Using AI safely:
Data protrction, copyright, transparency

By Designing AI Heroes

Why this matters

AI systems, especially machine learning, rely heavily on large amounts of data. When using AI, data protection is essential to ensure users' personal information is handled securely and ethically. Copyright matters because AI systems often learn from existing content, and creators deserve recognition and fair use of their work. Transparency is also crucial so users understand how AI models make decisions and what data they are trained on.

Without clear guidelines, misuse of data and intellectual property can lead to legal and ethical issues. Therefore, responsible AI use depends on strong policies that protect rights and build trust. Use the latest versions/models of AI tools, which often include improved security, features, and compliance updates.

Note: this document is created in April 2025. Any laws can change. This document will be updated when it will be necessary.

Data protection (GDPR - relevant throughout the EU)

- Legal basis: Any processing of personal data by AI requires a legal basis (e.g. consent, contract fulfilment, legitimate interest).
- Data minimisation: Only necessary data may be processed.
- Transparency: Data subjects must be clearly informed about what happens to their data.
- Rights of the data subjects: Information, erasure, objection, etc. must be guaranteed - even in the case of automated decisions.
- Profiling & automated decisions: Particularly strictly regulated - e.g. for credit decisions, application procedures, etc.

What you should bear in mind when using AI regarding data protection

- Do not use personal data without verification: Careful handling of the data entered. Check whether data allows conclusions to be drawn about individuals (name, behaviour, etc.).
- Maintain confidentiality: Avoid passing on personal, confidential or sensitive information.
- Anonymise data: use placeholders for names or any other sensitive data.
- Do not upload any company/administrative documents with sensitive data.
- Use the 'Provisional chat' function in ChatGPT for particularly sensitive requests.

Copyright and intellectual property

- Abuse potential.
- Training data: Copyright is infringed when AI is trained with copyrighted material.
- AI-generated content: Currently, no clear law or legislation that regulates the authorship of AI-generated content. it must therefore be decided on a case-by-case basis whether a human has had sufficient influence on a text, image or video to be regarded as the author.
- Use of AI-generated content: Check whether, for example, images, texts etc. from publicly accessible tools can be used in a legally secure manner.
- Use of AI-generated images: AI-generated content - this also means AI-generated images - is generally not protected by copyright, which means there are typically no legal restrictions on its use. However, users must adhere to the terms of service of the AI tool that is used to create the content. Additionally, care should be taken to ensure that the output does not unintentionally infringe on any third-party copyrights.

What you should bear in mind when using AI regarding copyright and intellectual property

- Check AI-generated content: Texts or images can unintentionally imitate copyrighted works.
- Use plagiarism checking tools (e.g. Plagscan, Copyscape) to check whether content may imitate existing texts too closely.
- Cite sources: If you use results from AI, be transparent about the source and the use of AI.
- Always check the answer: Do not simply use the output without checking the facts (hallucination).
- In case of uncertainty: consult subject matter experts.
- Use AI as a source of inspiration and add a your personal "touch" to the content and edit it before using it.

Liability and Transparency

- The user is always liable for the content generated by AI - in case of doubt, this means the company that uses AI-generated texts and images in its own name or adopts the results of an AI as its own, be it as content on the website, in customer documents or in marketing documents.
- 'The AI' itself, however, is not liable. It already lacks its own legal personality.
- According to general standards, the manufacturer can only be held liable if, for example, the AI does not have the contractually warranted characteristics or if the manufacturer has not taken sufficient safety precautions with the AI, resulting in damage.

What you should bear in mind when using AI regarding liability and transparency

- Document the use and purpose of the AI: Who uses the AI, with what data, for what purpose, for how long?
- AI should only support, not replace - e.g. when checking applications, calculating deadlines, completing forms.
- Create transparency for those affected: Provide clear information when AI is used, e.g. in customer service.
- Be Transparent About AI Use: Clearly disclose when content is created or assisted by AI, especially in academic, journalistic, or commercial contexts.
- Humans remain in control: AI must not decide on important matters alone (e.g. rejecting applications, cancelling customers), AI can make suggestions but not conclusively evaluate or reject them. Always involve human judgment, especially in legal, medical, or safety-related areas.
- Document results and make them verifiable: AI must not make any decisions that cannot be retraced and, if necessary, corrected by humans.