

# Data Ethics Review 2023



## Contents

Introduction	3
Specific for customer and employee data	3
Types of data	3
How we use data	4
Security	4
Advanced analytics	4
3rd party data processing	4
Compliance and training of employee competences	4
Governance and compliance	4

## 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 2023, the policy was revised to further strengthen our overall policy framework. In this revision, we have 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.

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.

## 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 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.
  - Information about which products and services our customers receive from us and how the customer uses them.

## How we use data

The usage of data has become an indispensable discipline that improves society in a variety of ways. Being a transport and logistics provider, we use data to maintain and improve our customer experience and our operational efficiency.

We ensure that data is collected for specific and legitimate purposes and processed lawfully and fairly, including that the processing only includes data that is necessary to fulfil any contract, legal obligation, or our legitimate interest.

At the same time, we endeavour to ensure that the data collected is adequate, relevant, and accurate. Appointed DFDS employees responsible for data protection work to ensure that personal data is not stored for longer than necessary, that processing is carried out with respect for the privacy of the person concerned, and that stored data is protected against unauthorised destruction, alteration, or disclosure.

## 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.

## 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 an integral part of building and testing algorithms, to ensure that we don't introduce unfair biases into our solutions. We don't use any personal data to train algorithms

and algorithm are not used to make any decisions that could potentially be discriminating towards any individuals.

## 3<sup>rd</sup> 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 data, including 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 data, including 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 envi-

ronment 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 and data protection 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 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, 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.

