

## Data ethics statement 2026

This statement is prepared in accordance with §99d of the Danish Financial Statements Act and describes the actions NTG has taken and continues to take to ensure that personal and other categories of data are used in a responsible and sustainable manner within its business and supply chain.

### Background

In the transport and logistics industry, each day huge amounts of data are generated, for example through vehicle locator systems, transport management systems, and CCTV monitoring systems.

In the coming years the amount of data will further increase due to further automation of data streams and regulatory oversight arising from, for example, the European Union's Corporate Sustainability Due Diligence Directive.

Because this statement covers use of all data types, it complements NTG's Data Privacy policies which cover the principles of transparency and personal data minimization and protection set forth in the European Union's General Data Protection Regulation (GDPR).

### Types of data, usage, and security

Data is an essential aspect of arranging and monitoring transport for our customers, and of performing our role as an employer. Data can, for example, be related to individuals and third party organizations, but also to the control and management systems of our operations, such as freight forwarding management systems that process and respond in real time to data.

Personal data processed by NTG will typically involve our employees, job applicants, visitors to our premises and websites, customers and other business partners, and/or other third parties, including general personal data, but also user behaviour data. Personal data is obtained either directly from data subject or via third parties. Such processing complies with GDPR.

NTG is committed to ethical data practices and has policies in place to ensure that data is only used for the intended purposes, in accordance with applicable laws and ethical practices. Group IT oversees the decisions related to investments in new technologies and data use at the Group level.

Data security is essential for data privacy and protection. NTG continuously enhances its organizational and technical measures and procedures to ensure proper data management and prevent any unauthorized use or disclosure.

### Third party data policy

To ensure that suppliers handle data ethically, NTG requires its suppliers to comply with its Code of Conduct for Suppliers or to have a similar document that aligns with NTG's own Code of Conduct.

We vet third parties who act on behalf of NTG with government agencies, such as a third party providing Custom's handling services or an agent. This helps ensure that these third parties have a good reputation and handle data responsibly.

When transferring personal data to or from third parties, we utilize Data Processor Agreements to define roles and responsibilities between the data processor and the data controller. The agreements help ensure compliance with applicable privacy laws, protecting the confidentiality, integrity, and availability of personal data, and define the terms of data processing, including its scope and duration. They also establish clear liability and recourse actions in case of a breach or non-

compliance. Additionally, our supply chain management includes conducting GDPR audits and obtaining assurance reports, or equivalent evaluations via questionnaires, to verify that third parties consistently adhere to the agreement and other contractual duties while handling our data.

We do not resell personal data but if legally required, we provide data in accordance with applicable laws, court orders, or authority decisions.

#### Artificial intelligence systems and their applications

We use artificial intelligence (AI) and machine learning (ML) to improve our services, and to optimize our operations and internal processes. We ensure that the data used is accurate, updated, complete, and that the technology we use does not produce discriminatory or biased results. We only make use of AI/ML in business processes and do not make automated decisions in our processing of personal data of employees or third parties.

#### Data ethics awareness among employees

We have implemented a Group-wide online cyber awareness training program for our employees. The program aims to improve employee behaviour and to protect against common data and privacy threats, such as phishing and data theft. We monitor how many employees have completed the online training and we expect them to avoid data and privacy risks and to report any potential unethical use of data or potential data privacy breaches to their managers or through our whistleblower system.

#### ISO/EIC 27001:2022 and CIS Critical Security Controls compliance and certification

Our data and information protection is anchored in internationally recognised cyber – and information security standards, ISO/EIC 27001:2022 and CIS Critical Security Controls. These frameworks are fully implemented across our Group organisation and form the foundation of our structured, risk-based approach to information security and data protection.

We are certified to ISO/IEC 27001:2022, confirming that we that we operate a robust and continuously maintained Information Security Management System (ISMS). Through systematic risk management, defined controls, and ongoing monitoring and improvement, we ensure the confidentiality, integrity and availability of data and information.

As part of our annual ISMS activities, we maintain a formal Data and Information Classification Policy and control supported by structured data classification processes and information labelling requirements. Information assets are classified based on sensitivity and business impact, and classification levels govern how data is accessed, stored and transmitted, and retained.

We also enforce an Acceptable Use Policy (AUP) for all employees to read and acknowledge. The policy defines responsible handling of data and information, and IT resources across our Group organisation.

Lastly, as part of our annual activities, we conduct training and awareness for all employees to understand data classification principles, labelling requirements, and responsible data handling.

#### Next steps

We will continue to enhance our knowledge of how data and artificial intelligence systems impact the transport and logistics sector and we will collaborate with our stakeholders to implement best practices regarding data ethics.