



Artificial Intelligence (AI) and Personal Data

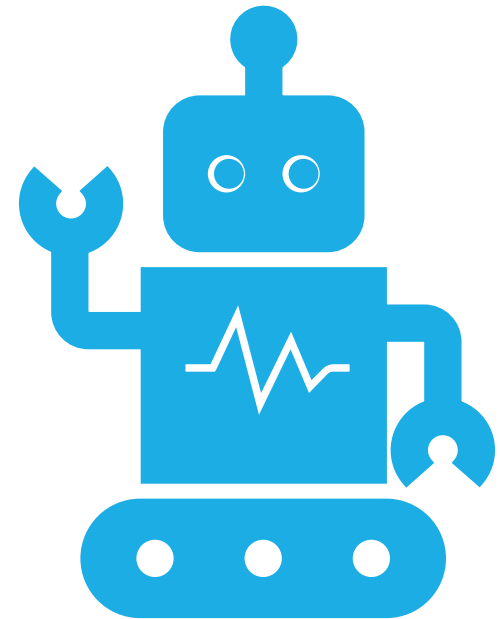
PERSONAL DATA AND PRIVACY ISSUES WITHIN THE FRAMEWORK OF AI

What is AI and how does it work?

It is important to understand the relationship of AI with personal data and how data protection rules are essential to apply before a processing takes place.

Artificial Intelligence (AI) refers to the development of computer systems or software that can perform tasks that typically require human intelligence. These tasks include learning, reasoning, problem-solving, understanding natural language, speech recognition, and visual perception. The goal of AI is to create machines capable of mimicking cognitive functions associated with human intelligence, enabling them to adapt, improve performance over time, and accomplish tasks without explicit programming for each step.

In summary, Artificial Intelligence encompasses the development of technologies that enable machines to exhibit intelligent behavior, simulate cognitive functions, and perform tasks traditionally associated with human intelligence.



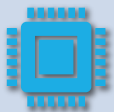
Relationship of AI and Personal Data



AI systems rely on vast amounts of data to train their models and make accurate predictions.



Some data are considered as personal data and are essential to AI because it is a crucial input to the functioning of certain AI systems.



Those data often includes personal and sensitive information.

It is crucial to ensure that data collection, storage, and processing adhere to strict privacy standards to protect individuals' personal information.


Is there a legal basis of use of AI?

Different jurisdictions have different legal bases for using AI, and these bases are impacted by current laws and regulations that cover technology, data protection, privacy, and other pertinent topics.

Here are some important things to think about:

- 1. General Legal Frameworks**
- 2. Data Protection Laws**
- 3. Ethical Guidelines and Standards**
- 4. Sector-specific Regulations**
- 5. Intellectual Property Laws**
- 6. Liability and Accountability**
- 7. International Agreements**
- 8. Government Regulations and Policies**

Businesses and developers need to be aware of how the law is changing, particularly when it comes to artificial intelligence (AI). New laws are being revised all the time to take into account the new opportunities and challenges that these technologies provide. To guarantee compliance with relevant rules, legal assistance from experts in data protection and technology law is also advised.



Is there a legal basis of use of AI?

The European Union (EU) has responded by taking a big step to regulate AI.

The first real attempt to regulate AI is the EU AI Act.

By establishing uniform regulations guiding the creation, promotion, and application of AI within the EU, it seeks to establish Europe as a reliable AI hub on a worldwide scale. The AI Act seeks to guarantee the safety and observance of fundamental rights and values by AI systems operating within the EU.

Its goals also include encouraging a single EU market for AI, improving governance and enforcement, and stimulating investment and innovation in AI.

Parliament priority is to make sure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly. AI systems should be overseen by people, rather than by automation, to prevent harmful outcomes.

On 14 June 2023, MEPs adopted Parliaments negotiating position on the AI Act.

The talks will now begin with EU countries in the Council on the final form of the law.

The aim is to reach an agreement by the end of this year.

When employing AI, maintaining data privacy is essential to safeguarding people's private information and adhering to legal requirements.

Several procedures to guarantee data privacy in AI applications include:

1. Data Minimization:

Only gather the information required to complete the particular AI task.

2. Anonymization and Pseudonymization:

Remove or encrypt personally identifiable information (PII) from the dataset using anonymization or pseudonymization.

3. Secure Data Storage:

To safeguard data that has been stored, put strong security measures in place.

4. Third-Party Assessments:

Evaluate the third-party service providers' or partners' data privacy policies.

By putting these procedures into place, businesses may meet legal obligations, build customer confidence, and greatly improve data privacy when utilizing AI.

5. Data Encryption in Transit:

Encrypt data as it's being transmitted by using secure communication channels.

6. Privacy by Design:

From the beginning of the design and development of AI systems, incorporate privacy safeguards.

7. User Education:

Inform users of their rights and data privacy procedures.

HOW CAN DATA PRIVACY BE MAINTAINED WHEN USING AI?

can AI be considered a threat towards data privacy?

THERE IS ALSO POSITIVE SIDE TO AI WHEN IT COMES TO DATA PRIVACY.

WHILE AI IN AND OF ITSELF DOES NOT REPRESENT A DANGER TO DATA PRIVACY, IMPROPER DESIGN, IMPLEMENTATION, AND USE MIGHT HAVE UNINTENDED CONSEQUENCES.

AI CAN BE USED TO MINIMIZE THE RISK OF PRIVACY BREACHES BY ENCRYPTING PERSONAL DATA, REDUCING HUMAN ERROR AND DETECTING POTENTIAL CYBERSECURITY INCIDENTS.

AI-related potential risks to data privacy

1. **Data Misuse:**

There is a chance that AI systems will be abused if they are built to gather, handle, or analyze more data than is required. Privacy violations may result from the excessive gathering of private data.

2. **Inadequate Security Measures:**

AI systems with weak security are more susceptible to intrusions, which could result in data breaches and illegal access. Strong security measures must be put in place to safeguard AI models and the data they process.

3. **Biases and Discrimination:**

AI models that have been trained on biased datasets have the potential to reinforce preexisting biases and even magnify them, producing discriminating results. People's privacy may be impacted by this, particularly in delicate sectors like recruiting, lending, or law enforcement.

4. **Surveillance and Monitoring:**

If AI applications are utilized for monitoring or surveillance—like facial recognition systems—without the appropriate permissions and safeguards, they may violate people's right to privacy.

5. **Inadequate Consent Mechanisms:**

A key component of data privacy is getting people's informed and explicit agreement before processing their data. If appropriate consent processes are not in place, AI applications may violate privacy laws.

6. **Insecure Data Sharing:**

There's a chance of data leakage or unauthorized access if AI systems require data sharing between entities, for cooperative learning or other reasons.

Apply data protection rules to AI systems

In order to ensure that personal data is handled responsibly and in line with privacy standards, applying data protection principles to AI systems requires a combination of technical measures, ethical considerations, and legal compliance.

Here's how to use data protection guidelines with AI systems:

- 1. Understand Applicable Regulations**
- 2. Data Minimization**
- 3. Informed Consent and Purpose Limitation**
- 4. Data Security**
- 5. Privacy by Design and Default**
- 6. Data Subject Rights**
- 7. Ethical AI Principles**
- 8. Transparency and Explainability**
- 9. Data Impact Assessments (DPIAs)**

By integrating these measures, organizations can create a privacy-conscious environment for their AI systems, fostering trust among users and ensuring legal compliance with data protection rules. It's essential to involve legal experts, data protection officers, and other stakeholders throughout the AI development lifecycle to address privacy considerations effectively.

AI a game-changing technology

It's critical to adhere to best practices like data reduction, encryption, transparency, and ethical considerations throughout the AI development lifecycle in order to reduce these risks and guarantee that AI does not pose a threat to data privacy. Respecting applicable data protection laws and regulations is also necessary because breaking them may have legal repercussions.

To address concerns about data privacy, organizations and developers should place a high priority on responsible AI practices, carry out in-depth privacy impact assessments, and interact with stakeholders. AI system audits and evaluations on a regular basis can assist in identifying and proactively addressing any privacy problems.



DATA PROTECTION IN THE ERA OF AI



Take advantage and use AI technology!



But not forget to implement proper safeguards to protect personal data!



Act Responsibly!

Technology can bring good if used without doing harm to others.



Filippos Panteli
Member **CAIPP**

Cyber Security Engineer
geevo[®]

filippos.p@geevo.eu

PRESENTER

Visit us at **www.caipp.eu**

Your Cybersecurity, our passion!



Join us today!

Memberships

Club member

The Club IPP (Information Protection and Privacy) member category is available to companies or other professional entities that operate a specialised team whose primary purpose is to improve Information Protection, Cybersecurity and Privacy and which group offers a variety of professionally provided Information and Privacy Services on a daily basis.

Full member

The Full IPP (Information Protection and Privacy) member category is available to professionals involved in Information and Privacy Protection who offer a variety of professionally-provided services on a daily basis.

Affiliated member

Affiliated members can be:

- a. People who are indirectly involved in Information and Privacy Protection and/or work in relevant categories (IT service providers, data management, legal counsellors), whether they are company owners or employees.
- b. Suppliers of equipment or solutions for information and privacy protection.

Contact Us



+357 22 889800



info@caipp.eu



<https://caipp.eu/>

Cyprus Association of Information Protection and Privacy

Your Cybersecurity, our passion!