority to re-identify individuals, the data can effectively be treated as anonymized from the recipient's perspective. This distinction is significant for AI development, as anonymized data provides greater usability and flexibility, enabling developers to process the data without being subject to GDPR requirements.

For hospitals and other data controllers, the processing of training data can rely on explicit consent for pseudonymization and its subsequent use in AI development. However, under Article 6(1)(e) and Article 9(2)(j), hospitals can process data for purposes of public interest, such as scientific research or improving healthcare, without the need for explicit consent. In these cases, the hospital must ensure that appropriate safeguards, such as robust pseudonymization techniques, are implemented. When pseudonymization is carried out lawfully by the hospital under the public interest exception, AI developers who receive the data in its pseudonymized form do not require explicit consent to use it, if re-identification is not possible. This provides a legally compliant framework for enabling medical AI development without the complexities of obtaining individual consent at every stage.

Anonymization remains a critical tool for facilitating data sharing and reducing compliance burdens. Once data is fully anonymized, GDPR restrictions no longer apply, and the AI developer can use the data freely without limitations. For pseudonymized data, hospitals as data controllers, bear the responsibility of ensuring that pseudonymization techniques are robust enough to prevent re-identification, even if combined with auxiliary information. This responsibility extends to overseeing how third parties, such as AI developers, handle the data. Contracts or other binding agreements must guarantee that the pseudonymized data cannot be misused or lead to re-identification, safeguarding the privacy of data subjects even after the data has been shared.

The GDPR also provides flexibility through the concept of "broad consent," outlined in Recital 33, which allows data to be used for scientific research when it is difficult to specify all research purposes in advance. However, the principle of purpose limitation (Article 5(1)(b)) still applies, requiring that further data use remains compatible with the original purpose of collection. Fully anonymized data offers the most freedom in this regard, as it is no longer subject to GDPR requirements. Pseudonymized data, while still regulated, provides a valuable middle ground that balances data utility and privacy protection.

Legitimate interest, under Article 6(1)(f), offers another lawful ground for processing training data without explicit consent, as it allows processing that serves the interests of the data controller, provided these do not override the rights and freedoms of data subjects. However, legitimate interest poses challenges when applied to sensitive data, such as balancing test[231] with respect to evaluating the possibility to use the health information, due to the additional safeguards required under Article 9. Additionally, demonstrating that the processing serves a legitimate interest without infringing on individual rights can be difficult, particularly in contexts like medical AI development, where public trust is critical.

[231] The Legitimate Interests Assessment (LIA) is another critical component in determining the lawfulness of data sharing under the GDPR. A thorough LIA evaluates the necessity of processing for the identified legitimate interest, balances this against the data subjects' rights and freedoms, and ensures that safeguards are in place to mitigate risks. In scenarios involving pseudonymized data, a well-documented LIA can justify the sharing of data with third parties, provided that the interests pursued are legitimate and proportional. See EDPB, Guidelines 2024/01, p. 12–13.

Public interest grounds are particularly relevant in healthcare, where AI development can provide transformative benefits such as improved diagnostics, personalized treatments and enhanced patient outcomes. Hospitals can process personal data, including health data, under these grounds without requiring explicit consent, provided safeguards such as pseudonymization are in place. By ensuring that the pseudonymization process is strong enough to prevent re-identification and that third parties are unable to reverse it, hospitals can comply with GDPR while enabling the use of high-quality datasets for AI training. When data transitions from pseudonymized to effectively anonymous in the hands of AI developers, the GDPR no longer applies, granting developers the freedom to use the data without additional restrictions.

In conclusion, the GDPR provides multiple pathways for processing training data without explicit consent, depending on the circumstances. Hospitals can rely on public interest grounds to process data for AI development, provided that strong pseudonymization safeguards are implemented. Alternatively, explicit consent can be obtained for pseudonymization and AI-related use. Once data is anonymized, it falls outside GDPR's scope, enabling unrestricted use by AI developers. By ensuring robust safeguards and carefully managing the transition from pseudonymized to anonymized data, hospitals and AI developers can collaborate to innovate responsibly while protecting data subjects' privacy.

6.3 The Future of Medical AI Development

One of the most significant hurdles posed by the GDPR lies in its lack of precise guidance on applying lawful bases for processing, leaving organizations uncertain about how to legitimately handle health data for AI research. Although the regulation permits avenues such as consent or legitimate interests, the criteria for meeting these requirements remain open to interpretation, thereby deterring many from collecting and processing the expansive datasets needed for robust AI model training. Equally problematic is the ambiguity around when data is considered sufficiently anonymized, as even minor uncertainties about re-identification risks can discourage data sharing and stifle innovation. Without a clear, consistent benchmark for achieving genuine anonymity, which leaves the anonymized data outside of the scope of the GDPR, researchers

and developers may choose a more cautious approach, avoiding potentially transformative projects. This regulatory ambiguity discourages bold innovation, undermining Europe's capacity to realize the full benefits of AI-driven healthcare. Addressing these gaps with sector-specific rules or clearer benchmarks for anonymity could help align strong data protection with the practical needs of medical AI development.

In May 2022, the European Commission introduced a proposal for the European Health Data Space (EHDS), a health-specific data-sharing framework designed to facilitate the use of electronic health data. This initiative, grounded in new legislation, aims to enable the use of such data for purposes like patient care, research, innovation, policy-making, patient safety, statistics and regulatory activities.[232] The EHDS is part of a broader vision laid out in the European Commission's 2020 European Strategy for Data, which identified nine distinct "data spaces."[233] As the first to be implemented, the EHDS seeks to leverage digitalization to empower patients, granting them greater control over and easier access to their health data while fostering secure data sharing within the EU. This approach supports a dual goal of enhancing healthcare delivery and advancing research and innovation. Through purpose-built legislation and governance structures, the EU aims to ensure that data flows smoothly across sectors and borders within the Union while upholding fundamental European values. These include personal data protection, consumer rights, and fair competition. The framework is designed to promote clear, practical, and fair rules for accessing and using data, along with reliable governance mechanisms. Additionally, the EHDS envisions an open yet principled approach to international data sharing, maintaining alignment with European standards and priorities.[234]

One debated aspect of the proposal is its allowance for non-healthcare professionals to use personal health data, including sensitive information. While data holders are narrowly defined

---

[232] Dove 2024, p. 29; European Union. (2022, May 3). *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space* (COM/2022/197 final). EUR-Lex. (Accessed January 5, 2025)
[233] The nine identified data spaces encompass a wide range of sectors, including manufacturing (industrial data), mobility, health, finance, energy, agriculture, public administration, skills, and data related to the European Green Deal.
[234] Dove 2024, p. 30.

(health or care sector actors, relevant researchers, and EU institutions), there are no explicit limits on who can seek access under Article 47. This opens the door to a wide range of uses, from public health research to development and innovation activities, and underscores the need for a defined list of acceptable purposes to prevent indiscriminate exploitation.[235] By broadening access to personal health data, the proposed regulation could attract more AI developers and technology companies, fostering greater innovation and competition in the medical sector. Such expanded data availability would help refine AI algorithms, leading to more accurate diagnostics, personalized treatment plans, and faster research breakthroughs. In turn, the growth of these AI-driven solutions could boost economic prospects—by attracting new investments, creating jobs, and promoting cutting-edge research—while simultaneously enhancing patient care and advancing public health. However, these benefits hinge on the creation of robust safeguards and clear standards to preserve patient privacy and maintain public trust.

The proposal cites Article 6(1)(c) of the GDPR as its legal basis, allowing data processing to fulfill legal obligations. However, it departs from key safeguards by omitting individual consent for secondary use and any formal patient involvement in granting data-access permits. Critics worry that this could enable large tech companies to obtain permits for loosely defined "healthy lifestyle" services, especially given the broad definitions of health data. Recent amendments seek to align secondary use of health data with GDPR principles, particularly regarding patients' right to information. Amendment 106 would have limited the circumstances in which health data access bodies could withhold specific details from data subjects, echoing Article 14(5)(b) of the GDPR, but Amendment 368 ultimately removed this safeguard, and the final text did not restore it, raising transparency concerns. Meanwhile, Amendments 84 and 312 aimed to strengthen patient involvement by proposing an EU-wide opt-out and an opt-in mechanism for highly sensitive information, such as genetic or wellness data. However, the final text now mandates a universal opt-out, allowing Member States to override it under clearly defined public-interest conditions—striking a balance between individual autonomy and the broader needs of

[235] Sokol 2024, p. 376.

public health and innovation.[236] While the proposal clarifies legal grounds for certain public-interest uses, it also raises concerns about weakening GDPR safeguards on informed consent and transparency, suggesting a need for further guidance or amendments to protect patient rights and privacy in medical AI.

EHDS is largely consistent with the current legal framework regarding data protection, aiming to enhance the application of data protection requirements in the development of medical AI. By providing clearer guidelines, the EHDS seeks to facilitate the integration of GDPR principles into medical AI projects, ensuring that data handling practices align with established standards. This initiative is expected to streamline compliance for healthcare institutions and AI developers, promoting innovation while maintaining robust data protection. However, the EHDS does not eliminate all regulatory ambiguities. Certain aspects of the regulation remain open to interpretation, particularly in defining the boundaries between public interest-driven innovation and the protection of individual rights over personal data. Consequently, while the EHDS clarifies some requirements, it still leaves room for discretion in how public interest justifications are applied. This ongoing flexibility necessitates that medical AI developers remain vigilant in balancing the advancement of healthcare technologies with the safeguarding of individuals' privacy rights, ensuring that public interest remains a valid and well-supported legal basis for data processing.

[236] Sokol 2024, p. 382–383.