AI POLICY OF THE KLINGER GROUP

Gernot Leithner

30.06.2025

INTRODUCTION

This policy governs the application of artificial intelligence (AI) within the KLINGER Group and is based on the provisions of the EU AI Regulation (EU AI Act).[1] The aim is to ensure responsible and safe use of AI technologies while promoting the innovative strength of the corporate group.

SCOPE

This policy applies to all employees of the KLINGER Group who use AI technologies in their work processes. It includes both internal and external applications of AI systems.

PRINCIPLES

1. Compliance with the EU AI Regulation: All AI applications must comply with the provisions of the EU AI Regulation to ensure a high level of protection in terms of health, safety, and fundamental rights.
2. Responsible use: AI systems may only be used for professional purposes that align with the company's goals. As with any IT system, only AI systems that are approved by the company's IT management and comply with all applicable internal and external regulations may be employed.
3. Transparency: The content generated must be reviewed and adjusted if necessary to ensure accuracy.
4. Safety: AI systems must not be used to make decisions that could compromise the safety of employees, machines, or products.
5. Confidentiality: Company data, personal data, and confidential information about third parties may only be used with AI systems if confidentiality is guaranteed and compliance with all applicable data privacy regulations is ensured.

PERMITTED USE CASES

Most use cases are permitted as limited risk or minimal/no-risk AI systems. These include for example:

1. Text creation: Support in creating reports, emails, and other business-related texts.
2. Training and education: Use as a learning resource for technical, professional, or general topics.
3. Problem-solving: Support in developing ideas and concepts for process optimization.
4. Communication: Improvement of internal and external communication, e.g., by drafting formal communications.
5. Customer service: Use of AI to support customer service, e.g., through chatbots that can respond to customer inquiries in real-time.
6. Data analysis: Use of AI to analyse large amounts of data to identify patterns and trends relevant to business decisions.
7. Process automation: Automation of routine tasks, such as processing invoices or managing orders.
8. Personalized advertising: Use of AI to create personalized advertising campaigns based on customer behaviour and preferences.
9. Quality control: Use of AI to monitor and improve product quality through automatic error detection.

[1] cf. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

PROHIBITED USE CASES

According to the EU AI Regulation, the following AI applications are expressly prohibited:

1. **Manipulative or deceptive techniques:** AI systems that use techniques of subliminal influence outside a person's consciousness or intentionally manipulative or deceptive techniques to significantly change the behaviour of a person or group of people. This impairs the ability to make an informed decision and causes significant harm.

2. **Exploitation of vulnerability:** AI systems that exploit the vulnerability or need for protection of a natural person or a specific group of people due to their age, disability, or a specific social or economic situation to significantly change their behaviour and cause significant harm.

3. **Social scoring:** AI systems for evaluating or classifying natural persons or groups of people over a certain period based on their social behaviour or known, derived, or predicted personal characteristics or personality traits. This leads to a disadvantage or discrimination in social contexts that are unrelated to the original circumstances or to an unjustified or disproportionate disadvantage.

4. **Risk assessments for crimes:** AI systems for conducting risk assessments regarding natural persons to evaluate or predict the risk of a person committing a crime solely based on profiling or assessing their personal characteristics and traits.

5. **Facial recognition:** AI systems that create or expand databases for facial recognition by indiscriminately reading facial images from the internet or surveillance footage.

6. **Emotion recognition in the workplace and educational institutions:** AI systems for deriving the emotions of a natural person in the workplace and educational institutions, unless the use of the AI system is introduced or marketed for medical or safety reasons.

7. **Biometric categorization:** AI systems for biometric categorization that categorize natural persons individually based on their biometric data to infer or derive their race, political views, union membership, religious or ideological beliefs, sexual life, or sexual orientation.

8. **Biometric real-time remote identification:** The use of biometric real-time remote identification systems in publicly accessible spaces for law enforcement purposes, except when it is absolutely necessary to search for specific victims, avert immediate danger, or identify offenders.

RESTRICTIONS FOR HIGH-RISK AI SYSTEMS

According to the EU AI Regulation, certain AI systems are considered high-risk applications. **The use of such systems is generally prohibited within the KLINGER Group.** These include:

1. **Biometrics:** AI systems for biometric remote identification, biometric categorization based on sensitive or protected attributes or characteristics, and emotion recognition.

2. **Critical infrastructure:** AI systems as safety components for the management and operation of critical digital infrastructure, road traffic, or water, gas, heat, or electricity supply.

3. **General and professional education:** AI systems for determining access or admission to educational institutions, evaluating learning outcomes, assessing educational levels, and monitoring and detecting prohibited behaviour during exams.

4. **Employment, personnel management, and access to self-employment:** AI systems for hiring or selecting individuals, deciding on working conditions, promotions, and terminations, assigning tasks, and monitoring and evaluating employee performance and behaviour.

5. **Accessibility and use of essential private and public services and benefits:** AI systems for assessing eligibility for public support services and benefits, creditworthiness assessment and credit scoring, risk assessment and

pricing for life and health insurance, and evaluating and classifying emergency calls and dispatching emergency and rescue services.

6. **Law enforcement:** AI systems for assessing the risk of becoming a victim of crime, as lie detectors or similar instruments, for evaluating the reliability of evidence, assessing the risk of committing or reoffending crimes, and profiling natural people in the course of detecting, investigating, or prosecuting crimes.

7. **Migration, asylum, and border control:** AI systems as lie detectors or similar instruments, for assessing security risks, irregular immigration, or health risks, for assisting in the examination of asylum and visa applications and residence permits, and for detecting, recognizing, or identifying natural persons in connection with migration, asylum, or border control.

8. **Justice and democratic processes:** AI systems to support judicial authorities in investigating and interpreting facts and legal provisions, and to influence the outcome of an election or referendum or the voting behaviour of natural persons.

These systems are classified as high-risk because they can have significant impacts on the health, safety, and fundamental rights of individuals.

If the use of a high-risk AI system is deemed necessary, prior review and approval by KLINGER Holding GmbH is required. In the event of approval, additional requirements must be met to ensure the safety and protection of fundamental rights.

USE OF "GENERAL PURPOSE" AI

The use of "General Purpose" AI is permitted in general.

However, **company data like specifications, contracts or worksheets (excluding personal data)** may only be processed in „General Purpose" AI if confidentiality is guaranteed by the AI operator and the data is not used for model training. These guarantees are frequently part of paid subscriptions. This is often not the case with free offers! This data must not be uploaded in a prompt of a “General Purpose” AI that is free and does not guarantee confidentiality!

Currently only classified as permissible are:

» **Microsoft 365 Copilot**
» **ChatGPT Team,**
» **ChatGPT Enterprise**
» **Perplexity Free with the option to opt out of data training (AI data retention turned off)**
» **Perplexity Pro with the option to opt out of data training (AI data retention turned off)**
» **Perplexity Enterprise Pro**

In addition, next to company data **personal data** may only be processed in a "General Purpose" AI if the conditions for processing this data according to the General Data Protection Regulation (GDPR) are met and the provisions of the General Data Protection Regulation (GDPR) are complied with.

To ensure compliance with the GDPR, a data processing agreement (DPA) with the provider of the "General Purpose" AI is required.

A data processing agreement is in place for the use of
» **Microsoft 365 Copilot**

For the use of **ChatGPT Team or ChatGPT Enterprise** to process personal data, a data processing agreement (Data Processing Addendum) with the provider of this AI (OpenAI) must be concluded by the KLINGER Company, in whose business operations (by its employees) this AI is used.

For the use of **Perplexity Enterprise Pro** to process personal data, a data processing agreement (Data Processing Addendum) with the provider of this AI is available for such an agreement.[2]

LABELING REQUIREMENT FOR AI-GENERATED CONTENT

Content generated **entirely** by AI must be appropriately labelled. In particular this applies to:

- Automatically generated reports or summaries.
- Generated texts in external and internal communication.
- AI-generated images or videos.

RESPONSIBILITIES

1. **Employees:** All employees are responsible for complying with this policy and ensuring that the use of AI technologies meets the established data protection and security requirements.

2. **IT Manager:** The IT Manager role is responsible for selecting appropriate AI models and monitoring compliance with data protection regulations.

FINAL PROVISIONS

This policy comes into effect immediately and will be regularly reviewed and updated to reflect the latest developments in AI and legal requirements.

It must be communicated to all employees.

[2] Perplexity refers to DataRep, a company registered at The Cube, Monahan Road, Cork, T12 H1XY, Republic of Ireland (EU), with the contact email address privacy@perplexity.ai, as their representative in the European Economic Area (**"EEA"**) for the purposes of the EU GDPR. Cf. https://www.perplexity.ai/hub/legal/privacy-policy