AI policy and guidelines

1. Purpose and scope

Purpose

The purpose of this policy is not only to promote the responsible and safe integration of Artificial Intelligence (AI) and other digital innovations into our operations, but also to enable increased competitiveness. By integrating AI, we aim to streamline workflows and create value for both customers and employees. In doing so, we position the company at the forefront of technological innovation, while maintaining high standards of privacy, user safety, and ethics.

Extent

This policy applies to all employees, contractors and partners within the company.

2. Principles for the use of AI and new technologies

Purchasing and implementation

All AI tools and digital innovations must be reviewed and approved by the CEO before purchase and use. This includes an assessment of the technology's reliability, safety, and compliance with ethical guidelines.

Definition of AI and new technologies

This policy focuses primarily on generative AI and LLMs (large language models), which use extensive datasets to generate decision support, texts and summaries. This technology is controlled by instructions from users, known as prompts, to extract data and information. Examples of these language models include Bing, ChatGPT, and image generation programs such as DALL-E.

Use and Approval

The use of AI tools requires the approval of the employee's immediate manager. Employees must be provided with relevant information regarding the use of AI to ensure the correct use of the technology.

Responsibility for end results and data

The employee is responsible for how the data is used and for the end result of a completed task. The employee must be transparent about whether and how AI has been used in the performance of a task and be able to explain the result. The duty of loyalty in the employment contract and laws on confidentiality and trade secrets apply.

When using open AI solutions at work, i.e. AI models that are not in-house, approval must be obtained from the immediate manager.

Under no circumstances should customer data be entered into open AI solutions. Nor may internal company information (Wenell) that can be considered business-critical (training material, finances, personal data, etc.) be used in open AI solutions.

3. Legal and ethical compliance

Laws and regulations

The use of AI tools must comply with applicable legislation, including, but not limited to, the General Data Protection Regulation (GDPR), the Work Environment Act and the Discrimination Act.

Ethical guidelines

All AI use must comply with the company's internal ethical guidelines and principles for responsible use of technology. The use of AI must be transparent, traceable and the approach and results must be explainable.

4. Risk and opportunity analysis

Regular analyses of the possible risks and benefits of AI use shall be carried out by the company's management. Reports and recommendations based on these analyses shall, where necessary, form the basis for decisions and measures.

5. Monitoring and reporting

Monitoring of AI use shall take place continuously to ensure that this policy and the company's overall goals are complied with. Incidents or issues related to AI should be reported immediately to a senior manager.

Any violation of this policy, whether intentional or mistaken, should be handled with both seriousness and understanding of the human factor in the use of technology.

Immediate action in case of mistakes

If an employee realizes that they have entered sensitive information into an AI tool by mistake, the first steps are to:

- Immediately cancel all running processes in the tool.
- Inform their immediate manager and IT manager without delay.
- Follow instructions to securely delete or anonymize the information entered, if possible.

An investigation shall be launched to determine the extent of the breach and to identify any security deficiencies. This will help to understand how the mistake occurred and how similar events can be prevented in the future.

The IT manager, together with legal expertise, must review the incident to assess any risks of data leakage and legal consequences. If sensitive information has left the organization's

control, a risk assessment must be carried out and appropriate measures taken according to applicable legislation, such as the GDPR. If there is a risk that personal data has been compromised, the organization shall comply with statutory reporting requirements and notify affected individuals and data protection authorities where necessary.

6. Disciplinary measures

While the focus is on education and preventing future mistakes, repeated or egregious violations of the policy can lead to action. These measures shall be proportionate to the seriousness of the infringement and may include warning, reassignment or, in particularly serious cases, dismissal.

Documentation and feedback:

All incidents and actions must be carefully documented. This documentation shall be reviewed to continuously improve our processes and policies. We encourage feedback from employees to further develop our understanding and management of AI tools.

Summary

Management is positive about the use of AI in work

The employees ensure that the use takes place in an orderly manner with respect for laws, regulations and the policy above

The employee is responsible for the end result

Skills development takes place through conversations and training

Security and privacy are prioritized.

7. Policy updates

This policy is a dynamic document that will be updated regularly to reflect the latest developments in technology and legislation.

Stockholm, September 3, 2024

……..

Tommy Olin, VD