Data Ethics Policy

Last updated: January 2026

Content

1. Introduction

DFDS is committed to protect any data collected when we conduct business. This could be personal data, or other sorts of data, pertaining to our customers, suppliers, business partners and employees. Our operation and connection with third parties is increasingly being powered by data and technology. Our ambition is to improve business value and increase efficiency, and usage of data is fundamental to achieve this goal. Therefore, it is crucial that we handle data with care and comply with all applicable laws and standards related to data, data privacy, and the ethical use of data.

To this extent, DFDS implemented our Data Ethics Policy in 2021. In 2024 we further strengthened our overall policy framework, with focus on expanding the description of what data we collect, how we use it, and the policies we have in place to ensure responsible handling and use of data. In the 2026 review we have added sections on AI and the EU AI act specifically.

This Data Ethics policy sets out the overall guidelines and principles for how data ethics are considered and included in the use of data, including personal data, and the design and implementation of technologies. Being a transport and logistics provider, we use data to maintain and improve our customer experience and our operational efficiency. We are committed to ensure that employees, customers, and business partners can entrust us with their data whether it being personal data or other business data. We are determined to handle this data in a sustainable manner and with great care. We recognise that digital development entails both responsibility and transparency.

This Data Ethics Policy supplements our Data Protection Policy and Privacy Notice which sets out the overall requirements for our handling of personal data, and our Information Security Policy and IT policies, which describes how we look after DFDS' data, including relevant security standards for data storage, access management, and safe IT usage.
The purpose of our Data Ethics Policy is to ensure a fair balance between, on the one hand, the many benefits that the use of data and new technology offers, and on the other hand, the consequences that the use of data can have for the individual, a business and for society in short and long term.

2. Scope

The Policy applies to all services, entities, and employees within the DFDS Group working with or planning to work with data.

3. Types of Data

DFDS process an array of data related to HR, customer data and interaction, and supplier contact, as well as production/operational data and marketing data. The data processing includes, but is not limited to, the following types of data:

- General personal data about our employees, customers, suppliers, and business partners.
- Information about which products and services our customers receive from us and how the customer uses them.
- Information about subcontractors, engaged by our customers (e.g. freight companies, drivers, etc.)
- We register our communication with the customer and record certain telephone conversations, e.g. regarding bookings.
- We register data points related to operational execution related to ships, trucks, warehouses, terminals etc. This data is used to optimize our internal efficiency but also to provide transparency towards our customers – e.g. how we together can help reduce their scope 3 emissions.
- Depending on the customer's own form of communication with us, sensitive information, including sensitive personal data may appear in the information received by us from the customer in an unstructured form. We do not use this data for any purpose, except when our customers need special assistance when receiving our services, and it is deleted when the processing purpose for which the information appears has been completed.

4. Our Core Principles of Data Ethics

We are committed to ensuring that employees, customers, and business partners can entrust us with their data. We are determined to handle data in a sustainable manner and with great care. We recognise that digital development entails both responsibility and transparency. We adhere to three principles of data ethics: Security, Confidentiality and Integrity.

4.1 Security

We assess risk, invest in new technology and establish organisational processes to mitigate and encounter global security threats. We continuously seek to improve our security measures and to grow our safety

culture throughout our business. We strive to be a reliable and responsible business and for us, security and safety are top priorities.

4.2 Confidentiality

We are dedicated to our Code of Conduct. We work to ensure that our employees are trained to care, and we work to ensure that employees are cared for. We abide by privacy laws and regulations. We respect privacy. We care for people.

4.3 Integrity

To us, integrity means engaging in ethical issues. We use artificial intelligence and other evolving technologies to improve internal processes and customer experience. We are open-minded and use new technologies with responsibility and transparency, and we desire to learn, develop, and improve every day. For AI specifically, we comply with the EU AI act.

5. Other Principles

5.1 Advanced analytics

We apply machine learning and optimisation algorithms to improve how we operate and serve our customers. These advanced solutions are used as decision support for our employees to improve decision making, with a focus on optimizing operational efficiency and improving the time to make decisions.

The risk of bias is always considered as in integral part of building and testing algorithms, to ensure that we do not introduce unfair biases into our solutions. We do not use any personal data to train algorithms and algorithm are not used to make any decisions that could potentially be discriminating towards any individuals.

5.2 Third party data processing

We never disclose information relating to employees, customers, suppliers, and business partners to others, unless this is permitted, required by law or under any other confidentiality agreement, or other agreement that imposes obligations of confidentiality obligations. Thus, we do not sell any personal data to third parties.

When we use third-party suppliers or outsourcing partners to perform functions that may give them access to personal data, including data storage, secure disposal, archiving, IT administration and office cleaning, we require that third parties who are acting as data processors enter into binding agreements that oblige them to comply with any applicable

regulation and policy regarding the processing of personal data. This includes not disclosing or selling personal data.

5.3 Compliance and training of employees

How we engage with each other and our customers in terms of trust, respect and equality has a big impact on our work environment and company culture. We prioritise that employees are well informed about data ethics, data security and the correct handling of personal data, including through cyber security, data protection and AI training in our onboarding program as well as ongoing training. This value is incorporated in the DFDS DNA as part of our Code of Conduct. The usage of data and personal data is in accordance with internal guidelines that, among other things, set the framework for authorisation and access control.

Much of our work depends on the gathering and handling of user data. It is therefore our employees' responsibility to safeguard individuals' privacy rights and comply with applicable laws, which is why data protection training is part of our onboarding programme. To ensure continued training, our employees are assigned to renew this training on an annual basis. As data protection in some manner will likely take part in an employee's daily work, the employees have access to informative and practical resources in the form of a library on our internal website where practical guidance on data protection is available.

6. Data Ethics Governance

As DFDS cares about its employees, customers and suppliers, compliance of relevant data protection laws is of utmost importance to DFDS. As such, DFDS has appointed a designated team with the purpose and task to support the DFDS Organization in all matters of data protection.

This designated team consists of several employees who daily works with data protection as well as other related areas. The team supports the organization with both externally and internally related matters. Just to mention some of the profiles who is part of this team, it consists of employees with skills in the field of IT Security, Data Governance, Privacy, Legal, GDPR, AI Act, HR, and Customer Relations. The designated team reports ultimately to DFDS's Chief Technology Officer and Executive Vice President of the Technology & Innovation Division.

As the DFDS Organization is vast and spreads across multiple countries and different services, the complexity of tracking data and processes across departments and business units is a complex task. As part of securing compliance, DFDS has invested in a data protection compliance platform whereby we have simplified and optimized our governance, risk, and compliance management. One of the functionalities of the platform is

to provide a complete overview and documentation of our processing activities when it comes to privacy and information security management. The platform is utilized by the designated team as well as relevant employees in other departments.

7. AI Policy & Use

The use of advanced solutions based on artificial intelligence (collectively referred to as "AI") has the potential to enhance DFDS efficiency and scalability.

AI can take various forms, including hardware, software, or any other innovative form. Based on massive amounts of data, these technologies make it possible to generate text, music, images, videos etc. in response to our user queries. AI can provide intelligent and effective solutions to various problems. From automated warehousing systems and AI Agent process automation, predictive analytics for demand forecasting and real-time shipment tracking, tailored shipping solutions and customized delivery options, dynamic route planning and fleet management systems to predictive maintenance for vehicles and risk assessment for cargo security.

In many ways, AI is ground-breaking. However, such technologies should be used with caution, and therefore, all employees of DFDS must commit themselves to adhere to this. Implementing AI also attracts certain risks such as breaches of privacy and confidentiality, decision-making biases, lack of transparency, job losses due to automation, increased dependence, and AI system failures. We are committed to addressing these risks through continued monitoring, timely upgrades, risk management strategies, and AI training.

When we, as employees in DFDS, use AI, we should always strive to be fair, honest and considerate – when in doubt consider our Codes of Conduct as guiding principles.

In DFDS we have introduced an AI Governance Board to support our organisation and ensure DFDS lives up to the EU AI Act. It is also the AI Governance Boards's role to provide oversight and strategic guidance to help the organisation make informed decisions about AI adoption and use.

7.1 Ethical Principles and Values when implementing AI

- **Respect for Privacy:** Our organization is committed to safeguarding data privacy and ensuring the confidentiality of our clients, employees, and stakeholders by complying with all local and international data protection laws.

- **Transparency:** We will ensure that our AI systems operate transparently. In alignment with current regulations, we need to be able to track how and why data is being used, offering clear documentation regarding our AI applications. This includes documenting the algorithms, data sources, and decision-making criteria used by AI systems

- **Accountability:** As part of continuous improvement, we need to be able to monitor the consequences and impacts of our AI systems, in order to ensure compliance with policies.

- **Security:** We pledge to prioritize the security of our AI systems to mitigate any potential risks associated with data breaches or cyber threats.

- **Fairness and Non-discrimination:** We commit to designing and deploying our AI systems in a manner that prevents biases and discrimination, ensuring equal treatment of all users.

- **Ethical and Legal Compliance:** The organization ensures that the development and use of AI technologies comply with ethical standards and legal regulations. This includes respecting the IPR of third-party AI technologies and avoiding infringement

7.2 Guidelines for how to use AI safely

AI output should be used in a manner that aligns with ethical standards, our Code of Conduct and company policies. This includes avoiding biases and ensuring fairness in decision-making processes. AI output must comply with data privacy and security regulations. Sensitive information should be protected, and access to AI-generated data should be controlled and monitored.

- **Use AI lawfully, ethically and responsibly:** The DFDS Code of Conduct extends to AI usage. So, if a DFDS employee is using any AI tool, remember not to input any information about DFDS you would not give a stranger on the street. DFDS employees are asked to always consult with their security team before using any embedded AI applications, extensions, or plugins.

- **Use only the vetted AI tools:** If a DFDS employee wants to interact with a GPT model, DFDS has an agreement with Microsoft to use their OpenAI model via AI Copilot. It has similar functionalities as other Chat GPT models in the market but with added security to safeguard interactions and DFDS data.

- **Use the AI tool as intended by the vendor or developer:** DFDS colleagues can refer to the internal AI Catalogue to check what has been built or secured, and if their needs are not cover by them, they

can reach out to the relevant T&I partner to scope together what are the possible solutions to adapt or acquire new solutions/tools.

- **Have meaningful human control at the right stage:** Ensure that humans retain real authority and informed oversight over AI systems at critical points in their lifecycle - especially where decisions are high-impact, irreversible, or ethically sensitive - so that humans can understand, intervene in, override, or halt the system when necessary.

8. Data Ethics Questions & Concerns

If you have any questions or concerns related to data ethics, please do not hesitate to reach out to one of the below policy owners:

- **Rune Frølund Keldsen** (EVP - CTO): rukel@dfds.com
- **Thomas Denager Rebeiz** (VP - Tribe Lead - Group Technology & Data): thodena@dfds.com

You are the key to an ethical environment at DFDS. If you witness or suspect a violation of the Data Ethics Policy, you are expected to raise your concern.

You can report the issue through different channels:

- Your direct manager or supervisor (Land) or Head of Department/Master (Sea)
- Your local HR Business Partner (Land) or Crewing Department (Sea)
- Any member of the Executive Management Team
- The DFDS Whistleblower line

You are advised to always speak with your supervisor or manager first unless the violation involves these individuals.

9. Roles & Responsibilities

9.1 The role of T&I

The Technology & Innovation(T&I) division is the designated owner of the Data Ethics Policy. T&I is responsible for ensuring the policy remains current and aligned with the latest developments in data ethics. Updates to the policy will be conducted annually, or more frequently if deemed necessary due to emerging regulation or ethical considerations. In updating the policy, the policy owners will draw upon resources from other business units including Group Sustainability, Legal, and other relevant stakeholders.

The policy owners are tasked with actively monitoring and tracking the latest issues within the realm of data ethics. This includes staying informed about evolving industry standards, legal requirements, and societal expectations related to data handling and privacy. In response to the dynamic nature of data ethics, T&I will adapt the company's approach to align with the most current ethical standards.

9.2 The role of employees working with data

It is the responsibility of every employee working with data to read, understand, and stay informed about the contents of the Data Ethics Policy. Regular review of the policy might be necessary to ensure ongoing compliance and understanding of ethical guidelines.

Employees are encouraged to actively participate in the enhancement of the Data Ethics Policy by providing feedback on potential ethical concerns or suggesting improvements.

Reporting any observed ethical lapses is crucial for maintaining a robust and continually improving ethical framework.

10. Approval

This policy has been reviewed and approved by:

Name: Rune F. Keldsen **Titel:** EVP, CTO **Date:** 21-01-2026

Signature: