CORPORATE IT & PROCESS MANAGEMENT

# Policy on the use of Artificial Intelligence

HOERBIGER

# Table of content

# 1. What is Artificial Intelligence?

Artificial Intelligence ("AI") enables machines, in particular computer systems, to perform tasks that only humans could do such as reasoning, learning, planning, analysing information, making decisions, and solving problems.

"AI system" means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

AI systems are fed with information from data sources; they process it and create trained models that use the input data as a reference. Usually, the more data an AI system has, the better it can learn.

AI systems can adapt their behaviour to a certain degree by analysing the effects of previous actions and even working autonomously.

There are different types of AI:

- **AI systems** are to be found for example in virtual assistants, image analysis software, web search engines, machine translations, speech and face recognition systems, chatbots, generative AI (e.g., ChatGPT, Midjourney, ...).

- **Embedded and Non-Embedded AI:** AI systems can be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serves the functionality of the product without being integrated therein (non-embedded).

# 2. Scope

This policy on the use of AI ("Policy") regulates (i) the purchase and (ii) the use of AI by the HOERBIGER group. This Policy applies to all employees of the companies of the HOERBIGER group, as well as other persons dealing with the operation and use of AI systems on HOERBIGER's behalf.

# 3. Purpose to regulate the use of AI

While AI, and in particular AI software, provides a better access to information and can be an efficient support to HOERBIGER's daily activities, AI comes with several risks.

Due to the nature of AI (e.g. biases, opacity, "AI black box"), one may not assume that all AI systems provide accurate, objective information or data nor that they will ensure the protection, privacy and confidentiality of the data and information they receive or generate without the implementation of sufficient compliance measures.

- AI is generally trained on limited datasets, the quality, source and limitations of which must be understood. AI often generates false responses, which appear plausible but are untrue.

- AI systems tend to generate biased or discriminatory responses which can be contractionary to our HOERBIGER values and our Code of Conduct.

- Many AI systems retain the information given and resulting outputs, analyse and store them for AI training purposes

For this reason, AI systems shall always be used with caution and due care.

The purpose of this Policy is to define the framework for the appropriate use of AI at HOERBIGER in compliance with applicable legal obligations and our values.

# 4. Key Rules

## 4.1 AI procurement

4.1.1 For any kind of procurement of new AI systems (e.g. AI supported software, or AI software) and/or functionalities you need to (1) get the approval of your manager and (2) upon your manager`s approval file an AI system request according to the New Software Request Policy[1] and wait before any purchase or use of AI system until your request has been approved by the Corporate IT department in writing (also electronic text). Such approval is not required if the AI system has already been approved by Corporate IT. In the Global IT Portal[2] you will find the list of software systems which have been pre-approved by Corporate IT.

4.1.2 Any new AI tool`s license agreement must be checked with special focus on data and machine learning rights & obligations contractual clauses by Group Legal & Compliance and Corporate IT.

4.1.3 A REASONABILITY Check of scenarios of the capability and potential impact within and outside of the use of the new AI system must be done (e.g. check on risk level of each AI system according to applicable laws, as well as business interests) and summarized in writing as basis for the decision for rejection or approval.

4.1.4 The approval process starts with several checks, in particular – without limitation - whether the AI system ensures state-of-the-art data security and privacy (e.g., encryption of all data processed using industry-standard protocols, restricted access based on the principle of “least privilege with regular reviews”), and is compliant with any applicable law or regulation, esp. such on artificial intelligence or data protection (e.g. EU General Data Protection Regulation ("GDPR"), AI Act).

4.1.5 When AI is used under HOERBIGER's authority HOERBIGER will regularly be considered a "deployer" under the AI Act and must comply with the applicable obligations. Special attention must also be given to data protection impact assessment and the respective lists published by local supervisory authorities, where applicable.

[1] Works Council check, IT Security Check and Data Protection Compliance check. Requests need a check on the required information as e.g. software name, provider, roles of the parties, intended use cases, assumed risk level, affected persons such as employees or customers, etc.

[2] https://hoerbigergroup.sharepoint.com/sites/GlobalITPortal/SitePages/Artificial-Intel.aspx?web=1

[3] E.g. prohibited AI practices such as subliminal manipulation or deception, exploitation of vulnerabilities, social scoring (cf Art 5 AI Act); or prompting confidential business or technical information into large language models or similar AI systems.

## 4.2 Use of AI

4.2.1 AI must only be used for the use cases defined in the procurement process or for any additional use case approved by the same procedure.

4.2.2 You use AI systems responsibly, ethically and in accordance with the applicable laws and regulations and HOERBIGER policies and Code of Conduct, particularly those related to data protection and intellectual property. AI must not be used to create content that infringes rights of any person (e.g. privacy, intellectual property rights). The use of AI shall be guided by the principles of respect for human autonomy, prevention of harm, fairness and explicability (transparency).

4.2.3 Where HOERBIGER acts as Deployer, High-Risk AI Systems may only be used in accordance with their official Instructions. For Use and Intended Purpose.

4.2.4 "USE WITH CARE" Principle: You DO NOT provide, prompt, give, enter, store etc. AI system with high sensitive information, including (without limitation):

- Special Categories of Personal Data (e.g. ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sex life) or other sensitive personal data of any individual person (employees, third parties, customers, consultants' data) like e.g. birth date, social security number, private address, private contact information (private email, private phones, social media accounts etc.), bank account information, fee or income data, health data of any kind etc.) – For avoidance of doubt, this Policy does not affect other policies on data protection and data privacy and merely complements them,
- HOERBIGER's or third parties' business & trade secrets, .
- Any information subject to confidentiality obligations or intellectual property protection or which has never been made publicly available (e.g. HOERBIGER company financials, customers' or suppliers' contracts, pricing information, market related strategies, etc.),
- Product research and development related information - whether related to HOERBIGER or related to its business partners in the value chain (up- and downstream).

4.2.5 Prior to using AI and thereafter in regular intervals you must partake in HOERBIGER's AI training, as provided from time to time.

4.2.6 You shall only use AI within your realm of expertise and with sufficient skills, knowledge and understanding of the AI's opportunities and risks and possible harm it can cause (AI literacy).

4.2.7 You shall only use the output & results generated by AI system without infringing any intellectual property rights. If you are unsure, contact Group Legal & Compliance before usage.

4.2.8 Content created with AI must be transparently labelled as such internally. This does not apply to texts (incl. translations and code) that have undergone a process of human review or editorial control.

4.2.9 You exclusively use the AI systems as a tool to support your expertise; it should not replace it. Any results or outputs generated by AI systems that you wish to use in your work must be thoroughly reviewed by you and can never replace your judgement of the subject matter.

# 5. Monitoring and Audits

HOERBIGER IT Security is responsible for monitoring the approved AI systems, HOERBIGER's role, approved use cases, the risk classification, the required AI literacy and will request the respective AI-System owners to perform regular bias and fairness audits and report the results to Corporate IT.

AI systems, which have been internally approved for use at HOERBIGER, must be:

- regularly monitored by HOERBIGER IT Security to identify potential security incidents; and
- subject to regular bias and fairness audits to ensure compliance with the applicable laws and regulations.

# 6. Consequences

Non-compliance with applicable AI regulations may result in severe adverse action against HOERBIGER (e.g. fines). Violations of this Policy thus, as well as violations of existing policies and work instructions, may result in various legal consequences.

# 7. Review of the Policy

This Policy, and the list of pre-approved AI systems, will be reviewed at least annually, and updated on a regular basis to reflect any new relevant development in artificial intelligence, any new relevant law or regulation and potential emerging security threat.