Data Ethics Review 2025

DFDS A/S · Marmorvej 18 · DK-2100 Copenhagen Ø
+45 3342 3342 · dfds.com · CVR 14 19 47 11

Contents

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 the Data Ethics Policy in 2021. In 2023, the policy was revised to further strengthen our overall policy framework. In 2024 the update focused 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 2025 update we have added sections on AI and the EU AI act specifically.

The 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.

The 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.

Specific for customer and employee data

We collect, process and store large amounts of data, including personal data. Therefore, we are also aware of our significant data responsibility and trust that our use of data is done in a responsible manner. We want to be clear about the basis on which we use data and how we prioritise our data protection efforts.

For DFDS, it is essential that our employees, customers, and the outside world have great confidence in our ability to protect their data. Respect for the privacy of customers and employees is a fundamental value for DFDS, and we safeguard the right to privacy.

How we use data

In DFDS data enables us to enhance customer experience, strengthen operational performance, and support informed decision-making across our organisation.

We continue to ensure that all data is collected for clear and legitimate purposes and that processing is carried out lawfully, fairly, and with respect for the individuals concerned. We process only the data necessary to meet contractual obligations, comply with legal requirements, or pursue DFDS's legitimate interests. At the same time, we strive to ensure that the data we handle is adequate, relevant, and accurate. Personal data is retained only for as long as required for the specific purpose for which it was collected.

In line with our updated Data Ethics Policy, we also ensure that the use of data aligns with DFDS's broader governance framework, including our Privacy Notice, Data Protection Policy, Information Security

Types of data

DFDS process an array of data related to HR, customer 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:

→ *About our employees:* General personal data, e.g. name, address, contact information, data of birth, national identification number, gender, financial information such as bank details, qualifications and work experience, family status, image, business contact data, access card (ID) number, and other data collected by DFDS, including sensitive data about health.

→ *About our customers and suppliers:* General personal data, e.g. name, address, national identification number, financial information such as bank details and possibly company registration/VAT number, and confidential data, such as passport details and other identifying information

→ 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.

Policy, and the principles of security, confidentiality, and integrity.

Security

DFDS values data security. We consider it paramount that all data is processed in a safe and secure manner. Security measurements include technical as well as organisational and physical measurements. We continuously check that data security is sufficiently secure and robust and ensure that our employees receive the necessary training in cyber security and data protection.

We have implemented detailed processes and procedures to identify and manage the risk of information security breaches. Our IT security organisation assesses all cyber and data security incidents with a view to continuously optimising our data security.

Employees in the DFDS organisation are subject to a duty of confidentiality by contract of employment on all matters that they become aware of in the course of their employment. The duty of confidentiality also applies after the employment relationship has ended.

AI & Advanced analytics

We apply machine learning and optimisation technologies to enhance how we operate and support our customers. These advanced solutions continue to serve as decision-support tools for our employees, helping improve the speed and quality of operational decisions and strengthening overall efficiency. As in previous years, we carefully assess the risk of bias when developing and testing algorithms to ensure that we do not introduce unfair or unintended outcomes. We do not use personal data to train algorithms, and no automated system is allowed to make decisions that could be discriminatory or have significant consequences for individuals.

With the evolution of Generative AI, DFDS has strengthened its focus on awareness, responsible use, and safe implementation across the organisation. As part of the updated policy framework, we now follow the requirements of the EU AI Act and have introduced a dedicated AI Governance Board to provide oversight and ensure that AI is used transparently and ethically. Only vetted and secure tools may be used, including DFDS-approved AI solutions such as Microsoft's AI Copilot. We also maintain meaningful human oversight at critical points, ensuring that AI supports rather than replaces informed human judgement. These measures help ensure that our use of AI remains safe, fair, and aligned with DFDS's ethical standards and governance practices.

3rd party data processing

We never disclose information relating to employees, customers, suppliers, and business partners to others, unless this is permitted and 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.

Compliance and training of employee competences

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.

Governance and compliance

As DFDS cares about its employees, customers and suppliers, compliance with relevant data protection laws remains of utmost importance. To support this commitment, DFDS has appointed a designated team with the responsibility to assist the organisation in all matters related to data protection and ethical data use. This designated team consists of employees with specialised competencies within IT Security, Data Governance, Privacy, Legal, HR and Customer Relations, and—following the updated policy—expertise in GDPR and the EU AI Act. These skills enable the team to guide the organisation on both internal and external matters, including the responsible use of emerging technologies and alignment with DFDS's wider governance framework. The team ultimately reports to DFDS's Chief Technology Officer and Executive Vice President of the Technology & Innovation Division, reflecting the strategic importance of data protection in DFDS.

As the DFDS organisation is large and spread across multiple countries and business areas, tracking data and processes across departments remains a complex task. To strengthen governance, DFDS has invested in a comprehensive data protection compliance platform that simplifies and optimises governance, risk and compliance management. The platform provides an up-to-date overview of processing activities, supports documentation of privacy and information security requirements, and enables more efficient monitoring across the organisation. vested in a comprehensive data protection compliance platform that simplifies and optimises governance, risk and compliance management. The platform provides an up-to-date overview of processing activities, supports documentation of privacy and information security requirements, and enables more efficient monitoring across the organisation. It is used both by the designated team and relevant colleagues throughout the business to ensure consistent and reliable compliance practices.