Committee: Council of the European Union (EU)

Topic: Re-visiting Data Protection Laws in the Context of Artificial Intelligence

Student Officer: Fotini Katoglou

Position: Deputy President

PERSONAL INTRODUCTION

Dear Delegates,

Welcome to the 7th session of the Deutsche Schule Thessaloniki Model United Nations. I am Fotini Katoglou, an 11th-grade German School of Thessaloniki student. This year, I have the pleasure to serve as the Deputy President of the Council of the European Union. Congratulations to each of you for being selected to participate in this esteemed committee!

MUN is a great means of connecting with individuals from diverse backgrounds worldwide and, above all, engaging in discussions on topics of global concern. It's an environment where we can come together to drive positive change in our world. I've always believed that MUN allows us to bridge cultural divides and collectively tackle the challenges shaping our future.

During the three-day session, we will tackle the issue of "**Re-visiting Data Protection Laws in the Context of Artificial Intelligence**." This topic is critical in today's digital era as technological developments find themselves against privacy concerns. DSTMUN promises an unmatched debating experience; rest assured!

Please note that, although this guide sets the stage, digging deeper through your research is the key. Familiarize yourselves with the EU EU Rules of Procedure manual beforehand to ensure that our discussions and procedures and procedures are smooth and clear.

Should you have any questions or concerns or need any kind of further clarification, do not hesitate to contact me at katoflouf@gmail.com.

I am truly looking forward to meeting you all!

Kind regards,

Fotini Katoglou

TOPIC INTRODUCTION

Artificial intelligence(AI) is increasingly becoming a part of our daily lives, altering interactions faster than ever before. AI by enabling tailored medicine, optimizing energy consumption in smart cities, and even creating new materials to address environmental issues, AI has the power to change our planet. Yet, as technology advances, so does the amount of information collected and shared online, increasing privacy concerns and reducing people's trust in existing data protection regulations.

In the digital age, personal data have become an extremely valuable asset that enables companies, governments, and organizations to make intelligent decisions and gain insights. However, this wealth of information often involves sensitive information that individuals may not wish to share or to be accessed, to be accessed, showing that privacy is a major concern. Privacy, a basic human right, ensures that people have control over their personal information and how it is used, protecting it against identity theft, fraud, and unwarranted surveillance.

Protecting personal data from AI is essential to prevent manipulation and discrimination. To avoid biased conclusions, AI systems using personal data must prioritize transparency and accountability. The EU recognized these issues and proposed the AI Act to manage AI systems under its control. The act was implemented in August 2024 and it classifies AI systems according to their level of risk—from unacceptable to minimal—and sets standards and requirements for suppliers, users, and importers.

Across Europe, member states are taking different approaches to controlling AI according to their own needs and interests. The California Consumer Privacy Act in the US and the General Data Protection Regulation in Europe are two of the most important data protection regulations. They may seem strong in theory, but these laws cannot keep pace with the ever-evolving and complex world of AI. “The EU’s GDPR and California’s CCPA are just the beginning. Neither is perfect and both will evolve, but privacy laws will expand.”[1], says a technology analyst.

However, despite these laws, data breaches continue to occur. For instance, in January 2023, a database containing information about over 200 million Twitter users was leaked online following the exploitation of an API vulnerability[2]. This breach exposed email addresses, names, and usernames. Such incidents show that it is urgent to protect against evolving threats.

[1] https://www.forbes.com/sites/davidteich/2020/08/10/artificial-intelligence-and-data-privacy--turning-a-risk-into-a-benefit/

[2] An API vulnerability is a security flaw in an Application Programming Interface (API), which is a tool that lets different software programs talk to each other and share information. When an API has a weakness, attackers can exploit it to access or misuse data they shouldn’t be able to reach.

As AI moves forward, clear ethical guidelines to protect privacy are crucial. Industry leaders and international organizations stress the need for AI systems to prioritize transparency, accountability, and fairness to address the privacy paradox. The Council of the EU must act urgently and decisively.

DEFINITION OF KEY TERMS

Artificial Intelligence (AI)

Computer programs can carry out tasks that would normally require human intelligence, like problem-solving, learning from experience, and solving complicated problems. AI systems can learn from existing data, form decisions, and perform tasks autonomously; there's no clear instruction at each stage. One major challenge: AI makes decisions that are difficult to understand, also known as the "black box" problem. This occurs because AI algorithms are highly complex and involve intricate layers of data processing that are not easily interpretable by humans. Legally and ethically, it raises questions of accountability and fairness because a lack of transparency can lead to biased or unjust outcomes that are hard to detect or correct.

General Data Protection Regulation (GDPR)

"The GDPR is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in and outside of the EU."[3]

Data protection authorities (DPAs)

"DPAs are independent public authorities that monitor and supervise, through investigative and corrective powers, the application of the data protection law."[4]

European Data Protection Board (EDPB)

The EDPB is an independent body that ensures the consistent application of the GDPR across the EU. It promotes cooperation between data protection authorities from all EU countries and includes representatives from national data protection authorities and the European Data Protection Supervisor (EDPS). Besides overseeing GDPR enforcement, the EDPB also manages tasks under the Police and Criminal Justice Data Protection Directive and other EU legislative instruments.

[3] "General Data Protection Regulation (GDPR): Meaning and Rules.", Investopedia, https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp.

[4] "What are Data Protection Authorities (DPAs) and how do I contact them?", European Commission, https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/redress/what-are-data-protection-authorities-dpas-and-how-do-i-contact-them_en

Privacy paradox

The contradiction is that people want to keep their personal information private but share it online for the convenience or benefits of digital services.

Privacy

A fundamental human right that grants individuals control over their personal information, safeguarding them from unauthorized access, use, or disclosure.

Ethical guidelines

“Ethical guidelines or codes are used by groups and organizations to define what actions are morally right and wrong. The guidelines are used by group members as a code with which to perform their duties.”[5]

BACKGROUND INFORMATION

What is AI?

Even though this is a concept we’ve been hearing about more recently, AI is not something new. It started in the 1950s with the mathematician and computer scientist Alan Turing. He speculated about the possibility of machines that could "think." So, he created the Turing test, which a computer would pass if it could act just like a human. AI became more popular again recently due to the internet, powerful and affordable cloud computing, and the vast amount of data available for analysis. Inspired by the human brain’s structure, these AI systems process great amounts of data, recognizing patterns and making decisions based on the information they receive. When AI receives data, it learns and accumulates it, improving its accumulates it, improving its performance. Corporations, Corporations, like Amazon and Alphabet (Alphabet (Google)), with data from billions of users, need ways to analyze all this information, and AI is the solution., and AI is the solution.

The General Data Protection Regulation (GDPR)

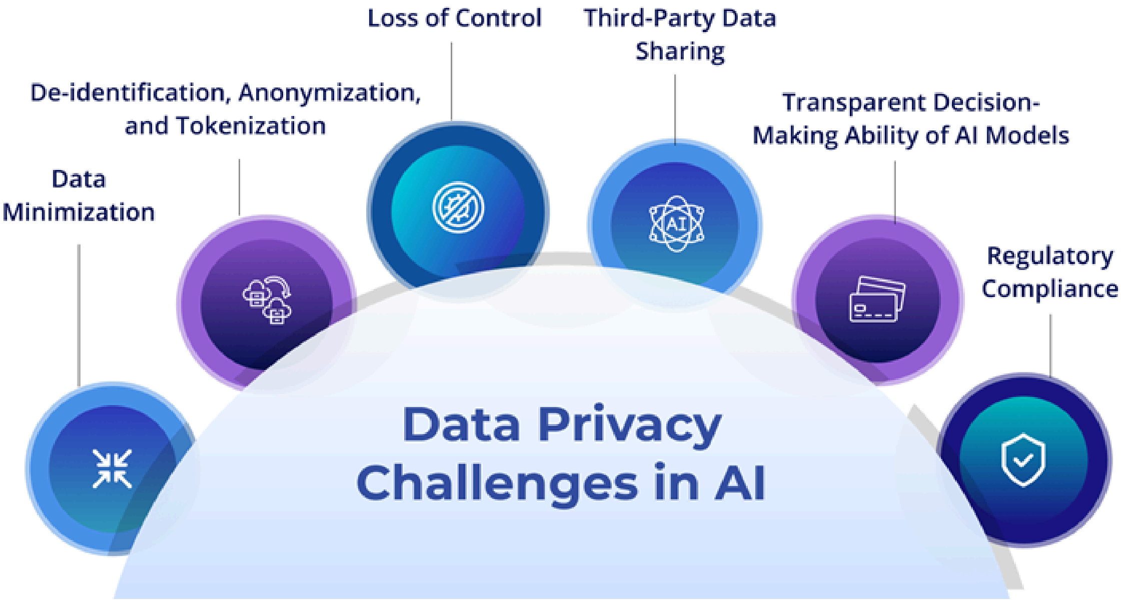
A Quick Overview

For years, the EU's data protection laws have set the bar high around the world. Given how technology has evolved in the past 25 years, regulations need updating. The GDPR, which entered into force on May 24, 2016, replaced the outdated 1995 Data Protection Directive from the early internet era. The GDPR set a new global standard when it applied on May 25, 2018. It aims to give people more control over their personal information and sets strict rules for companies that handle this data. The GDPR imposes

[5] “Ethical Guidelines”, AlleyDog.com, https://www.alleydog.com/glossary/definition.php?term=Ethical+Guidelines

strict rules on personal data processing, including automated decision-making and profiling (Article 22) and sensitive data processing (Article 9). AI applications are not exempt and must adhere to these criteria. Negotiated for over four years, it stresses data minimization and purpose limitation, meaning that AI systems should use necessary data for specific, legitimate purposes. First, if you process the personal data of EU citizens, or you offer goods or services to them, then the GDPR applies to you even if you're not in the EU. Second, the fines for non-compliance are very high. The regulation demands individuals' explicit consent for data processing and grants individuals rights to access, correct, and remove their data. Additionally, it requires clear communication about data processing processes and holds corporations responsible for protecting personal information.

Figure 1: Data privacy challenges organizations face in the context of AI:[6]


Loss of Control
Third-Party Data Sharing
De-identification, Anonymization, and Tokenization
Transparent Decision-Making Ability of AI Models
Data Minimization
Regulatory Compliance
Data Privacy Challenges in AI

GDPR's gaps; AI concerns and missed protections

In the context of AI, the GDPR urgently needs to be revised to address new technologies. Its current framework has limitations, specifically because it is not clear how AI collects, stores, and uses personal data. This is why it can be difficult for individuals to fully understand and agree on how their data will be used.

The GDPR's "right to be forgotten" is problematic with AI; once personal data is used to train AI models, removing it becomes nearly impossible, which undermines the right to data deletion. The GDPR applies to personal data, but does it address scenarios where non-personal data is leveraged? Data breaches also pose a large threat; AI systems can

[6] Rawate, Ankita. "Overcome Data Privacy Challenges." Fortanix, 7 June 2023, https://www.fortanix.com/blog/confidential-computing-ai-to-overcome-data-privacy-challenges

become victims of cyberattacks, opening up the possibility for personal data to be misused. “The GDPR and AI are neither friends nor foes. The GDPR does in some cases restrict—or at least complicate—the processing of personal data in an AI context.”

The GDPR has surely established strong principles to protect data, but it falls short of addressing the challenges posed by AI. They often act as "black boxes,” and no one really knows how data is processed. No transparency can mean biased decision-making and unauthorized use of data. Last but not least, many new ways in which AI handles personal information are not covered explicitly by the current provisions of the GDPR.

Article 22 GDPR: Evaluation of Limitations

Article 22 of the GDPR protects against decisions made solely by automated systems with significant effects. However, its vague wording means it doesn’t cover cases where even a small amount of human involvement is present. The "right to explanation" is also limited; GDPR does not demand detailed explanations of "how" and "why" an automated decision was made. For example, if a loan application is rejected by an automated system, the company only needs to provide general factors considered, not specifics. This lack of detail fails to address algorithmic biases and ethical issues. While other GDPR rules aim for fairness and transparency, they may not fully address AI’s complexities. Better data quality, bias control, clearer explanations, and human reviews are needed for fair and ethical AI.

Data privacy laws

AI liability directive (AILD)

In September 2022, the European Commission implemented a directive on the adaptation of non-contractual civil liability to AI. The goal is to ensure that people harmed by AI systems receive the same level of protection as those harmed by other technologies in the EU. It will also create a "presumption of causality" that will make things easier for victims to prove that an AI system caused them damage. National courts can also demand the disclosure of evidence from high-risk AI systems suspected of causing harm. Nonetheless, stakeholders and academics are questioning whether this proposed liability regime is adequate and effective, how it aligns with the AI Act, its potential impact on innovation, and how it interacts with EU and national laws.

The EU Artificial Intelligence Act (AI Act)

On August 1, 2024, the AI Act became law, marking the world's first comprehensive AI regulation. This new law aims to ensure that AI developed and used in the EU is trustworthy and protects people's rights. It categorizes AI systems by risk: minimal risk systems have no obligations; specific transparency risk systems, like chatbots, must disclose machine interaction and label deep fakes; high-risk systems like those used in recruitment must meet strict requirements; and unacceptable risk systems, like those manipulating behavior or enabling social scoring, are banned. General-purpose AI models that perform many tasks must be transparent and address systemic risks that affect entire systems or industries. By August 2, 2025, Member States must appoint national authorities to enforce the Act, with the Commission's AI Office as the main implementation body. Three advisory bodies will assist: the European Artificial Intelligence Board, a scientific panel, and an advisory forum. Non-compliant companies face fines of up to 7% of their global turnover. Most rules apply as of August 2, 2026, but bans on unacceptable AI systems and rules for general-purpose AI will take effect six months after they enter into force. The Commission is working on guidelines and standards and inviting stakeholder input. The Act builds on the GDPR, adding AI-specific rules for safety, transparency, and, of course, accountability.

Why are the EU AI Act, AI Liability Directive, and GDPR not fully aligned?

The AI Act, AILD, and GDPR each cover different areas, which can lead to mismatches and gaps. The AI Act focuses on safety and transparency for AI systems in the EU. The GDPR, on the other hand, is about protecting personal data and preventing privacy violations. The AILD adds to these laws by dealing with who’s responsible for damages caused by AI systems. The AI Act applies to all global AI providers and users, while the GDPR targets controllers and processors handling personal data in the EU. This overlap in roles between the GDPR and the AI Act can create confusion about who’s responsible for what. The AI Act requires human oversight of AI but lacks specific instructions on how this should be done. Meanwhile, the GDPR insists on “meaningful human involvement” in automated decisions. Both laws require assessments: the AI Act mandates conformity assessments for safety, while the GDPR requires Data Protection Impact Assessments (DPIAs) to manage risks to personal data. High-risk AI systems frequently process personal data. AILD fixes liability rules on the harm caused by AI, which is independent of the GDPR’s data protection orientation and the AI Act’s safety and transparency requirements. Misalignment across these regulations takes place because they serve different purposes, which may lead to misunderstandings among citizens and corporations over their compliance duties.

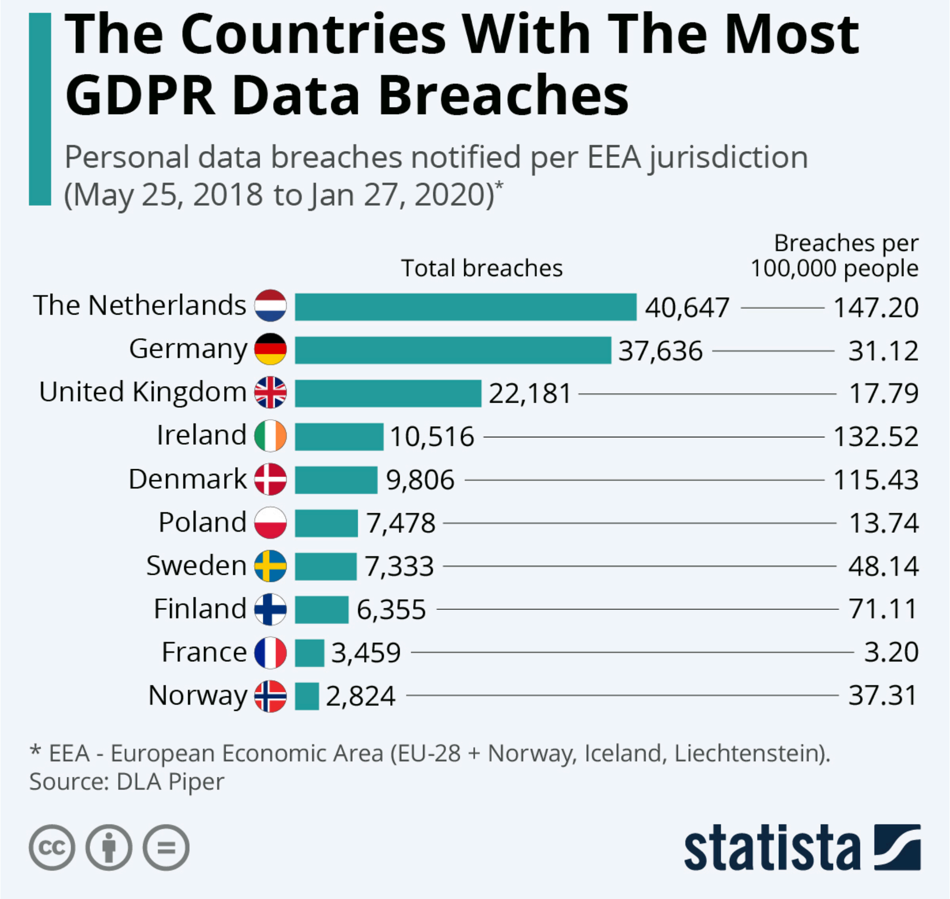


Figure 2: Top countries with GDPR breaches[7]

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

Italy

The Italian Data Protection Authority banned ChatGPT in early April 2023 due to privacy concerns. The Italian watchdog found that the app failed to comply with GDPR and suffered a data breach, arguing that there was no legal basis for mass data collection and storage used to train algorithms. The lack of age verification exposed minors to answers unsuitable for their level of development and awareness. A few weeks later, OpenAI addressed these issues and released a privacy policy, but the Italian regulator continued to call for greater transparency and stricter compliance with data privacy regulations. Unfortunately, new privacy violations were reported in early 2024.

Hungary

In September 2021, the NAIH[8] investigated Budapest Bank for using AI in customer service calls. The AI analyzed speech for silence, overlapping voices, keywords, and

[7] McCarthy, Niall. “Infographic: The Countries With The Most GDPR Data Breaches.” *Statista*, 21 January 2020, https://www.statista.com/chart/20566/personal-data-breaches-notified-per-eea-jurisdiction/

[8] Hungarian Data Protection Authority

emotional cues to detect dissatisfaction. Bank staff reviewed flagged calls and contacted customers. The bank justified its use of AI as necessary to improve call quality, reduce complaints, and prevent churn. Customers were notified about call recordings but not the AI analysis to avoid lengthy explanations. No identifiable data or automated profiles were stored, and high risks were mitigated by human oversight. Budapest Bank was fined €670,000.

France

France updated its data protection laws to tackle AI-related privacy issues, led by the CNIL[9]. The case involved Clearview AI, which scraped images from websites and social media without user consent for facial recognition. It was found to break GDPR rules by using personal photos to compose a facial recognition database illegally. The CNIL ordered Clearview AI to stop collecting data from French residents and delete the gathered data. The company was fined up to EUR 20,000,000 and faced daily fines for non-compliance. In May 2023, the CNIL published an “AI action plan” with guidelines concerning data handling, purpose definition, and impact assessments to ensure AI systems comply with privacy laws.

Greece

Greece’s Law 4961/2022 governs AI use, especially in hiring and workplace conditions for medium and large businesses using AI for profiling consumers or evaluating employees and partners. The law focuses on transparency, accountability, and responsible AI use, requiring an electronic Register of AI systems and a Data Use Code of Conduct to ensure companies operate with clarity and ethical standards. While the tools improve tracking of AI usage and ethical practices, maintaining these can be costly, especially for smaller businesses. The law’s strict compliance requirements and penalties create a significant administrative burden.

Spain

Spain's national strategy, led by the AEPD[10], was released in December 2020. Its role is to ensure compliance with GDPR and EU policy. Not only does it conduct investigations, but it also issues fines for data protection violations, such as the serious penalty on Spanish financial services company CaixaBank for mishandling data. The agency also explicitly develops ethical AI frameworks to ensure human-centric systems.

Germany

On May 6, 2024, Germany’s Conference of Data Protection Supervisors[11] (DSK) released AI and data protection guidelines to ensure GDPR compliance. The guidelines

[9] The French Data Protection Authority, Commission Nationale de l'Informatique et des Libertés

[10] The Spanish Data Protection Agency, Agencia Española de Protección de Datos

[11] Datenschutzkonferenz

address the need for transparency, limiting data collection, and maintaining strong data security. Users must be able to understand and contest AI decisions, especially in high-risk areas like facial recognition. Specialists should stay updated on AI privacy laws, perform Privacy Impact Assessments (PIAs) for high-risk AI, and consult experts. The DSK represents all German data authorities and enforces these rules.

The Court of Justice of the European Union (CJEU)

Though the CJEU does not impose fines, its judgments are very indicative of how GDPR fines are set, especially with AI-driven businesses. The court determines that the fines should be proportional to the global turnover of the group as a whole, a decision that could potentially place extremely large fines on major companies. Under the GDPR, fines can be as high as 4% of a company's global turnover for serious breaches. In later judgments, it was ruled that the CJEU interpreted fines can be imposed on controllers only if they are deliberately or negligently violating the GDPR. In this case, a Lithuanian public health authority that dealt with data inappropriately on a COVID app and a German real estate company that kept the data more extensive than necessary.

BLOCS EXPECTED

Pro-Regulation Bloc

This bloc pushes for stricter data protection and privacy rules within AI. The alliance stands for fair and transparent AI development to respect rights and ensure responsible data use. They support creating independent and competent bodies to oversee AI and enforce these rules. They prioritize an internet that ensures privacy and data protection at all costs, with clear safety and transparency guidelines.

Pro-Innovation Bloc

The second bloc believes that AI is indeed crucial for economic growth and technological progress. It supports flexible regulations that adapt as AI evolves so laws stay relevant and don’t stifle innovation. They insist on a risk-based approach, focusing on high-risk AI applications and allowing safer AI systems to operate with fewer rules. In this way, resource use will be effective, and innovation will ensue. High-risk AI, like in healthcare or self-driving cars, needs stronger regulations to protect people. This move also gives room for the rules to change if new risky AI technologies develop, therefore always keeping the regulations current. The delegates thus call for both standards from the industry and government regulations.

TIMELINE OF EVENTS

Date	Description of event

4 October 2011	Apple releases Siri.
15 January 2018	Alibaba develops an AI model that scores better than humans in a Stanford University reading and comprehension test.
25 May 2018	GDPR comes into effect.
17 September 2018	The First World Artificial Intelligence Conference is held in East China.
2019	Initial discussions focus on the interplay between AI and GDPR.
April 2019	EU presents Ethics Guidelines for Trustworthy AI.
April 2021	Dutch groups criticize the GDPR for not protecting personal data from AI misuse. The Dutch childcare benefits scandal shows how a flawed algorithm harms low-income families and immigrants by wrongly accusing them of fraud, causing financial and emotional distress.
April 2021	European Commission proposes AI Act.
November 2021	France adopts the National Strategy for AI under the "France 2030" plan. This strategy builds on the "AI for Humanity" phase (2018-2022) and aims to boost France's AI capabilities and drive economic growth.
13 November 2022	ChatGPT launches.
June 2023	EU AI Act is first published.
6 July 2023	WAIC 2024 was held in Shanghai.
October 2023	UN has created an advisory body to address AI governance.
December 2023	EU Parliament reaches a provisional agreement with the Council on the AI Act.
February 2024	EU AI Act is agreed upon.
13 March 2024	European Parliament votes on and adopts the AI Act.
21 March 2024	The UN General Assembly adopts the first global resolution on AI, covering human rights, data protection, and AI risks.
2 August 2024	The EU AI Act comes into force, establishing a common regulatory and legal framework for AI within the EU.
2 February 2025	Ban on AI systems with unacceptable risk.

RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Convention 108+ (Convention for the Protection of Individuals about Automatic Processing of Personal Data)

Convention 108+ is a revised international treaty that preserves individuals' data when using AI and other technologies. It guides governments, AI developers, manufacturers, and service providers on respecting human rights and privacy during AI development. AI applications manage risks associated with data processing, transparency, and human control over data usage. Decisions should not be solely automated without human oversight. The treaty builds public trust, provides international regulations, identifies and reduces AI risks, and ensures AI considers human rights and freedoms. However, it faces challenges in uniform application, lack of resources needed for implementation and legal enforcement, constant updates due to rapid AI advancements, and global coordination difficulties. Despite these hardships, the convention is an important step toward the responsible use of AI.

Global Privacy Assembly (GPA)

The GPA[12] is a global conference that tackles data protection issues. At its 45th session in Hamilton, Bermuda, in 2023, the GPA was interested in how data protection laws match AI usage.

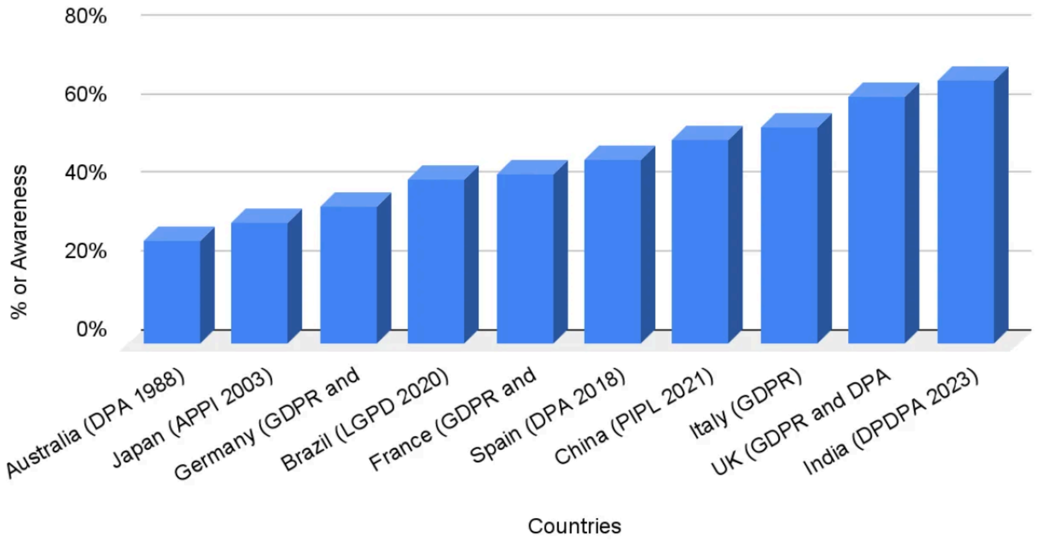
The goal is to ensure that generative AI follows privacy rules and uses privacy by design from the start. This means developers and providers need to apply these principles throughout the entire lifecycle of their systems, including doing Data Protection and Privacy Impact Assessments (DPIAs).

The Assembly also approved the G7 Data Protection and Privacy Authorities' statement on generative AI. AI developers must document their systems' functions, training data, and potential impacts on data protection. They ought to make this documentation available for external audits to address risks like biases and inaccuracies.

Lastly, it encourages ongoing global dialogue and raising awareness about AI risks. The other sphere, which is about renewing periods of data protection laws, also requires attention. Though not legally binding, these resolutions show how data protection authorities unite to address AI privacy challenges.

[12] Previously called the International Conference of Data Protection and Privacy Commissioners.

Figure 3: Data Privacy Law Awareness by Country[13]



PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

Organization for Economic Co-operation and Development (OECD)

Adopted in May 2019 and updated in May 2024, the OECD AI Principles help AI developers create trustworthy AI systems and provide guidance for policymakers on effective AI policies. Nations use OECD principles and tools to shape domestic AI policies and risk frameworks, promoting international collaboration and interoperability. The EU, the CoE, the US, the UN, and other jurisdictions' legislative and regulatory frameworks integrate the OECD's definitions of AI systems and lifecycles. The principles promote responsible AI by emphasizing inclusive growth, sustainable development, human-centered values, accountability, and transparency. Policymakers can use them as a comprehensive framework to develop national AI programs, but the lack of legally binding limits their efficacy. The degree to which these concepts are used consistently can vary depending on the resources and level of commitment of each nation. The OECD AI Policy Observatory offers materials to help policymakers grasp the implications of AI and develop informed legislation. The principles were upgraded to address more current challenges of general-purpose and generative AI, including privacy concerns, intellectual property rights, and secure data integrity. Some of the critical changes include measures to ensure that AI systems do not cause unintended harm to human beings and the environment. Other changes target misinformation management and data integrity. Furthermore, the principles offer OECD ethical business practices throughout the AI system's lifecycle and encourage engagement with knowledge suppliers as well as academics in AI.

[13] "Alarming Statistics and Details Behind Data Privacy in 2024." Edge Delta, 14 March 2024, https://edgedelta.com/company/blog/data-privacy-statistics

Data Protection Authorities (DPAs)

DPAs should take charge of watching over AI systems the high-risk ones, because they have a lot of know-how. From August 2025, DPAs could serve as the main contact for AI regulation. Improved communication between regulatory bodies is important to avoid oversight gaps. Clear procedures for cooperation and strong ties between the EU AI Office and DPAs will improve coordination.

European Data Protection Supervisor (EDPS)

The EDPS holds various conferences and seminars that focus on AI and privacy. Among these is the CPDP[14] conference held in May, which introduced panels on AI and data protection, and the European Data Protection Summit in June, which covered the role of data protection in a democratic society. Additionally, the EDPS conducts public events such as the EU Open Day and press conferences to present annual reports and updates on data protection strategies.

POSSIBLE SOLUTIONS

Call for clear and transparent AI reports

AI providers need to publish detailed reports on their systems as a function of creating transparency and trust consistently. Companies like Google and Facebook should provide details of how their AI processes data, and decisions, and safeguards privacy. The reports will detail what kind of data has been collected, how the data is used in the training of AIs, and what effect this has had on consumers. Organizations such as the EDPB, the European Union Agency for Cybersecurity (ENISA), and the EDPS can help set and guide these disclosure standards. Publicly available data assists users and authorities in understanding AI, ensuring privacy, and promoting trust.

Improve Data Anonymization

Effective anonymization ensures that personal data used in AI training cannot be connected to individuals. This entails methods like data masking and aggregation to de-identify information. Regular audits and updates are necessary to stay ahead of emerging re-identification techniques. Such techniques will be refined to protect privacy while enabling AI to examine massive datasets on a regular basis.

Clear guidelines for AI and GDPR compliance

We need to clarify GDPR rules for AI. The EDPB should issue clear guidelines on what’s acceptable with AI and how, in general, to follow GDPR. These describe how to use data for training AI, profiling, and automated decisions while protecting privacy. Separating general

[14] Computers, Privacy and Data Protection

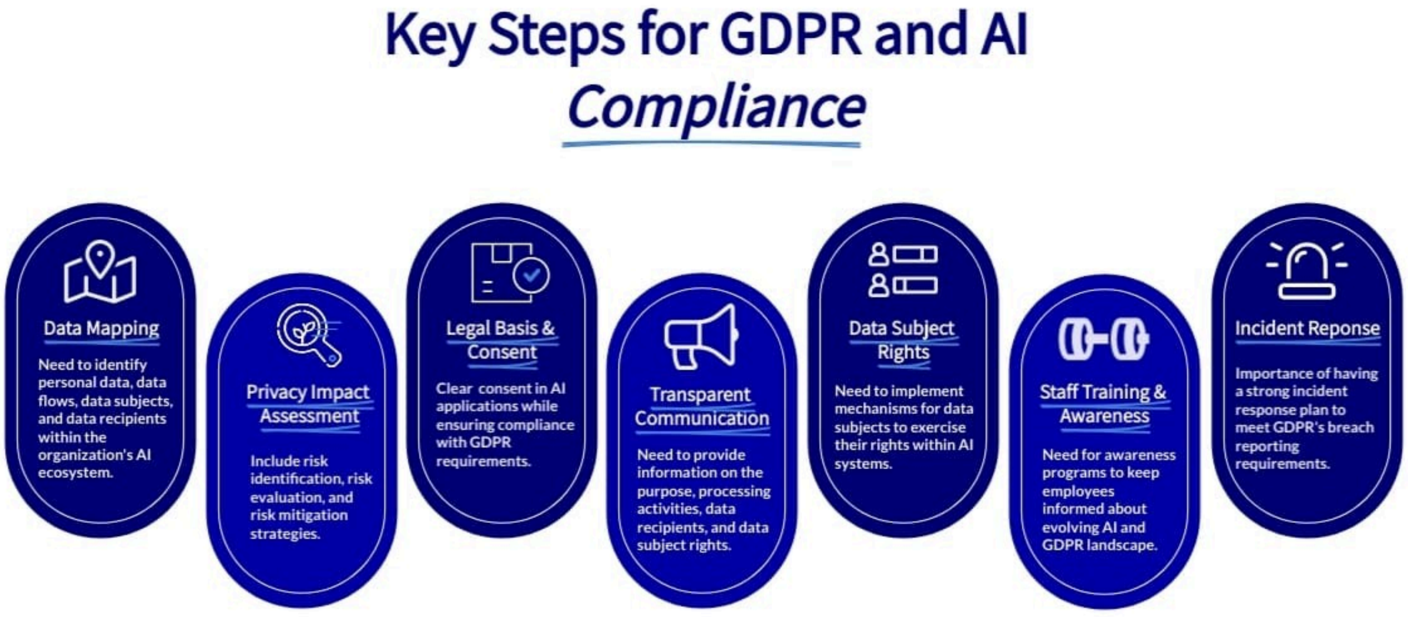
training data from individual assessments shall ensure that GDPR compliance reduces the risks of re-identifying individuals. Specific advice is needed for different industries, like healthcare and finance, ideally from agencies like the ICO[15] or BfDI[16]. AI systems should provide easy explanations of their decisions so people can understand and question them as needed. Thus, firms will adhere to GDPR and deploy AI responsibly.

Strengthen Human Oversight in AI

High-risk AI systems should have "human-in-the-loop" mechanisms, which allow humans to intervene before making final decisions. DPAs should audit these controls regularly to evaluate their effectiveness. Every firm, big and small, should provide mandatory training on AI oversight, including the ethical implications for employees. AI activity must be tracked by real-time monitoring dashboards, with any irregularities prompting immediate human intervention. Professionally staffed oversight committees should regularly review and approve the types of AI being deployed.

Raise awareness and education about AI rules

Easy-to-understand guidelines, FAQs, workshops, and seminars on data protection and AI transparency shall be provided by European organizations and NGOs. So, we can educate enterprises and the general public about AI legislation and their rights.



Key Steps for GDPR and AI *Compliance*

Data Mapping: Need to identify personal data, data flows, data subjects, and data recipients within the organization's AI ecosystem.

Privacy Impact Assessment: Include risk identification, risk evaluation, and risk mitigation strategies.

Legal Basis & Consent: Clear consent in AI applications while ensuring compliance with GDPR requirements.

Transparent Communication: Need to provide information on the purpose, processing activities, data recipients, and data subject rights.

Data Subject Rights: Need to implement mechanisms for data subjects to exercise their rights within AI systems.

Staff Training & Awareness: Need for awareness programs to keep employees informed about evolving AI and GDPR landscape.

Incident Reponse: Importance of having a strong incident response plan to meet GDPR's breach reporting requirements.

Figure 4: Impact of AI on Privacy and GDPR[17]

[15] ICO: Information Commissioner's Office

[16] BfDI: The Federal Commissioner for Data Protection and Freedom of Information

[17] "Impact of AI on Privacy and GDPR." LinkedIn, 13 September 2023, https://www.linkedin.com/pulse/impact-ai-privacy-gdpr-siddharth-srinivasan

BIBLIOGRAPHY

Wolford, Ben. “What is GDPR, the EU's new data protection law? - GDPR.eu.” *GDPR compliance*, https://gdpr.eu/what-is-gdpr/

“Alarming Statistics and Details Behind Data Privacy in 2024.” *Edge Delta*, 14 March 2024, https://edgedelta.com/company/blog/data-privacy-statistics

“Data Privacy Laws and Regulations Around the World.” *Securiti.ai*, https://securiti.ai/privacy-laws/

Spyridaki, Kalliopi. “GDPR and AI: Friends, foes or something in between?” *SAS Institute*, https://www.sas.com/en_us/insights/articles/data-management/gdpr-and-ai--friends--foes-or-something-in-between-.html

“Rethinking Decisions under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making.” *CEUR-WS.org*, 19 June 2023, https://ceur-ws.org/Vol-3423/paper8.pdf

Molnar, Petra, et al. “EU's AI Act Falls Short on Protecting Rights at Borders.” *Just Security*, 20 December 2023, https://www.justsecurity.org/90763/eus-ai-act-falls-short-on-protecting-rights-at-borders/

Fisher, Bill. “GDPR and AI: The next frontier for digital privacy regulation.” *eMarketer*, 2 June 2023, https://www.emarketer.com/content/gdpr-ai-next-frontier-digital-privacy-regulation

“ChatGPT banned in Italy over privacy concerns.” *BBC*, 1 April 2023, https://www.bbc.com/news/technology-65139406

Lawton, George. “AI and GDPR: How is AI being regulated?” *TechTarget*, 11 April 2024, https://www.techtarget.com/searchdatabackup/feature/AI-and-GDPR-How-is-AI-being-regulated

“Finally, the ECJ is interpreting Article 22 GDPR (on individual decisions based solely on automated processing, including profiling).” *Official Blog of UNIO*, 10 April 2023, https://officialblogofunio.com/2023/04/10/finally-the-ecj-is-interpreting-article-22-gdpr-on-individual-decisions-based-solely-on-automated-processing-including-profiling/

Winston, Eric. “GDPR — How does it impact AI?” *Information Age*, 5 June 2023, https://www.information-age.com/gdpr-impact-ai-14032/

Sartor, Professor, and Francesca Lagioia. “The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.” *European Parliament*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

Hilliard, Airlie. “AI Regulation Around the World: Spain.” *Holistic AI*, 23 March 2023, https://www.holisticai.com/blog/spain-ai-regulation

“EDPB adopts statement on DPAs role in AI Act framework, EU-U.S. Data Privacy Framework FAQ and new European Data Protection Seal | European Data Protection Board.” *European Data Protection Board*, 17 July 2024, https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en

Ford, Neil. “EU GDPR News Update: Three Legal Cases and AI Guidance - IT Governance Blog En.” *IT Governance EU*, 27 October 2023, https://www.itgovernance.eu/blog/en/eu-gdpr-news-update-three-legal-cases-and-ai-guidance

“Transparency requirements under the EU AI Act and the GDPR: how will they co-exist?” *Fieldfisher*, 11 April 2024, https://www.fieldfisher.com/en/insights/transparency-requirements-under-the-eu-ai-act-and-the-gdpr-how-will-they-co-exist

"Lessons from GDPR for artificial intelligence regulation | World Economic Forum." *The World Economic Forum*, 16 June 2023, https://www.weforum.org/agenda/2023/06/gdpr-artificial-intelligence-regulation-europe-us/

"Artificial Intelligence and Personal Data Protection: Complying with the GDPR and CCPA While Using AI." *Secure Privacy*, 4 October 2023, https://secureprivacy.ai/blog/ai-personal-data-protection-gdpr-ccpa-compliance

"International: The interplay between the AI Act and the GDPR - AI series part 1." *DataGuidance*, https://www.dataguidance.com/opinion/international-interplay-between-ai-act-and-gdpr-ai

Roser, Max. "The brief history of artificial intelligence: the world has changed fast — what might be next?" *Our World in Data*, 6 December 2022, https://ourworldindata.org/brief-history-of-ai

"AI Timeline – Artificial Intelligence." *UO Blogs*, https://blogs.uoregon.edu/artificialintelligence/ai-timeline/

Baig, Anas, and Maria Khan. "The Impact of the GDPR on Artificial Intelligence The Impact of the GDPR on Artificial Intelligence." *Securiti.ai*, 29 September 2023, https://securiti.ai/impact-of-the-gdpr-on-artificial-intelligence/

"EU AI Act: first regulation on artificial intelligence | Topics." *European Parliament*, 8 June 2023, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

"European Union AI Act Published in the Official Journal—Critical Milestones on the Road to Full Applicability." *WilmerHale*, 16 July 2024, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240716-european-union-ai-act-published-in-the-official-journal-critical-milestones-on-the-road-to-full-applicability

"Timeline - Artificial intelligence - Consilium." *Consilium. Europa. EU*, https://www.consilium.europa.eu/en/policies/artificial-intelligence/timeline-artificial-intelligence/

"AI Regulations around the World - Oxford." *Mind Foundry*, 25 January 2024, https://www.mindfoundry.ai/blog/ai-regulations-around-the-world

"The roadmap to the EU AI Act: a detailed guide." *Alexander Thamm GmbH*, 12 July 2024, https://www.alexanderthamm.com/en/blog/eu-ai-act-timeline/

"Does ChatGPT compromise privacy?" *BBC Science Focus Magazine*, https://www.sciencefocus.com/future-technology/does-chatgpt-compromise-privacy

"AI Act and GDPR: managing the world of data in the world of privacy." *EuroCloud Europe*, 24 October 2023,
https://eurocloud.org/news/article/ai-act-and-gdpr-managing-the-world-of-data-in-the-world-of-privacy/

"A pro-innovation approach to AI regulation: government response." *GOV.UK*, 6 February 2024, https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response

"CNIL confirms the compatibility of AI with the GDPR," CNIL confirms the compatibility of AI & the GDPR - Hogan Lovells Engage, https://www.engage.hoganlovells.com/knowledgeservices/news/cnil-confirms-the-compatibility-of-ai-the-gdpr_1/