



# GDPR's Reflection in Privacy-Enhancing Technologies: Implications for AI Data Protection

Tytti Rintamäki

Thesis submitted for assessment with a view to obtaining the degree of Master of Arts  
in Transnational Governance of the European University Institute

Florence, 15.05.2023.

European University Institute

**School of Transnational Governance**

## GDPRs Reflection in Privacy-Enhancing Technologies: Implications for AI Data Protection

Tytti Rintamäki

Thesis submitted for assessment with a view to obtaining the degree of Master of Arts  
in Transnational Governance of the European University Institute

**Andrea Renda**

Professor Andrea Renda, European University Institute

© Author, [Year] . This work is licensed under a [Creative Commons Attribution 4.0 \(CC-BY 4.0\) International license](#)

If cited or quoted, reference should be made to the full name of the author, the title, the series, the year, and the publisher.

**Student declaration to accompany the submission of written work School of Transnational Governance**

I Tytti Rintamäki certify that I am the author of the work <title> I have presented for examination for the Master of Arts in Transnational Governance. at the European University Institute. I also certify that this is solely my own original work, other than where I have clearly indicated, in this declaration and in the thesis, that it is the work of others.

I warrant that I have obtained all the permissions required for using any material from other copyrighted publications.

I certify that this work complies with the Code of Ethics in Academic Research issued by the European University Institute (IUE 332/2/10 (CA 297)).

The copyright of this work rests with its author. Quotation from this thesis is permitted, provided that full acknowledgement is made. This work may not be reproduced without my prior written consent. This authorisation does not, to the best of my knowledge, infringe the rights of any third party.

I declare that this work consists of 9333 words.

Signature and date:



15.05.2023

## **ABSTRACT**

The responsibility for regulating emerging technologies such as AI is falling into the hands of the Data Protection Regulators as responsibility is attributed to them through the AI Act. The General Data Protection Regulation (GDPR) will serve as the data governance framework that is expected to protect European data. Despite debates, this paper will show that GDPR and AI systems can coexist. But how should AI systems begin to implement GDPR in their design? This study turns to Privacy-enhancing technologies (PETs) and how well they reflect GDPR to draw lessons for future AI. This analysis finds through content analysis that GDPR is largely reflected in the privacy policies, bylaws and codes of conduct of various PETs and encourages AI systems to learn from this. Specifically this research suggests that AI systems should utilize PETs as tools to further enhance their data protection and compliance with GDPR.

## TABLE OF CONTENTS

Introduction	1
Literature Review	5
Theoretical Framework	12
Research Question and Methodology	13
Analysis	16
Discussion	21
Conclusion	22
Annex	24
Bibliography	25

## **LIST OF ABBREVIATIONS:**

AI Artificial Intelligence

GDPR General Data Protection Regulation

PETs Privacy-enhancing technologies

PDG Privacy by design

EU European Union

UNESCO The United Nations Educational, Scientific and Cultural Organization

## Introduction

In this era of the explosion of artificial intelligence (AI) applications into public use, concerns over data protection and privacy are warranted and need attention. Unfortunately, it has already become clear after multiple cases of issues of data protection that adequate frameworks are missing and not enough privacy measures are in place. Luckily within Europe, the data governance framework of the General Data Protection Regulation (GDPR) provides policies and guidelines to protect Europeans and their data. However, AI system applications do not necessarily respect this European legislation for many reasons, including the vagueness of the regulation, lack of implementable advice and much more. Instead, it is up to data protection authorities to investigate and issue fines when AI software owners have established headquarters within member states. In cases where these companies operate within Europe without having located their operations here, it is up to member state countries to initiate their investigations and issue their fines or bans on the technology.<sup>1</sup> Countries like Italy have taken action when they've seen injustice, like in the recent case of temporarily banning ChatGPT. After urging Open AI to comply with GDPR and influencing changes to be made, age verification before accessing the system, amongst some other fixes, took place, and the ban has now been lifted.<sup>2</sup> ChatGPT is only one of the use cases of AI systems interacting currently with our societies. The risks posed by these systems vary depending on their size and area of implementation, but AI systems are used by government, healthcare, aviation, transport, communications etc., so the challenges are faced in almost all industries.

Not only are European member states concerned by these AI systems, but this worry is also growing in the populations and tech giants abroad. A study by the European Consumer Organisation surveyed whether Europeans believe that increased AI system deployment will come at the cost of personal data violations. Over half of those who responded strongly agree.<sup>3</sup> The public and public authorities are concerned with the lack of data protection, but interestingly so are those in the industry. Big names in the tech industry (including Elon Musk, Steve Wozniak and Microsoft and Google engineers) that previously encouraged AI development and investment are encouraging to slow down or pause AI development for six months. This request came in the form of an open letter in March, urging that the industry pause the development of AI systems that exceed the capabilities of the GPT-4 update and instead spend the time designing measures to protect from the harm these systems can do to safety.<sup>4</sup>

---

<sup>1</sup>Goujard, C., & Volpicelli, G. (2023, April 10). *Chatgpt is entering a world of regulatory pain in Europe*. POLITICO. Retrieved from: <https://www.politico.eu/article/chatgpt-world-regulatory-pain-eu-privacy-data-protection-gdpr/>

<sup>2</sup>Kayali, L., & Goujard, C. (2023, April 13). *Chatgpt could come back to Italy by end of April*. POLITICO. Retrieved from: <https://www.politico.eu/article/chatgpt-italy-lift-ban-garante-privacy-gdpr-openai/#:~:text=In%20late%20March%2C%20ChatGPT%20was,them%20from%20accessing%20the%20chatbot>

<sup>3</sup>Von Gravrock, E. (n.d.). *Artificial Intelligence Design must prioritize data privacy*. World Economic Forum. Retrieved from: <https://www.weforum.org/agenda/2022/03/designing-artificial-intelligence-for-privacy/>

<sup>4</sup>Guardian News and Media. (2023, April 1). Letter signed by Elon Musk demanding AI research pause sparks controversy. The Guardian. Retrieved from <https://www.theguardian.com/technology/2023/mar/31/ai-research-pause-elon-musk-chatgpt>



This shows that the creators and users of this technology understand and foresee the damage that could be done if AI software continues developing at this rate with little to no regard for protective measures.

The question of how to better protect data in the age of AI is being worked on around the globe. Internationally UNESCO and the OECD have published reports around governing AI.<sup>5</sup> Canada pioneered a framework that developed categories and ranked their significance regarding what was at stake. Germany took a different route and defined some AI systems as completely or partly prohibited due to potential wrongdoings. Japan has prepared contract clauses that must be accounted for in data or AI systems, taking a more corporate approach. The United Kingdom has prioritised the user in ensuring that AI systems are fair and safe by pushing for measures to increase compliance with transparency, fairness and legal requirements. Most recently they published the draft of their Online Safety bill which will subject AI to some regulatory requirements.<sup>6</sup> Singapore has opted for a neutral approach in the technology, algorithm, sector, scale, business and more, resulting in more of a risk reduction method. The United States wishes not to put up barriers that will stifle innovation and AI system growth but understands the importance of protecting society from harm through the draft of their sectoral approach targeting agencies that are in direct contact with AI systems.<sup>7</sup> At the EU level, many AI governance frameworks have been proposed and formulated, including the Ethical Guidelines for Trustworthy AI by the High-level Expert Group on AI and the AI Act, which is soon to be published to implement legislative measures to mitigate the many challenges these systems pose. The findings point truth to the following statement by Gabriela Zanfir-Fortuna from the Future of Privacy Forum, “Data protection regulators are slowly realizing that they are AI regulators”.<sup>8</sup> These data protection regulators are now being tasked with creating legislation that impacts transnational data flows and transfers, and this geographical scope only adds to the complexity that AI systems bring to the table.

An important aspect of the debate on how to regulate AI is whether the GDPR is an adequate framework to address the problems posed by the systems. One of GDPRs authors and member of the European Parliament at the time, Axel Voss, warned in 2020 that he thought the regulation was already out of date when dealing with the world post-COVID-19.<sup>9</sup> He even went on to explicitly state that “We have to be aware that GDPR is not made for artificial intelligence,”. Sophie in’t Veld, a Dutch Member of the European Parliament, disagreed and

---

<sup>5</sup> Koerner, K. (2022, January 20). *Privacy and responsible ai*. Privacy and responsible AI. Retrieved from: <https://iapp.org/news/a/privacy-and-responsible-ai/>

<sup>6</sup> Draft online safety bill - joint committee on the Draft Online Safety Bill. (n.d.). <https://publications.parliament.uk/pa/jt5802/jtselect/jtonlinesafety/129/12906.htm>

<sup>7</sup> Renda et al. (2021), Study in support of the European Commission’s impact assessment of the Ai Act <https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1>

<sup>8</sup> Goujard, C., & Volpicelli, G. (2023, April 10). *Chatgpt is entering a world of regulatory pain in Europe*. POLITICO. Retrieved from: <https://www.politico.eu/article/chatgpt-world-regulatory-pain-eu-privacy-data-protection-gdpr/>

<sup>9</sup> Espinoza, J. (2021, March 3). *EU must overhaul flagship data protection laws, says a “father” of policy*. Financial Times. Retrieved from: <https://www.ft.com/content/b0b44dbe-1e40-4624-bdb1-e87bc8016106>

stated that no legislation is perfect but GDPR took years to finalise after extensive research and discussion, and its strength lies in its flexibility.

This research project will assist this debate by assessing the GDPRs data governance framework's ability to have impacted Privacy-Enhancing technologies. Specifically, this paper will investigate how comprehensively GDPR is reflected in Privacy-enhancing technologies (PETs) and use these findings to discuss what implications this has on AI systems that will soon need to abide by GDPR. The specific objective is to examine to how the data governance framework of GDPR is reflected in PETs by analysing the presence of the principles of Article 5 of GDPR within the privacy policies of various PETs. The precise research question to be examined is how comprehensively is the GDPR (Article 5) reflected in Privacy-enhancing technologies design. In sum, this thesis will argue that PETs strongly reflect GDPR were applicable, and this means AI systems should either be designed like PETs or utilise them as tools for their data protection compliance.

The structure of this thesis goes as follows, the current debate of existing literature will be explained. Then the data governance approach will be made clear in the theoretical framework section and placed into the context of why it is the best guiding structure for this study. Then the method of analysis will be explained, followed by the analysis and concluding with a discussion of the findings.

## **Literature Review**

With concerns about data protection and privacy circulating current discourse, studies have been interested in what framework to follow to ensure the protection of data subjects from the risks posed by emerging technology. GDPR has been the data governance framework of the EU for the past five years now and is attributed as the regulation AI systems should follow to abide by European data protection rules. This regulation has influenced other technologies, such as Privacy-enhancing technologies, companies dealing with personal data and research taking place in Europe. PETs, despite their name, vary in their privacy purposes and abilities to address data-related issues. This literature review will examine GDPR as a data governance framework and its relevance, what relationship there exists between AI and GDPR, the possible similarities between GDPR and the Ethical Guidelines for Trustworthy AI, how Privacy laws have changed since GDPR, and concluding on what PETs are and why they are the unit of analysis for this paper. By summarising what existing literature has to say about each of these topics, an overview of data protection within Europe will be covered, especially what this means in this day and age of AI systems and PETs.

### *GDPR as a data governance framework*

It is not surprising that the AI Act highlights complying with GDPR to achieve data protection measures as it is the predominant data governance framework within Europe. GDPR

established itself as a European data governance framework<sup>10</sup> after harmonising data protection and privacy across the continent in 2018.<sup>11</sup> The data protection regulation created requirements through policy and guidance for companies, organisations and other entities on how personal data is collected, processed, used and shared.<sup>12</sup> This means companies, organisations and other entities are now expected to consider how they go about data in all the stages of the data lifecycle and what role they play in ensuring privacy.<sup>13</sup> This has resulted in overall coherence in how data is treated in Europe. Despite this understanding, compliance rates are not incredibly high as it is at the member states discretion to decide how to implement GDPR and their data protection authority to investigate adherence. Critics of this regulation argue that the biggest weakness in this regulation is its divergent implementation leading to weak compliance.<sup>14</sup>

### *Article 5 of GDPR*

The key principles of Article 5 of the GDPR covers different stages of the data lifecycle and is therefore the analytical framework of choice for this research paper. The seven principles in this Article are Lawfulness, fairness, transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality (security) and Accountability. This Article covers different stages of data lifecycles, making it comprehensive in its demands and applicability. The first four touch on the collection of data, ensuring this is done lawfully, fairly and transparently, the purpose is defined, only the minimum required data is collected, and it is ensured that it's accurate. The storage limitation involves storing data and doing so for the disclosed time. All of these principles apply to the processing of data touching on yet another stage of the data lifecycle. The analysis and deployment stages of data are concerned in general with the accuracy, integrity and confidentiality and accountability principles. Lastly, the archiving life stage is implied in the storage limitation and the security principle because archiving sensitive information poses a risk of being hacked into and exposed in the future, requiring security features to prevent this. This goes to show that Article 5 of GDPR involves all six stages of the data lifecycle, which are collection, storage, processing, analysis, deployment and archiving.<sup>15</sup> This is relevant for this research paper as the framework to be analysed is this specific Article amongst some other aspects of GDPR but nonetheless, this shows how comprehensive just this one article is.

---

<sup>10</sup> Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection regulation: what it is and what it means, *Information & Communications Technology Law*, 28:1, 65-98, DOI: [10.1080/13600834.2019.1573501](https://doi.org/10.1080/13600834.2019.1573501)

<sup>11</sup> D. Torre, G. Soltana, M. Sabetzadeh, L. C. Briand, Y. Auffinger and P. Goes, "Using Models to Enable Compliance Checking Against the GDPR: An Experience Report," *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*, Munich, Germany, 2019, pp. 1-11, doi: 10.1109/MODELS.2019.00-20.

<sup>12</sup> *Data Governance and GDPR: An introduction*. Splunk. (2021, May 1). [https://www.splunk.com/en\\_us/data-insider/data-governance-and-gdpr.html](https://www.splunk.com/en_us/data-insider/data-governance-and-gdpr.html)

<sup>13</sup> Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection regulation: what it is and what it means, *Information & Communications Technology Law*, 28:1, 65-98, DOI: [10.1080/13600834.2019.1573501](https://doi.org/10.1080/13600834.2019.1573501)

<sup>14</sup> He Li, Lu Yu & Wu He (2019) The Impact of GDPR on Global Technology Development, *Journal of Global Information Technology Management*, 22:1, 1-6, DOI: [10.1080/1097198X.2019.1569186](https://doi.org/10.1080/1097198X.2019.1569186)

<sup>15</sup> *6 data lifecycle stages: Data Cycle Management Guide*. Segment. (n.d.). Retrieved from: <https://segment.com/blog/data-life-cycle/>

## Transparency

One of the seven principles of Article 5 that will be analysed in depth within this analysis is Transparency. Transparency is a part of the principles of GDPR but is also a requirement in the AI Act and they differ in their definitions. GDPR mandates transparency comes with transparent means of processing data (article 5) and transparent information and communication (Articles 12, 13 & 14). This means that by informing users through effective communication and making clear what the procedures are for processing data, transparency can be achieved. Importantly GDPR calls for transparency at two points in time, first at the moment a user's information enters the system (ex-ante transparency) and at the output stage when the system produces an outcome that concerns the users data (ex-post transparency).<sup>16</sup> Transparency within GDPR is, therefore, informed communication and openness of data processing before data is used and after output is run, requiring means to achieve this at both stages of the data lifecycle.

On the other hand, transparency in the AI Act appears alongside information “Provision of information and transparency”<sup>17</sup>. This shows a move away from transparency as an open system, open source, but instead to providing information, essentially explainability. There is no mention of making processes or processing of data clearly open. There are also specific transparency obligations for informing users that they are interacting with an AI system, or biometric systems are in use, or what they are seeing is a deep fake (Article 52). This calls for transparency as instructions for the use of AI systems. Some say it addresses transparency adequately, siding with explainability equalling transparency.<sup>18</sup> Recently the European Parliament released an update on the transparency requirements that will affect large language models like ChatGPT. These additional transparency requirements appear in the AI Act outside of just informing users that they are interacting with AI to divulge the content was created by their system but also making sure no unlawful content is produced and delivering reports on the data used in training.<sup>19</sup> But all descriptions considered if one can explain what is happening within the system and to the data, then one would be considered transparent. Both versions of transparency will be taken into consideration in this analysis so that a thorough understanding of how it may appear in PETs will be identified.

---

<sup>16</sup> European Parliament. (2020, June 25). *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Think tank: European parliament*. Think Tank | European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530)

<sup>17</sup> European Commission et al. (2021). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206>

<sup>18</sup> Niet, I., van Est, R., & Veraart, F. (2021). Governing AI in Electricity Systems: Reflections on the EU Artificial Intelligence Bill. *Frontiers in Artificial Intelligence*, 4. <https://doi.org/10.3389/frai.2021.690237>

<sup>19</sup> *Ai Act: A step closer to the first rules on Artificial Intelligence: News: European parliament*. AI Act: a step closer to the first rules on Artificial Intelligence | News | European Parliament. (2023, May 11). Retrieved from: <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence>

## *AI and GDPR*

With the AI Act dictating the GDPR to be followed by AI systems, research has flooded to discuss whether a regulation drafted in 2015, and enforced in 2018 has the ability to regulate technology emerging in 2023. After reviewing the research, the answer is simple. The GDPR framework outlines data protection measures in a way that leaves enough room to manoeuvre and, therefore, enough room for AI systems to be able to interpret these rules in their own systems. There are, however, some concerns that need to be discussed.<sup>20</sup>

The biggest concern surrounding GDPR and AI is the use of big data by AI systems as the larger the data set, the better the results are. There is room within GDPR to navigate the pros of using big data but this is where a lot of tension lies. To overcome this grey area researchers urge GDPR to be implemented into AI systems with assistance from data protection authorities to ensure correct and suitable interpretations of the guidelines. To give this assistance more teeth, AI developers and companies need to all conform to comply with GDPR and increasing the enforcement mechanisms of issuing harsher fines would likely incentive this.<sup>21</sup>

“GDPR does not seem to require any major change in order to address AI.”<sup>22</sup> is the consensus of a study issued by the European Parliament. Though much of it is true, it does point to some data problems that arise from AI systems that GDPR does not provide solutions for. An example of this is automated decision-making, where the algorithm makes decisions which are beyond difficult to explain or backtrack, and what this means for users and exercising their rights in these conditions. GDPR is also focused on the individual data users whereas AI systems go further to pose serious threats to society as a whole and democratic values, creating larger issues that require discussion that GDPR simply cannot address.

But so the issue is not the compatibility of AI and GDPR but the effectiveness of GDPR in general. Its articles and wording often leave too much room for interpretation due to their vague nature. Defining something specifically and outlining action items for these, would be more effective but is detrimental in the technology industry that advances so fast that by weeks end, the technology and the ways it can be used will have adapted so that these regulations do not apply anymore. Therefore the balancing act of making guidelines more impassable and precise but without limiting future applications is where the incompatibility lies. And in general, GDPR was drafted and implemented when AI was not a concern, therefore, the regulators did not predict this hence why it is not mentioned nor do the guidelines suit perfectly. Nevertheless, it

---

<sup>20</sup> European Parliament. (2020, June 25). *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Think tank: European parliament*. Think Tank | European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530)

<sup>21</sup> European Parliament. (2020, June 25). *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Think tank: European parliament*. Think Tank | European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530)

<sup>22</sup> European Parliament. (2020, June 25). *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Think tank: European parliament*. Think Tank | European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530)

shows resilience in its ability to be comprehensive and workable even with these challenges.<sup>23</sup> But the real issue with the effectiveness of GDPR is in its ability to have companies, organisations etc., comply with its guidelines. Studies of company compliance with GDPR have repeatedly shown poor results. In some cases, the companies do not even possess the ability to deal with data-related requests.<sup>24</sup> This is because, without a clear and working data management system, entities will have a hard time complying with any requests from users regarding requesting evidence of processing of their data or erasure of their data. The reason so many companies lack a workable data management system to assist them with GDPR measures is because of the vagueness of the regulation. Without clear and concise requirements, companies are left to decipher how best to abide by the rules and too often, non-compliance becomes the easier option.<sup>25</sup> Therefore actionable guidelines need to be issued by the European Commission and European Parliament on how best to implement GDPR for these companies and the ones concerned with AI development. But the compliance issue is also complicated by the fining enforcement mechanism not deterring companies as much. Critics of GDPR worry that burdening data protection authorities with the task of overseeing AI systems on top of what they already do will slow the rollout of fines and lessen the deterrence effect for not complying.<sup>26</sup> Therefore the EU is encouraged to expand their data protection supervisor body and invite member states to do the same.

### *GDPR and Ethical Guidelines for Trustworthy AI*

Though there is a discussion on whether it is effective or feasible to have AI regulated by GDPR, there is a notable correlation between GDPR and the Ethical Guidelines for Trustworthy AI. There are seven requirements outlined by the European commissions high-level expert group on AI in the guidelines for AI. These are “Human agency and oversight, Technical Robustness and safety, Privacy and data governance, Transparency, Diversity, non-discrimination and fairness, Societal and environmental well-being, and Accountability”.<sup>27</sup> Interestingly, these overlap heavily with GDPR articles with the exception of one, the societal and environmental well-being, which is not explicitly stated but can be inferred from the notion of protecting fundamental rights. The requirement of human agency correlates with Article 22, which outlines that users have the right not to have decisions made completely by technology but have some human oversight in the decision. The technical robustness and safety requirement overlaps with Article 25, where the controller is tasked with implementing necessary technological and organisational controls to limit the risks to data, and Article 32,

---

<sup>23</sup> European Parliament. (2020, June 25). *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Think tank: European parliament*. Think Tank | European Parliament.

[https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530)

<sup>24</sup> Help Net Security. (2019, December 4). *Despite potential fines, GDPR compliance rate remains low*. Help Net Security. Retrieved from: <https://www.helpnetsecurity.com/2019/12/04/gdpr-compliance-rate/>

<sup>25</sup> Koerner, K. (2022a, January 20). *Privacy and responsible ai*. Privacy and responsible AI. Retrieved from: <https://iapp.org/news/a/privacy-and-responsible-ai/>

<sup>26</sup> Council of Europe. (2019, January 25). *Artificial Intelligence and data protection - RM.COE.INT*. <https://rm.coe.int/prems-192119-gbr-2051-lignes-directrices-sur-l-intelligence-artificiel/1680a4ca4a>

<sup>27</sup> European Commission. (2019). *Ethics guidelines for trustworthy AI*. Retrieved from <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>



where controllers are required to implement actions to increase security. The privacy and data governance requirement correlates with Article 5, which outlines the principles for analysing data on all the data lifecycle stages but also demands extra security measures to be in place on the organisational level. Transparency is mentioned under Article 5 in data processing, in Article 12 under transparent information and implied in Article 15 about the right to have access. Article 9 specifies that data should be of non-discriminatory nature, which coincides with non-discrimination, and Article 5(1) stipulates data should be processed fairly, which corresponds with the requirement of fairness. And accountability is addressed in articles 24 and 25, where controllers have to produce results of compliance with GDPR upon request. The overlap of these two texts strengthens the push to have AI regulated by GDPR principles which are reinforced by the Ethical Guidelines for Trustworthy AI.

### Privacy laws after GDPR

Privacy policies after the implementation of GDPR reflect many of the guidelines as privacy laws are generated from their national or regional privacy regulation environment. The specificity of the type of personal data in question at any part of the data lifecycle has been more defined since GDPR, for example, specifying when personal information meant email address or telephone number. The ambiguity of the privacy text also sharply increased with the use of words such as “may”, “typically”, or “sometimes”, despite GDPR urging for more clarity to increase transparency. The possibility of action ex-ante also appeared where previously there were no abilities such as the right to erasure, objection, or access. A more obvious observation was the increased data protection measures and the delegation of responsibility. User consent rose most notably in the mentioning of cookies.<sup>28</sup> As a result of the introduction of GDPR, updated privacy policies have emerged to protect European user data. But this is not to paint a rosy picture of the situation. Studies of privacy policies often find vague language and a lack of clarification and information. A machine learning technology that analyses the fairness of privacy policies was used to investigate this,<sup>29</sup> called the Claudette system.<sup>30</sup> This showed that though the various articles do make an appearance in privacy policies, they are often left to be too vague for actual actionable options for users. The level of capabilities users actually have and what are just decorated words in the policies is worth further investigation.

*What are PETs, and why are they the unit of analysis?*

PETs data back to as far as 1995 when Dutch and Canadian authorities on data and privacy joined forces and wrote a report on creating anonymous transactions on the internet. Since then, they have increased and provided solutions to a multitude of privacy and data protection problems. There are various ways of defining PETs, but this study draws on academic and

---

<sup>28</sup> Bateni, Nastaran & Kaur, Jasmin & Dara, Rozita & Song, Fei. (2022). Content Analysis of Privacy Policies Before and After GDPR. 1-9. 10.1109/PST55820.2022.9851983.

<sup>29</sup> EUI. (n.d.). *Use our tools!*. CLAUDETTE. Retrieved from: <http://claudette.eui.eu/use-our-tools/index.html>

<sup>30</sup> T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz, “The privacy policy landscape after the GDPR,” arXiv, 2018, doi: 10.2478/popets- 2020-0004.

practical definitions to define them as technologies and tools that provide possibilities for increasing data protection and privacy through various technical means.<sup>31</sup>

The European Commission, amongst others, agree that PETs can be a solution towards enhanced data protection because of their varied applicability and use.<sup>32</sup> PETs come as tools or even technologies and are often regarded as complementary to systems that already exist to enhance privacy, as stated in their name. Critics of the effectiveness of PETs argue that their complexity, cost, difficulty overseeing, and lack of standards create a false image of true privacy protection. They dispute that the different technologies are a means to solve privacy and data protection issues by stating that they are actually complicated to use and costly in terms of implementation and maintenance. An added layer of complexity is the difficulty in ensuring these technologies abide by existing regulations or assess their capacity to enhance privacy. This is also because various standards exist, meaning the technologies do not necessarily abide by similar protocols, making assessing their effectiveness increasingly difficult. Critics state that despite their name providing a sense that these technologies provide increased data protection and simultaneously causing us to assume they strongly abide by data protection measures and regulation, they have actually played a part in the problems with data. This is because of all the reasons mentioned above and the use of these technologies being expensive, used inaccurately, making claims that sound convincing, yet don't follow the same standards, risking data, and lacking enforced adequate measures. This goes to show that PETs in the hands of people, not equipt to understand, properly utilise and validate operability pose more problems than solutions.<sup>33</sup>

Despite varying thoughts on the effectiveness of PETs in enhancing privacy and data protection, the purpose of this research is to investigate whether these technologies abide by GDPR. The current literature is lacking in a genuine comparison of PETs and GDPR. It seems futile to investigate if a privacy-enhancing technology abides by a privacy regulation because it is assumed. But what this study understands is that if such is true, then this has wide implications for future technologies that are expected to abide by GDPR. Because if GDPR is best represented in PETs, does that assume future technologies should look like PETs? But specifically, does that mean that the AI Act expects future AI systems to be like PETs when abiding by GDPR? This will be debated further in the discussion section of this research paper and will add to the current discussions on how AI systems can implement the data protection measures outlined in GDPR.

This literature review has been extensive, providing insights from the various topics related to the discussion of data protection in emerging technology. What this research found was that

---

<sup>31</sup> Renieris, E., Zafir-Fortuna, D. G., Bartoletti, I., Marda, V., & Peppin, A. (2021, April 29). *Why pets (privacy-enhancing technologies) may not always be our friends*. Ada Lovelace Institute. Retrieved from: <https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/>

<sup>32</sup> Communication COM (2007)228 from the Commission to the European Parliament and the Council. On Promoting Data Protection by Privacy Enhancing Technologies (PETs) (2007)

<sup>33</sup> Renieris, E., Zafir-Fortuna, D. G., Bartoletti, I., Marda, V., & Peppin, A. (2021, April 29). *Why pets (privacy-enhancing technologies) may not always be our friends*. Ada Lovelace Institute. Retrieved from: <https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/>



GDPR is a reasonable data governance framework to demand AI systems abide by because its principles can coexist with AI systems, other AI-related publications strongly mirror this framework, and it is comprehensive in what principles it covers. The following section will present the selected theoretical framework of the data governance approach and how this will frame the analysis at a later stage.

## Theoretical Framework

The chosen theory to guide researching this question is the data governance approach. The data governance approach shows how a data governance framework that details how existing technologies should implement data protection policies regarding the collection, storage, use, and sharing of data will result in unity amongst those under the framework. The chosen data governance framework for this analysis is GDPR, specifically Article 5, which will be used to investigate how well the regulation has achieved unifying data protection and privacy in privacy-enhancing technologies used in Europe.

Data governance is essentially an approach that aims to ensure data protection by complying with existing regulations and laws. Data governance aims to achieve unity amongst many bodies interacting with data, be they companies or organisations. Within the EU, a general data protection regulation is in place to achieve coherent data governance within the various member states. Within data governance exists the data governance framework, which includes a variety of different policies, requirements, logistics and codes of conduct which are all concerned with how data is governed.<sup>34</sup> This study is concerned with the policies, requirements etc., outlined in GDPR and how data is governed within this regulation. This regulation aims to protect personal data from harm and ensure protective measures are in place to respect the fundamental rights of European Data subjects. This means that this regulation applies to technologies that conduct their business globally or in many European countries and therefore use data from European data subjects, impacting their privacy. Whilst this approach is often concerned with how data quality, data security is managed and whether this data governance framework is complied with. This study takes a few of these aspects for granted. This study proceeds on the footing that GDPR ensures data quality and security are managed if a high level of compliance exists. Therefore the question remains, whether privacy-enhancing technologies comply with GDPR.<sup>35</sup>

Other theories were considered to frame the analysis, including privacy by design and the capability approach. Privacy by design was contemplated as it involves assessing how well privacy is implemented into the design phase, making it a built-in essential feature.<sup>36</sup> This approach includes seven principles prioritising privacy in the early stages of development, but

---

<sup>34</sup> Leveneur, F. (2023, April 22). *How data governance helps achieve regulatory compliance*. Data Sleek. Retrieved from: <https://data-sleek.com/blog/data-governance-best-practices/>

<sup>35</sup> Leveneur, F. (2023, April 22). *How data governance helps achieve regulatory compliance*. Data Sleek. Retrieved from: <https://data-sleek.com/blog/data-governance-best-practices/>

<sup>36</sup> Privacy by design. Etyca. (n.d.). Retrieved from <https://etyca.com/about-privacy-by-design>

these are slightly different from those in the GDPR. This is because the purpose of these principles is to include privacy in the design of technologies vs principles for achieving a legal framework that protects data. It is no surprise that PETs implement privacy by design, they are privacy-enhancing technologies, after all, but the question is whether these design elements respect the GDPR. Some elements of Privacy by design are still relevant and will be incorporated in the analysis as they are relevant and included under the seven principles of GDPR (Article 5). Privacy by design is also mentioned in GDPR under Article 25. However, it does not go further than stating that “appropriate technological and organisations measures” need to be put in place in the design to protect the data protection principles. This exposes a weakness in the push for PBD as it is advised in a vague and open nature. Therefore the mention provided in GDPR is not an adequate framework due to the lack of a process and options for achieving PBD features.<sup>37</sup>

Another theory that was considered is the capability approach. The capability approach would have put the lens on how many capabilities users are given to control their data or to enhance their level of privacy. These would’ve become apparent through the actionable options users are provided but would be an ex-ante approach to fixing privacy issues only once a user has felt the negative effects of lack of data protection and wanted to lock down their data further. This approach was disregarded as it does not fit the goal of the research, which is to see how well GDPR is reflected in technologies as a whole.

This research project is therefore framed by the data governance approach, providing the context of GDPR as a data governance framework encouraging protective and privacy-enhancing features in any industry concerned with data. The following section will elaborate on how this research will conduct the analysis of how well GDPR is reflected in PETs, assessing privacy policies, bylaws etc. and comparing these to Article 5 of GDPR.

## **Research Question and Method**

This research aims to answer the question of how comprehensively is Article 5 of the GDPR reflected in PETs privacy policies, bylaws and codes of conduct. This will be done by conducting a content analysis of the seven principles of Article 5 in GDPR in PETs. The principles in Article 5 are key aspects of the GDPR data governance framework that happen to also cover all stages of the data lifecycle, which will showcase the level of compliance with data protection and privacy in the units of analysis. The chosen units of analysis are PET’s privacy policies, codes of conduct and privacy bylaws. This was chosen to identify patterns, themes, and trends in the different data units to evaluate how well existing regulation is reflected in the technology and therefore show the level of compliance with data protection regulation.

---

<sup>37</sup>Privacy by design. General Data Protection Regulation (GDPR). (2021, October 22). Retrieved from: <https://gdpr-info.eu/issues/privacy-by-design/>

Previous studies have analysed the effects of GDPR on the privacy policies of major companies since its implementation to see the level of compliance with the regulation and protections in place for personal data. These studies utilised their own codebooks therefore, there are plenty of codebooks on GDPR that already exist. The most exhaustive codebook was extracted from previous studies<sup>38</sup> and adapted to be more comprehensive by focusing on the specific principles that are focused on and relevant terminology to these. Specifically, this study will utilise the codes to uncover the amount of GDPR principles present in privacy-enhancing technologies to assess the compliance of GDPR within these technologies. As mentioned, the codebook was expanded to include other relevant articles and terminology for a more comprehensive overview of how GDPR might be incorporated into the technologies. It was also expanded due to the understanding that the technologies may use terminology similar to that used in GDPR but not the exact working<sup>39</sup>, requiring it to be improved upon.

The qualitative content analysis methodology will allow for analysing and interpreting textual data from various sources to establish patterns and connections. Privacy policies of PETs were picked as the unit of analysis due to these documents containing how user data is collected, stored and used.<sup>40</sup> The study is limited to privacy-enhancing technologies that are based in Europe or conduct enough of their operations within the borders to have taken GDPR into consideration in their design phase to ensure compliance with the regulation. Another element that played a role in data collection was whether their privacy policies or codes of conduct were publically available and readable, meaning not full of technical jargon or embedded in code. This was for the purpose of the coding software to be able to actually analyse the text because relevant terminology or in general, text was present. The chosen methodology and data pool is, therefore, appropriate within the conceivable limits of this research project.

This content analysis method will produce results showing text compatibility, exposing how much of the same terminology and processes are involved in the different privacy bylaws. It will also show how widely and comprehensively the topics are covered. Lastly, this method will expose other relevant aspects of user privacy that are not necessarily incorporated with GDPR. The software is able to run an independent analysis assessing for common themes that have not been defined in its system by the researcher. This will expose if there is anything shared amongst these technologies regarding data protection that is not covered in GDPR. The analysis will first cover how the different principles of Article 5 are present and their context within these privacy laws. These seven principles are lawful, fair and transparent processing, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security) and accountability. Secondly, the analysis will compare the technologies to one another to identify similarities and differences among them. Lastly, the

---

<sup>38</sup> Bateni, Nastaran & Kaur, Jasmin & Dara, Rozita & Song, Fei. (2022). Content Analysis of Privacy Policies Before and After GDPR. 1-9. 10.1109/PST55820.2022.9851983.

<sup>39</sup> V. Ayala-Rivera and L. Pasquale, "The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements," *2018 IEEE 26th International Requirements Engineering Conference (RE)*, Banff, AB, Canada, 2018, pp. 136-146, doi: 10.1109/RE.2018.00023.

<sup>40</sup> Bateni, Nastaran & Kaur, Jasmin & Dara, Rozita & Song, Fei. (2022). Content Analysis of Privacy Policies Before and After GDPR. 1-9. 10.1109/PST55820.2022.9851983.

other themes and possible data protection measures that came up that are not mentioned in Article 5 will be outlined and explained in their context.

The advantages of using this method are the effectiveness of achieving frequency analysis and the presence of specified text in the content. It is easily replicable and, therefore, also easily verifiable. The limitations, on the other hand, are that some of the terminology used in the content used for analysis can and does differ from the terminology in GDPR. Despite extensive coding and aiming to incorporate similar terminology, there are limitations in the scope of relevant factors that were not involved in the analysis. Another issue is how much context is lost in the analysis<sup>41</sup>, but this study did not simply pull the relevant terminology but went over each coded element and placed it in the context it was originally written.

It is relevant for the improved understanding of the PETs in question to outline what each technology is and what their intended purpose is. The PETs involved in the analysis include MyData, SOLID, LifeID, SOVRIN, Signal, Jitsi, MySudo, OnionShare and OpenMined. MyData is an approach to data management that understands the need for data by various bodies but prioritises technical guidelines for going about it lawfully.<sup>42</sup> SOLID is a data storage platform placing data in decentralised pods that the user can grant or ban access to.<sup>43</sup> LifeID is a privacy-focused identity platform on blockchain.<sup>44</sup> SOVRIN is an identity system that provides users with “self-sovereign identity on the internet.”<sup>45</sup> Signal is an encrypted messaging platform that is in use around the globe and notably by the European Commission.<sup>46</sup> Jitsi is an open-source video conference programme.<sup>47</sup> MySudo is an app that allows you to securely go about navigating digital interactions by using your Sudo profile rather than personal data and information.<sup>48</sup> Onionshare is an open-source tool that allows access to their Tor network, which facilitates the protected sharing of files, chatting and other interactions.<sup>49</sup> OpenMined is an open-source software that enables users to ask questions that involve other people's data without having access to that data.<sup>50</sup>

Content analysis will allow this study to pursue the research objective of the reflection of GDPR in PETs. What will follow is the analysis of the presence of the principles from Article 5 and other data protection measures beyond just those seven in the various PETs mentioned above. This will increase the understanding about PETs and GDPR compliance within Europe,

---

<sup>41</sup> Stemler, Steve (2001) "An overview of content analysis," *Practical Assessment, Research, and Evaluation*: Vol. 7, Article 17. DOI: <https://doi.org/10.7275/z6fm-2e34>

<sup>42</sup> *About*. MyData. (n.d.). Retrieved from: <https://www.mydata.org/about/>

<sup>43</sup> *Solid*. About Solid · Solid. (n.d.). Retrieved from: <https://solidproject.org/about>

<sup>44</sup> *Lifeid*. Tracxn. (n.d.). Retrieved from: [https://tracxn.com/d/companies/lifeid/\\_jk4Y1opUdH\\_2qhBLufGiQQwVXgeywt-97gJ5qcoHh6w](https://tracxn.com/d/companies/lifeid/_jk4Y1opUdH_2qhBLufGiQQwVXgeywt-97gJ5qcoHh6w)

<sup>45</sup> *Home*. Sovrin. (2023, February 1). Retrieved from: <https://sovrin.org/>

<sup>46</sup> Dussutour, C. (2020, March 12). *Signal Messaging Service*. Joinup. Retrieved from: <https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/signal-messaging-service>

<sup>47</sup> *8x8 privacy notice*. 8x8. (n.d.). Retrieved from: <https://www.8x8.com/terms-and-conditions/privacy-policy>

<sup>48</sup> *Home*. MySudo. (2022, May 4). Retrieved from: <https://mysudo.com/>

<sup>49</sup> Sorrentino, G. (n.d.). *OnionShare*. OnionShare. Retrieved from: <https://onionshare.org/>

<sup>50</sup> OpenMined. (n.d.). Retrieved from: <https://www.openmined.org/>

and allow us to make connections on what this means for the EU stating other technologies need to abide by GDPR.

## Analysis

In theory, if the seven principles of GDPR are embedded into the design of the technologies, then a high level of compliance is achieved and data should be adequately protected. This is because Article 5 touches upon so many stages of the data/information lifecycle.<sup>51</sup> The analysis will be divided along the different principles of GDPR (article 5) and a section to consider other elements that play a role in privacy by design. The hypothesis to be tested is that Privacy-enhancing technologies (PETs) reflect the principles of the General Data Protection Regulation (GDPR), and as a result of the AI Act's requirements, AI systems are expected to begin to imitate PETs. The analysis will be divided along the seven principles of GDPR (article 5), which are: lawful, fair and transparent processing, the purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security) and accountability.<sup>5253</sup> The analysis will reflect to what extent these principles were present in the privacy bylaws, privacy policies and codes of conduct/ service. This will be followed by comparing the frequency and addition of any other relevant article content mentioned.

### *Lawful, fair and transparent*

The first principle specifies that the processing of personal data needs to abide by the laws in place, be fair in the sense of non-discrimination and other factors, and be transparent so the subject is aware of their data being processed. MyData abides by this principle by prefacing that their data collection methods, processing of data and sharing of it, are all lawful. Because their overall structure resembles GDPR, the law they are referring to is this data protection regulation. Transparency and fairness also come up in MyData's principles. They push for transparency in their conduct, having open publications of meetings, and aim to keep processes and all matters related to data open so that users are genuinely informed. Fairness is pushed for in their principle of respect, where measures are taken to mitigate disagreements and ban discriminatory behaviour in their codes of conduct. LifeID SSI does not incorporate the concept of fairness and lawfulness in the rights assigned to users. However, transparency comes up on multiple occasions, such as transparent processes on the platform and transparency in the codes of conduct by the platform. The algorithm is also said to be transparent by being open source. Therefore, mechanisms are in place to ensure a transparent understanding of the technology. Signal outlines the lawfulness of its platform emerges through maintaining that conduct abides

---

<sup>51</sup> Report2018-02-14T09:26:00+00:00, P. (2018, February 14). *GDPR and the information lifecycle*. GRC World Forums. Retrieved from: <https://www.grcworldforums.com/knowledge/gdpr-and-the-information-lifecycle/22.article>

<sup>52</sup> *Art. 5 GDPR – principles relating to processing of personal data*. General Data Protection Regulation (GDPR). (2021a, October 22). Retrieved from: <https://gdpr-info.eu/art-5-gdpr/>

<sup>53</sup>*The principles*. ICO. (n.d.). Retrieved from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/#:~:text=Lawfulness%2C%20fairness%20and%20transparency,Accuracy>

by national laws and also explicitly mentions that if legal bodies request information, they are legally bound to disclose what they have. Additionally, Signal includes a clause that states they will respect the rights that the law has expressed. Transparency and fairness are absent from this technology's codes of conduct and privacy bylaws. SOLID includes the concept of fairness in the treatment of users by the codes of conduct committee, whom investigate behaviour on SOLID. In OpenMined, fairness comes up similarly to SOLID. Sovrin, on the other hand, does not process personal data, so aspects of processing do not apply.

### *Purpose limitation*

The Purpose limitation article states that purposes for data collection and data usage need to be explicitly stated and reasonable. MyData outlines the purposes for their data collection. So does Signal, and there it is detailed that the purposes for data collection, usage and sharing are defined for the sake of an informed user. Jitsi explains that the purposes for which data is collected are: “providing, managing, deploying, enhancing, or improving our services”. MySudo details the processing and purpose of collecting and using data.

### *Data minimisation*

The Data minimisation principle means that only the minimum required data is collected. Within MyData, data minimisation is mentioned regarding data being stored for only the minimum required time. LifeID SSI also respects this principle in all platform aspects, claiming that only the necessary data is collected and used. Signal upholds data minimisation by simply stating that only the necessary amount of data is collected. SOVRIN claims data minimisation processes are in place when storing personal data. Jitsi claims to achieve data minimisation by explaining that only the most minimal amount of data is stored about a user to create and launch a meeting, like name and telephone number (to send activation code). MySudo shortly mentions this principle when stating that only the minimum required data is utilised for the platform to work.

### *Accuracy*

Accuracy alludes to the fact that data is correct and kept timely if necessary, with actions in place to correct if data is found to be incorrect. Within MyData's policies, accuracy comes up when options are presented for users to change the data about them if it is inaccurate. Signal is similar to many other technologies and platforms, as there is no mention of whether data is accurate on the platform. In Signal's case, it is a messaging service. Similarly, they outline they cannot be held accountable for what is shared on the app. This is inferred from the lack of accountability.

### *Storage limitation*

Storage limitation covers that storing of data takes place only under a defined and minimum required period of time. MyData explicitly states that they store their data mainly in Europe

but outlines that where necessary, they maintain the right to access data from outside the borders. LifeID SSI include statements that provide users with the ability to decide on what they wish to share with third parties, which also means they will know what data is held by them. However, they also state that LifeID SSI maintains the right to retain information and says that this is positive due to not having to rely on outsiders, but importantly they fail to quantify the amount of time or under what circumstances data is held for a defined period of time. Regarding data storage, Signal does not store any personal information that is deemed “sensitive”. All data about transitions on the app are stored on the devices using it and not in their servers. They only hold technical data, such as authentication tokens. Onionshare has practically achieved the concept of storage limitation, as data generated on the platform does not travel to a server. This is because in all cases, including if a user starts a conversation, that data will be stored on the users device, so the concept of storage limitation is achieved. Jitsi covers storage minimisation by expanding on how data is stored for quality assurance purposes but once the video or meeting is downloaded onto the device, record of it leaves the programme. Similarly, the chat history is stored during the call, but once it has ended will be deleted. MySudo touches upon storage but clarifies that data is stored outside of European borders, which contradicts with GDPR.

### *Integrity and confidentiality*

Integrity and confidentiality (security) require that data is protected with a certain level of lawful and preventative measures to safeguard against harm. MyData maintains that they take measures to enhance security and protect their data. But they do mention that they do not take responsibility for what may happen on their users end, being that of the device accessing the information and their data infrastructure. This implies there are no strict security measures in place that can mitigate if imposter devices try to dive into the system. Regarding security, LifeID SSI emphasises confidentiality in their communication with users and in what and how data is stored, maintaining that this is only done after obtaining consent. Signal does not take a stance on integrity, just states that others must act with integrity or risk being limited in their access to the app. SOLID includes a level of confidentiality that exists with interactions with the employees of SOLID. SOVRIN incorporates confidentiality when it states that there are agreements with certain users of a layer of its technology regarding confidentiality and privacy. SOVRIN maintains discoverable data has been labelled as having no value, so what can be seen cannot be traced back to users. OnionShare uses anonymity to achieve confidentiality. Onionshare also uses another privacy-enhancing technology called encryption on the platform to achieve end-to-end security, as data cannot be accessed outside of the interaction, strengthening the concept of security. Jitsi has organisational measures in place to protect security and confidentiality. Jitsi also utilises encryption for sensitive data. MySudo is the first of the technologies to detail “integrity” in their privacy policy, but it is in the context that the information used by the platform guarantees its own “integrity”.

### *Accountability*

Accountability comes in the form of the technology provider holding themselves accountable for abiding by data protection. MyData outlines that they hold themselves accountable for any outcomes that arise from their agreements, even if these are negative. On the other hand, within SOVRIN, accountability is not as easily achieved due to the decentralised network structure resulting in data protection supervisors having a difficult time differentiating between who is the data controller, data users and processors.

### *Other rights*

Embedded within these principles are requirements such as user rights and control and consent, which are ways to achieve enhanced data protection. Therefore it is relevant to also expand on these and mention if and how they are present in the technologies. MyData also outlines the rights that data users have where familiar terms from GDPR are used, such as: “the right to rectification”, “the right of access”, and “the right to erasure”. Within LifeID SSI consent is emphasised in all the technologies. Consent to using the technologies, consent to data being collected and consent to be processed and information shared.

### *Comparison of the technologies*

Concerning the first principle, MyData, Life ID SSI and Signal all demonstrate following the principle of lawfulness in their processing and collection of data, and all also touch on being open and transparent in some form. MyData and LifeID SSI also touch on fairness which is not present in Signal’s documents. The second principle about the purpose sees MyData, Signal, Jitsi and MySudo state their purposes for data collection. The third about data minimisation sees the most compliance amongst the technologies alongside taking action to ensure a high level of security with the principle of integrity and confidentiality. Additional technological measures, such as encryption, get mentioned in the section for additional security. The storage limitation principle comes with a high level of compliance with MyData, Signal, Onionshare and Jitsi. Some of these technologies do not store any of their user data on servers but leave that fully in the hands of users and their own devices. For this reason, this principle sees the highest level of compliance regarding the degree of compliance, as some technologies exceed expectations. User rights and controls are incorporated by MyData, LifeID SSI and Signal.

All of these technologies establish what data is collected, stored and processed and what role/position the user has in the technology. Almost all provide options for users to act on their data. The concept of consent also comes up in each and every technology. It takes varying forms, being included in consent for data collection, processing, and sharing but also consent to use the technology and consent to be interacted with etc. When it comes to outlining the purposes for which data was collected, whether it be for advertising or identification, the data showed that the most common purpose was for verifying.

It is relevant to touch upon how the different types of technologies that were analysed vary in their ability to implement GDPR principles considering their purposes. MyData is the only analysed technology concerned with the accuracy of the data and correcting if it's inaccurate,



but also on the principle of accountability. This highlights how the policies and principles MyData abides by strongly resemble that of the GDPR. SOLID is a data storage technology, so aspects such as accuracy, accountability, data minimization etc., are not so directly related. Within SOLID the protocols and privacy bylaws are impeded in code which does not translate into the content analysis well. Relevant terminology is mostly absent, so identifying which aspects of GDPR might be involved in the design is not possible. This has created a technical jargon with non-experts of the technology having a hard time understanding what is being communicated, and in GDPR terms, this is an issue of transparency. The Sovrin governance framework was actually created following the privacy-by-design approach as outlined in their privacy policy. This showed some fundamental differences with the GDPR principles in line with what the research predicted. Despite some existing tensions, another EU body is keen to see what can come about with these decentralised governance forms that provide users control over their own data, with the European Parliament lessening restrictions regarding innovation in this sector.<sup>54</sup>

### *Summary of analysis*

Though the findings show varying levels of GDPR compliance and incorporation of the principles in the privacy bylaws, privacy policies and codes of conduct, considering what is plausible for the technologies and platforms, overall, the level of adherence to GDPR principles is high. There remains room to improve compliance in areas such as accountability, accuracy and integrity. The data suggest that privacy-enhancing technologies emulate most of the principles of GDPR, such as data and storage minimisation, but all heavily ignore other principles, such as transparency and accuracy. This is because the most frequent terminology present was storage-related concepts, and the least frequent was integrity and transparency. Transparency emerged mainly in transparent processes such as the enforcement of policies by the technology creators but less or even minimally regarding the technology itself.

The evidence suggests that the hypothesis is correct. Taking into account the various technologies and their design (messaging platform, decentralised network etc.) a large majority of the concepts that can be incorporated into the design of these technologies are present. This means that the current discourse surrounding the AI Act is expecting that AI system design begins to look like that of these PETs. The purpose of involving a variety of different kinds of privacy-enhancing technologies was to show that taking into consideration that in some systems some principles are not relevant, there is still room to be compliant with GDPR where principles do apply to conduct.

---

<sup>54</sup>Council of the European Union. (2020). *Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age*. EUR. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0720>

## Discussion

The analysis showed that, where applicable, PETs do a decent job at incorporating principles of Article 5 in their privacy policies. Though there is room for improvement, PETs deserve credit for taking so many of the aspects into consideration. There is also the chance that for those that lacked some principles, the analysis had a hard time realising this if different terminology was used. Similarly, these technologies vary in their purpose therefore, it is difficult to compare such different technologies when not all principles apply to each one. However, with all this considered, GDPR is well reflected in PETs. This study understands that the different principles of GDPR differ in their ease of compliance and their technical requirements to be achieved. But the results do imply a hint at higher GDPR compliance if the principles are implemented in the design of the technology.

These findings have implications outside of this research. Firstly if this is what adequately complying with GDPR looks like, then existing technologies are encouraged to adapt their privacy policies and design to resemble that of the various articles of GDPR, which PETs can be an example to draw from. This also means that AI systems should consider emulating these principles like privacy-enhancing technologies. This is not to say that AI systems should become PETs, that is an unrealistic expectation that this research does not encourage. However, AI systems can learn a lot about how to implement GDPR into their design. More importantly, this hints at a suggestion that this paper would like to discuss. AI systems should utilize PETs that clearly comply to a large extent with GDPR already and can be further improved, to enhance their own systems GDPR compliance in the future. PETs can be the tool used to extract the required aspects of data by AI systems without the unnecessary personal details that impact data protection.<sup>55</sup>

This analysis exposes that transparency is an issue for privacy-enhancing systems, and literature shows that it also poses a challenge for AI systems. The current discourse surrounding transparency has changed from openness to explainability.<sup>56</sup> Transparency, according to the GDPR principles, is achieved by these technologies that make an effort to communicate, inform and explain the processing criteria to their users. Many of the technologies also prioritise obtaining consent from users and explicitly state clear and concise communication to maintain an informed user. Transparency, according to the AI Act is regarded as explainability, and this is absent from being explicitly stated in the privacy policies. This is coupled with the lack of accountability in these technologies, no one can be held responsible for explaining the technical specifics that go into the technology. The reason this is extra concerning is combining these systems would lead to further complexity regarding transparency. However studies from this year have found a solution for this that they call structured transparency. This form of transparency in AI and PETs would come at the assistance of PET tools to provide auditing,

---

<sup>55</sup> Dilmegani, C. (2022, December 21). *Top 10 privacy enhancing technologies & use cases in 2023*. AIMultiple. Retrieved from: <https://research.aimultiple.com/privacy-enhancing-technologies/>

<sup>56</sup> BUSUIOC, Madalina, CURTIN, Deirdre, LASMAR ALMADA, Marco Antonio, *Reclaiming transparency : contesting the logics of secrecy within the AI Act*, European law open, 2022, OnlineFirst - <https://hdl.handle.net/1814/75390>

verification of sources and external review / surveillance of the system.<sup>57</sup> So despite PETs adding a layer of complexity, they also provide a moderate solution to one of the major concerns of transparency of AI and PET technology.

The White House in the United States has called for public involvement in researching PETs for their possible benefits in standing between researchers and data. They state this could have broader implications for PETs standing in the intersection between artificial intelligence systems and data. The possibility that AI systems could access data without ever obtaining knowledge of the personal characteristics of said data would be revolutionary. It is already known that a large amount of resources and research will need to be invested into how GDPR principles will be incorporated into AI systems. What if, instead, we invested these resources into expanding and improving our PET systems? This is not to say that PETs are the perfect solution to data protection problems. As they are, PETs require much revision and improvements to mitigate risks associated with discrimination, biases and a false sense of privacy. They also remain incredibly technical so they lack the ability to be implemented into systems without expertise which includes high financial costs.<sup>58</sup>

In regards to data governance, the representation of these principles in PETs shows a successful effect of GDPR as a data governance framework. These technologies take the privacy policies and guidelines into consideration within the design and work to unify approaches to data protection within Europe.

## Conclusion

In summary this analysis of how well GDPR is reflected in PETs found that where relevant, GDPR principles were largely covered. The content analysis of Article 5 found varying results over how comprehensively or narrowly different principles were taken into consideration in the design. These results were expected as the different principles involve differing amounts of effort and some were not applicable to all the different technologies. Nevertheless, this study produced interesting findings that imply that emerging technologies looking to have a strong GDPR compliance rate, should look at the privacy policies of PETs.

Regarding data protection in emerging technologies, I echo what other researchers have said. Direction and instruction are needed to guide AI systems to be GDPR compliant. Too much vagueness and a lack of implementation recommendations make GDPR seem like a problem for AI systems. In reality, the two do not exist in too much tension, so research is encouraged to go further into practical guidelines.

---

<sup>57</sup> Bluemke, E., Collins, T., Garfinkel, B., & Trask, A. (2023). Exploring the Relevance of Data Privacy-Enhancing Technologies for AI Governance Use Cases. *ArXiv*. /abs/2303.08956

<sup>58</sup> Macgillivray, A. (2022, June 28). *Advancing a vision for privacy-enhancing technologies*. The White House. Retrieved from: <https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/>

Regarding PETs, the language used in codes of conduct, privacy bylaws and policies needs to be revised to ensure it is understandable to the reader what they are giving their consent for. Hence technical jargon should be discouraged. It is also advisable to use harmonised terminology derived from legislation to showcase high levels of compliance and incentive other technologies to follow suit. However, in summary of the findings of this study PETs possess a high level of GDPR compliance where it is possible. The technologies vary in their purpose and design and what they use personal data for. Therefore it cannot be expected that these technologies need to abide by each aspect of GDPR if their activities are not concerned with many of the points. But what this study did find is that where these technologies do process, collect or use personal data, this was always conveyed to the user.

And finally, AI systems are strongly encouraged to utilise PETs in their design. Implementing GDPR measures to vast AI systems is a challenge and this task will require much research and resources. But this study proposes a solution to this issue. That solution being that AI systems should instead utilise the increased data protection that PETs offer and incorporate these technologies into their systems. If the reasons are not obvious yet, utilizing PETs that already abide by GDPR to a large extent and can be further improved upon, would strengthen GDPR compliance in AI systems and better protect European citizen's data in the future. Future research should therefore investigate which PETs and where in the design or models of AI they should be situated for maximum productivity and security.

## APPENDIX

Codes in content analysis:

Access	Collect\telephone number	Retention\Data
Access\Access	Collect\Username	Retention\Delete
Access\Account	Consent	Retention\Discard
Access\Accurate	Data aggregation	Retention\Keep
Access\Change	Data aggregation\Aggregation	Retention\Long period
Access\Correct	Data aggregation\Combine	Retention\Remove
Access\Delete	Data aggregation\Multi	Retention\Retain
Access\Edit	Data aggregation\Other	Retention\Retention
Access\Modify	Data aggregation\Similar	Retention\Storage
Access\Preferences	Data aggregation\Source	Retention\Store
Access\Profile	Data Protection	Review and Update
Access\Removal	Do not track	Security
Access\Request	Do not track\Cookies	Security\Access
Access\Section	Do not track\Disable	Security\Compromise
Access\Settings	Do not track\Signal	Security\Encrypt
Access\Update	Do not track\Track	Security\Fraud
Account deletion	Do not track\Track request	Security\Protect
Account deletion\Deletion	Do not track\Track Setting	Security\Restrict
Account deletion\Withdraw	Fairness	Security\Safeguard
Choice	Free	Security\Secure
Choice\Agree	Law and Regulatory	Security\Unauthorised
Choice\Choose	Requirements	Share
Choice\Consent	Personal Data	Share\Advertisor
Choice\Disable	Policy Change	Share\Analytics
Choice\Do not track	Policy Change\Change	Share\Buisnesses
Choice\Opt	Policy Change\Notice	Share\Company
Choice\Option	Policy Change\Policy	Share\Disclose
Choice\Setting	Policy Change\Update	Share\Law or Regulation
Choice\Subscribe	Privacy	Share\Organisations
Choice\Unsubscribe	Privacy Enhancing	Share\Partner
Choice\Wish	Technologies	Share\Provider
Collect	Privacy Enhancing	Share\Safe
Collect\Account	Technologies\Encryption	Share\Security
Collect\Address	Privacy Enhancing	Share\sell
Collect\Age	Technologies\Pseudonymising	Share\Third Party
Collect\collect	Process	Share\Transfer
Collect\contact	Purpose	Transparency
Collect\Credit Card	Purpose\Advertising	User Rights and Control
Collect\Date of birth	Purpose\Fraud	User Rights and
Collect\email	Purpose\Identification	Control\Control
Collect\Health	Purpose\Improve	User Rights and
Collect\identifiable	Purpose\Personalize	Control\Personal information
Collect\IP-address	Purpose\Prevention	User Rights and Control\Right
Collect\Location	Purpose\Purpose	to Access
Collect\Name	Purpose\Use	User Rights and Control\Right
Collect\password	Purpose\Verifying	to Correct
Collect\personal	Retention	User Rights and Control\Right
Collect\postal code	Retention\Backup	to Delete

## BIBLIOGRAPHY

*10 Best Artificial Intelligence Software (AI software reviews in 2023)*. Software Testing Help. (2023, April 28). <https://www.softwaretestinghelp.com/artificial-intelligence-software/>

*6 data lifecycle stages: Data Cycle Management Guide*. Segment. (n.d.). <https://segment.com/blog/data-lifecycle/>

*8x8 privacy notice*. 8x8. (n.d.). <https://www.8x8.com/terms-and-conditions/privacy-policy>

*About. MyData*. (n.d.). <https://www.mydata.org/about/>

*AI Act: A step closer to the first rules on Artificial Intelligence: News: European parliament*. AI Act: a step closer to the first rules on Artificial Intelligence | News | European Parliament. (2023, May 11). <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence>

*Art. 5 GDPR – principles relating to processing of personal data*. General Data Protection Regulation (GDPR). (2021a, October 22). <https://gdpr-info.eu/art-5-gdpr/>

Batani, Nastaran & Kaur, Jasmin & Dara, Rozita & Song, Fei. (2022). Content Analysis of Privacy Policies Before and After GDPR. 1-9. 10.1109/PST55820.2022.9851983.

Bluemke, E., Collins, T., Garfinkel, B., & Trask, A. (2023). Exploring the Relevance of Data Privacy-Enhancing Technologies for AI Governance Use Cases. *ArXiv*. /abs/2303.08956

BUSUIOC, Madalina, CURTIN, Deirdre, LASMAR ALMADA, Marco Antonio, *Reclaiming transparency : contesting the logics of secrecy within the AI Act*, European law open, 2022, OnlineFirst - <https://hdl.handle.net/1814/75390>

Camarillo, A. (2022, March 17). *Artificial Intelligence and privacy by design*. TechGDPR. <https://techgdpr.com/blog/artificial-intelligence-and-privacy-by-design/>

Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection regulation: what it is and what it means, *Information & Communications Technology Law*, 28:1, 65-98, DOI: [10.1080/13600834.2019.1573501](https://doi.org/10.1080/13600834.2019.1573501)

Competition Policy International. (2023, April 11). *Spain requested EU Data Protection Board to discuss OpenAI's chatgpt*. Competition Policy International. <https://www.competitionpolicyinternational.com/spain-requested-eu-data-protection-board-to-discuss-openais-chatgpt/>

Council of Europe. (2019, January 25). *Artificial Intelligence and data protection - RM.COE.INT*. <https://rm.coe.int/prems-192119-gbr-2051-lignes-directrices-sur-l-intelligence-artificiel/1680a4ca4a>

Council of the European Union. (2020). *Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age*. EUR. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0720>

D. Torre, G. Soltana, M. Sabetzadeh, L. C. Briand, Y. Auffinger and P. Goes, "Using Models to Enable Compliance Checking Against the GDPR: An Experience Report," *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS)*, Munich, Germany, 2019, pp. 1-11, doi: 10.1109/MODELS.2019.00-20.

*Data Governance and GDPR: An introduction*. Splunk. (2021, May 1). [https://www.splunk.com/en\\_us/data-insider/data-governance-and-gdpr.html](https://www.splunk.com/en_us/data-insider/data-governance-and-gdpr.html)

Dilmegani, C. (2022, December 21). *Top 10 privacy enhancing technologies & use cases in 2023*. AIMultiple. <https://research.aimultiple.com/privacy-enhancing-technologies/>

Draft online safety bill - joint committee on the Draft Online Safety Bill. (n.d.). <https://publications.parliament.uk/pa/jt5802/jtselect/jtonlinesafety/129/12906.htm>

Dussoutour, C. (2020, March 12). *Signal Messaging Service*. Joinup. <https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/signal-messaging-service>

Espinoza, J. (2021, March 3). *EU must overhaul flagship data protection laws, says a "father" of policy*. Subscribe to read | Financial Times. <https://www.ft.com/content/b0b44dbe-1e40-4624-bdb1-e87bc8016106>

*EU Artificial Intelligence Act*. Center for AI and Digital Policy. (n.d.). <https://www.caidp.org/resources/eu-ai-act/>

EUI. (n.d.). *Use our tools!*. CLAUDETTE. <http://claudette.eui.eu/use-our-tools/index.html>

European Commission et al. (2021). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206>

European Commission. (2019). *Ethics guidelines for trustworthy AI*. Retrieved from <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

European Parliament. (2020, June 25). *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Think tank: European parliament*. Think Tank | European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530)

Goujard, C., & Volpicelli, G. (2023, April 10). *Chatgpt is entering a world of regulatory pain in Europe*. POLITICO. <https://www.politico.eu/article/chatgpt-world-regulatory-pain-eu-privacy-data-protection-gdpr/>

Guardian News and Media. (2023, April 1). *Letter signed by Elon Musk demanding AI research pause sparks controversy*. The Guardian. Retrieved from <https://www.theguardian.com/technology/2023/mar/31/ai-research-pause-elon-musk-chatgpt>

He Li, Lu Yu & Wu He (2019) *The Impact of GDPR on Global Technology Development*, Journal of Global Information Technology Management, 22:1, 1-6, DOI: [10.1080/1097198X.2019.1569186](https://doi.org/10.1080/1097198X.2019.1569186)

Help Net Security. (2019, December 4). *Despite potential fines, GDPR compliance rate remains low*. Help Net Security. <https://www.helpnetsecurity.com/2019/12/04/gdpr-compliance-rate/>


Home. MySudo. (2022, May 4). <https://mysudo.com/>

Home. Sovrin. (2023, February 1). <https://sovrin.org/>

Hoyos Flight, M. (2023, March 6). *Technological vulnerabilities that threaten the European Union's 'Open Strategic Autonomy' and the EU's response*. Science Media Hub. other. Retrieved May 13, 2023,.

Jha, P. (2023, March 31). *Elon Musk-led petition to halt AI development divides Tech Community*. Cointelegraph. <https://cointelegraph.com/news/elon-musk-led-petition-to-halt-ai-development-divides-tech-community>

Kayali, L., & Goujard, C. (2023, April 13). *Chatgpt could come back to Italy by end of April*. POLITICO. <https://www.politico.eu/article/chatgpt-italy-lift-ban-garante-privacy-gdpr-openai/#:~:text=In%20late%20March%2C%20ChatGPT%20was,them%20from%20accessing%20the%20chatbot.>

- Koerner, K. (2022a, January 20). *Privacy and responsible ai*. Privacy and responsible AI. <https://iapp.org/news/a/privacy-and-responsible-ai/>
- Koerner, K. (2022b, January 20). *Privacy and responsible ai*. Privacy and responsible AI. <https://iapp.org/news/a/privacy-and-responsible-ai/>
- Leveueur, F. (2023, April 22). *How data governance helps achieve regulatory compliance*. Data Sleek. <https://data-sleek.com/blog/data-governance-best-practices/>
- Lifeid. Tracxn. (n.d.). [https://tracxn.com/d/companies/lifeid/\\_jk4Y1opUdH\\_2qhBLufGiQQwVXgeywt-97gJ5qcoHh6w](https://tracxn.com/d/companies/lifeid/_jk4Y1opUdH_2qhBLufGiQQwVXgeywt-97gJ5qcoHh6w)
- Macgillivray, A. (2022, June 28). *Advancing a vision for privacy-enhancing technologies*. The White House. <https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/>
- Niet, I., van Est, R., & Veraart, F. (2021). Governing AI in Electricity Systems: Reflections on the EU Artificial Intelligence Bill. *Frontiers in Artificial Intelligence*, 4. <https://doi.org/10.3389/frai.2021.690237>
- OpenMined. (n.d.). <https://www.openmined.org/>
- Paul, K. (2023, April 1). *Letter signed by Elon Musk demanding AI research pause sparks controversy*. The Guardian. <https://www.theguardian.com/technology/2023/mar/31/ai-research-pause-elon-musk-chatgpt>
- Privacy by design*. General Data Protection Regulation (GDPR). (2021b, October 22). <https://gdpr-info.eu/issues/privacy-by-design/>
- Renda et al. (2021), Study in support of the European Commission's impact assessment of the Ai Act <https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1>
- Renieris, E., Zanfiri-Fortuna, D. G., Bartoletti, I., Marda, V., & Peppin, A. (2021, April 29). *Why pets (privacy-enhancing technologies) may not always be our friends*. Ada Lovelace Institute. <https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/>
- Report2018-02-14T09:26:00+00:00, P. (2018, February 14). *GDPR and the information lifecycle*. GRC World Forums. <https://www.grcworldforums.com/knowledge/gdpr-and-the-information-lifecycle/22.article>
- Solid. About Solid · Solid. (n.d.). <https://solidproject.org/about>
- Sorrentino, G. (n.d.). *OnionShare*.  OnionShare. <https://onionshare.org/>
- Stemler, Steve (2001) "An overview of content analysis," *Practical Assessment, Research, and Evaluation*: Vol. 7, Article 17. DOI: <https://doi.org/10.7275/z6fm-2e34>
- The principles*. ICO. (n.d.). <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/#:~:text=Lawfulness%2C%20fairness%20and%20transparency,Accuracy>
- V. Ayala-Rivera and L. Pasquale, "The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements," *2018 IEEE 26th International Requirements Engineering Conference (RE)*, Banff, AB, Canada, 2018, pp. 136-146, doi: 10.1109/RE.2018.00023.
- von Gravrock, E. (n.d.). *Artificial Intelligence Design must prioritize data privacy*. World Economic Forum. <https://www.weforum.org/agenda/2022/03/designing-artificial-intelligence-for-privacy/>



Wallace, N. (2018, May 25). *Europe is about to lose the global ai race - thanks to GDPR*. [www.euractiv.com](http://www.euractiv.com).  
<https://www.euractiv.com/section/data-protection/opinion/europe-is-about-to-lose-the-global-ai-race-thanks-to-gdpr/>