



Danish Crown

AI and Data Ethics policy



1. Our policy

1.1 Our commitment

Danish Crown complies with both Danish and EU legislation on AI, data ethics and privacy protection. In addition, Danish Crown recognizes that the technological development and the evolving benefits and risks of large-scale data use, require thoughtful and responsible decision-making.

This policy describes Danish Crown's approach to good data ethics and the principles that apply to Danish Crown's ethical, responsible and transparent handling of data and AI.

Danish Crown takes its responsibility as a data controller seriously, as we want to be perceived as a respected and competent company that complies with applicable legislation and follows developments in good data ethics.

1.2 AI and data ethics principles

At Danish Crown we have adopted a set of data ethics principles to support ethical decision-making when using data and AI in our company and throughout the value chain.

The AI and data ethics principles cover all types of data collected, analyzed, stored, shared, deleted and otherwise processed.

The principles draw on well-established concepts in privacy, human rights, AI, data and business ethics to ensure that we use data in a way that maximizes benefit and minimizes harm for individuals and society.

Our principles are as follows:

- Danish Crown must process data transparently and openly.
- Data processing must always comply with applicable national law and regulations.
- Data processing must be carried out in a sufficiently secure, robust and reliable manner that meets international best practice standards.
- Data must not be used in a way that could mislead our customers, employees, society, or other stakeholders.
- Data processing of data must not discriminate based on gender, ethnicity, sexuality, socio-economic background, disability, health-related data, or any other ground.

- Computer programs, algorithms, artificial intelligence and other technologies must be used fairly and responsibly.

1.3 Prohibited AI systems

The AI Act (Regulation (EU) 2024/1689) defines the following AI practices as strictly prohibited and these may not be developed, deployed, or used within Danish Crown:

- AI systems that use subliminal techniques to distort the behavior of a natural person.
- AI systems that exploit vulnerabilities of a natural person, due to their age, disability, social or economic situation.
- AI systems that use 'real-time' remote biometric identification.
- AI systems that infer the emotions of a natural person in the workplace, except for medical and safety reasons.

1.4 Use of high-risk AI systems

The AI Act (Regulation (EU) 2024/1689) defines high-risk AI systems that require additional safeguards and mitigation measures to minimize the risk of discrimination and bias.

The following types of AI systems are considered high risk within Danish Crown:

- AI systems used in human resources and recruitment for purposes such as, evaluating CV's, ranking candidates and assessing job performance.
- AI systems used to monitor critical infrastructure, such as food safety and food production lines.

For such high-risk AI systems Danish Crown must implement mitigation measures such as:

- An impact assessment that identifies potential risks of bias, discrimination and systemic error.
- Human oversight to monitor the evolution of AI and ensure that it does not evolve to create bias or discrimination.
- A risk assessment of the supplier's technical documentation, upon procurement.



1.5 Top tips to using AI in a compliant and legal manner

When using AI, you may unknowingly be at risk of violating copyright law, intellectual property rights of third parties, data protection law or compliance policies.

To avoid non-compliance, you must observe the following:

- DO NOT use personal data when prompting AI generated content. Otherwise, you risk sharing personal data with other companies, violating individuals' privacy.
- When using confidential information, ensure that the AI system does not train or learn from the confidential information provided by you.
- Be careful about sharing confidential information when prompting AI. You may risk violating our compliance policies, or our contractual obligations, by sharing data that is considered confidential. When using company data, make sure that you are using an authorized AI system.
- Do NOT ask the AI system to resemble or base its output on already known images, pictures, works, brands and similar, that are not owned by Danish Crown. Be careful that you do not use or publish AI-generated content that has a high degree of resemblance and likelihood to other images, pictures, works, brands and similar.
- Bear in mind that AI-generated content as a starting point is not protected by copyright law unless an exceptional high degree of human involvement is required. Please consult Group Legal in cases of doubt.
- When using AI in images, you must indicate that the image is created by AI if it depicts existing people, objects, places, entities or events and would mislead a person into believing it to be authentic.
- Use our authorized AI systems to minimize the risk of non-compliance. Ask Global IT if you are in doubt of what AI systems are authorized.
- Read the Danish Crowns AI guideline for more detailed information on how to avoid violating our policies and the rules when using AI.

1.6 Globally consistent high standards

This policy covers the entire Danish Crown Group and obliges all employees to follow Danish Crowns AI and data ethics principles. The policy reflects the need for globally consistent and high standards so that Danish Crown can demonstrate our commitment to conduct business in accordance with Danish Crown's values.

1.7 Data in Danish Crown

At Danish Crown we process personal data as a data controller. In our role as data controller, we process personal data from e.g., job applicants, employees, owners, and customers. In addition to personal data, we also process non-personal data such as financial, marketing, production, sales and sustainability data.

1.8 Responsibility

The overall responsibility for AI and Data Ethics rests with the Group Executive Management Team.

An AI and Data Ethics Committee, consisting of functional leaders within Legal, Finance and IT has been appointed to ensure implementation of and compliance with this policy.