NORTHERN DATA GROUP

Supplier Code of Conduct

Version 2, 20.01.2026

Table of contents

Introduction

At Northern Data Group (hereinafter “Group” or “Northern Data”), we are committed to upholding the highest standards of ethical conduct, environmental sustainability, and social responsibility across our global operations. As a leader in cloud services and data center solutions, we recognize that our suppliers play a critical role in helping us achieve these objectives.

This Supplier Code of Conduct (hereinafter “Code”) outlines the expectations we have for our suppliers, vendors, contractors, and other partners. It reflects our dedication to ensuring that our supply chain operates in a manner that aligns with the following values:

- Respect of human rights,
- Protection of the environment, and
- Commitment to fair, transparent, and sustainable business practices.

The Global Procurement team is responsible for ensuring that all suppliers are aware of this Code, and suppliers must ensure full compliance with it.

We expect all suppliers to adhere to these principles, ensuring compliance with applicable laws, regulations, and industry standards while fostering a culture of integrity, innovation, and sustainability. By collaboration with suppliers who share our commitment to ethical practices, we aim to build long-lasting relationships that contribute to mutual success, drive positive change, and support global sustainability initiatives.

Failure to comply with the Supplier Code may result in disqualification as a Group supplier, constitute a material breach of contract, and could lead to termination of contracts and exclusion from future business with the Group.

We also expect our suppliers to ensure that all subcontractors in their supply chains are equally compliant with our Supplier Code.

Suppliers are obligated to report to Group any (suspected) violation of this Supplier Code, any law, or any regulation, including those relating to unethical behavior, human rights, and environmental issues, as soon as they become aware. Reports can be made confidentially and, if desired, anonymously by using our Whistleblowing System (see section “Reporting Channel”).

We thank you for your partnership and commitment to meeting the expectations outlined in this Code, which are essential to maintaining a responsible, resilient, and innovative global supply chain.

1. Compliance with Laws, Rules, and Regulations

1.1 Bribery and Corruption

Northern Data maintains a zero-tolerance policy towards bribery and corruption in all forms. Suppliers must not engage in, authorize, or offer any bribes, kickbacks, or improper payments – whether in cash or any other form of value – to any individual or entity. This includes government officials, employees, or representatives of public or international organizations, as well as private sector entities, with the intent of securing or retaining business or influencing any favorable business decision related to Northern Data.

This prohibition includes not only direct actions but also indirect facilitation, such as routing funds or benefits through third parties to improperly influence public officials or private entities.

Suppliers are expected to comply fully with all applicable anti-bribery and anti-corruption laws, including the German Criminal Code, the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, EU Anti-Corruption Directives, and relevant local regulations.

1.2 Anti-Money Laundering

Suppliers are required to comply with all relevant anti-money laundering laws and regulations. They must implement due diligence procedures to identify and report suspicious transactions and ensure that their operations cannot be used, intentionally or unintentionally, to facilitate money laundering or terrorism financing. It is strictly prohibited for suppliers to engage in any activities or with any entities that could potentially involve Northern Data in money-laundering schemes.

1.3 Antitrust and Fair Competition

Antitrust and competition laws are designed to protect consumers and competitors against unfair business practices and promote and protect healthy competition. Northern Data is fully committed to adhering to all applicable antitrust and competition laws across the jurisdictions in which we operate, and we expect our suppliers to uphold these standards as well. While competition laws may vary by country, they universally prohibit agreements or actions that unfairly restrict trade, mislead or deceive, or reduce competition in ways that harm consumers without delivering clear benefits. Any behavior that undermines fair competition - including price-fixing, market allocation, bid-rigging, or other anti-competitive practices - is strictly against the principles and ethical standards of Northern Data. Suppliers must ensure full compliance with these laws, supporting open and fair competition in all markets.

1.4 Securities and Insider Trading

Northern Data expects suppliers to comply with applicable insider trading and securities laws governing transactions in relation to the securities of the Group. Suppliers and their employees, contractors, and agents are prohibited from using material or non-public information obtained through their business relationship with the Group as a basis for trading in securities.

Material information refers to any information that a reasonable investor would deem important when making decisions to buy, hold, or

sell securities. This may include, but is not limited to, financial performance and key business metrics, details regarding mergers, acquisitions, or divestitures, news of the award or cancellation of major contracts, changes in senior leadership, projections of unexpected financial results, significant legal proceedings, or the gain or loss of a major customer or supplier. Such information can have a substantial impact on an investor's judgment and must be handled with the highest degree of care and confidentiality. These restrictions also apply to family members, friends, and associates of suppliers.

1.5 Export Control and Trade Sanctions

Suppliers must not provide Northern Data with products or services that originate from, or are manufactured in, countries subject to import and export controls or sanctions, including, but not limited to, those imposed by the United States, the European Union, and Germany. Suppliers are responsible for ensuring compliance with these laws and should refer to the official current sanctioned party lists published by the respective authorities (EU, OFAC, UN). Suppliers must ensure that the products and services provided to Northern Data do not involve entities or individuals subject to transaction prohibitions under applicable export control and sanctions laws. This includes compliance with any relevant sanctioned party lists, such as the European Union Consolidated Sanctions List, the U.S. Specially Designated Nationals (SDN) List, the U.S. Denied Persons List, the Bureau of Industry and Security (BIS) Entity List, and the United Nations Security Council Sanctions List.

1.6 Conflicts of Interest

While performing work for Northern Data, suppliers must exercise due care and diligence to avoid any actions or circumstances that could create, or appear to create, a conflict of interest. A potential conflict of interest occurs when a supplier's personal or financial interests clash with, or could be perceived as clashing with, the interests of Northern Data. Suppliers are expected to proactively manage and disclose any situations that may compromise their objectivity or the integrity of their business relationship with Northern Data. Suppliers are expected to proactively manage and immediately disclose any situations that may compromise their objectivity or the integrity of their business relationship with the Group. This is particularly important when a supplier is working for a prospective customer, supplier, or competitor, or if their business activities may conflict with those of Northern Data. It also includes situations where there is a conflict between our company‘s interests and the supplier‘s personal interests or those of their close relatives, friends, or associates. Any potential conflict of interest must be disclosed to the supplier‘s contractual representative at Northern Data or the Global Procurement team and approved in advance of performing any contracted work. This disclosure ensures transparency and allows for appropriate review and disposition of the situation.

1.7 Offering and Accepting Anything of Value

Suppliers must not offer, promise, give, or receive anything of value to improperly influence decisions or actions related to Northern Data. This applies to all Northern Data employees and anyone acting on its behalf. Offering gifts, money, or other benefits may create

conflicts of interest or appear to compromise integrity and independence. Suppliers are strongly discouraged from offering benefits to Northern Data employees. If any benefit is offered, it must be reasonable, lawful, and not perceived as a bribe or improper inducement. It is strictly prohibited for suppliers to offer, and for any Northern Data employee to accept, any gifts, entertainment, or favors (including, but not limited to, tickets to sporting events) during a tendering process, as these actions are expressly forbidden and must not be used to influence tender outcomes or award decisions. Cash, gift cards, or special discounts for Northern Data employees are strictly prohibited unless extended to all employees under the same terms. All actions must comply with local laws and company policies.

1.8 Financial Integrity

Accurate and reliable financial and business records are essential for Northern Data to meet its financial, legal, and operational obligations. Suppliers must ensure that all entries in any accounting books or records related to Northern Data are truthful and accurate, with no falsifications or misrepresentations for any reason. Furthermore, suppliers are required to retain all business records in compliance with their record retention policies and in strict accordance with applicable laws and regulations.

2. Labor and Human Rights Standards

2.1 Child Labor

Child labor is strictly prohibited at every stage of the supply chain. Child labor is defined as employing individuals under the minimum age of 15, as set by the International Labor Organization (ILO Convention No. 138). Suppliers must ensure that no child labor is used in their operations or their supply chain. If local laws applicable to the supplier or its supply chain set a higher minimum working age, the higher standard must be followed.

Suppliers are required to implement robust mechanisms to verify the age of their employees. Legitimate apprenticeship programs that comply with all relevant laws and regulations are supported, but young workers must not be assigned tasks that are mentally, physically, socially, or morally harmful, nor should they be required to work night shifts. Suppliers must also ensure proper management of student workers, maintaining accurate student records, conducting due diligence on educational partners, and safeguarding student rights in compliance with applicable laws and regulations.

2.2 Forced Labor, Human Trafficking and Modern Slavery

Suppliers must not engage in any form of modern slavery, including forced, bonded, or indentured labor as described in the International Labor Organisation (ILO Convention No. 29). All work must be voluntary, with employees free to resign or be terminated with reasonable

notice. Suppliers must not restrict worker freedoms, such as by withholding personal documents or limiting movement, nor should they impose illegal fees or deductions during recruitment or employment. Participation in human trafficking, slave labor, or prison labor is strictly prohibited across the entire supply chain. No employee, including migrant workers and their families, should be coerced into employment through threats of denunciation to authorities. Suppliers are expected to take all reasonable measures to ensure that their supply chains are free from practices that constitute modern slavery. Suppliers are obligated to educate and train their employees about prohibited trafficking activities and implement disciplinary measures for those found to have engaged in such activities.

2.3 Hiring and Employment Practices

Suppliers must verify workers‘ legal right to work in the country and ensure all mandatory documents, such as work permits, are available. Northern Data suppliers must provide equal opportunity for all workers, including the rights to freedom of association and collective bargaining.

2.4 Non-Discrimination

It is the responsibility of suppliers to foster a respectful recruitment process and an ongoing work environment free from harassment or discrimination, while recognizing diversity and inclusion in accordance with EU Anti-Discrimination Directives. Equal employment opportunities should be provided regardless of culture, race, color, religion, gender, age, national origin, disability, marital status, sexual orientation, ethnicity, pregnancy, political affiliation, or any other protected characteristic under applicable laws. Effective grievance mechanisms should be implemented to allow employees to voice concerns without fear of retaliation.

2.5 Humane Treatment

No worker shall be subjected to harsh or inhumane treatment, including any violence, gender-based violence, sexual harassment, sexual abuse, corporal punishment, mental or physical coercion, bullying, public shaming, or verbal abuse. Furthermore, there shall be no threat of such treatment. Disciplinary policies and procedures must be clearly defined and communicated to workers.

2.6 Working Hours and Benefits

Suppliers must ensure that working hours comply with all applicable laws while providing fair compensation and humane working conditions. Workweeks must comply with local legal limits and the International Labor Organization (ILO) Standards (ILO Convention No. 1). In any case, workweeks should not exceed 60 hours, including overtime, which must always be voluntary. Exceptions are permitted only in emergencies or exceptional circumstances. Employees are entitled to at least one day off in every seven-day period, in accordance with ILO Convention No. 14. Overtime must be compensated at rates defined by law or industry standards. Transparency in pay structures should be communicated clearly upon onboarding.

2.7 Freedom of Association

Suppliers must respect employees‘ rights to freely associate, as stated in the International Covenant on Civil Political Right (ICCPR),

Article 22, including the right to join or refrain from joining labor unions, seek representation, or participate in workers‘ councils, in accordance with local laws. Employees should be able to engage in open communication with management about workplace conditions without fear of retaliation, intimidation, or harassment.

3. Health and Safety

3.1 Occupational Safety

All workers must be identified, assessed, and mitigated for potential exposure to health and safety hazards. These include electrical and other energy sources, fire, vehicles, chemical, and fall hazards. The hierarchy of controls must be used to eliminate the hazard, substitute processes or materials, control through proper design, implement engineering and administrative controls, implement preventative maintenance and safe work procedures (including lockout/tagout), and provide ongoing occupational health and safety training. If these measures are insufficient, workers must be provided with appropriate personal protective equipment and educational materials about the risks associated with these hazards. At Northern Data, we expect as a minimum standard that our suppliers‘ management actively encourage workers to raise any safety concerns. Reasonable steps must be taken to remove pregnant women and nursing mothers from working conditions with high hazards. Furthermore, any workplace health and safety risks to pregnant women and nursing mothers, including those associated with their work assignments, must be removed or reduced. Finally, reasonable accommodations for nursing mothers must be provided.

3.2 Emergency Preparedness

Potential emergency situations and events must be identified and assessed, and their impact minimized by implementing emergency

plans and response procedures. These include emergency reporting, employee notification and evacuation procedures, worker training, and drills. Emergency drills must be executed at least annually or as required by local law, whichever is more stringent. Emergency plans must also include appropriate fire detection and suppression equipment, clear and unobstructed egress, adequate exit facilities, contact information for emergency responders, and recovery plans. Such plans and procedures must focus on minimizing harm to life, the environment and property.

4. Environmental Responsibility and Sustainabilit

Northern Data is fully committed to protecting the environment. Our suppliers must share our commitment and integrate proactive practices to minimize their environmental impact and waste. In line with the OECD Guidelines for Multinational Enterprises, suppliers must consider the full lifecycle of products or services, actively manage risks across their operations, products and supply chain, and work for continuous improvement. Our suppliers must work with us to be good stewards of the environment. They must operate in a manner that actively manages risk, conserves natural resources, and protects the environment, including with applicable chemical regulations such as EU REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) and POPs (Persistent Organic Pollutants), where relevant. Our suppliers must establish and apply a systematic approach to managing environmental issues, aligning with the OECD‘s recommendations on environmental management systems. This approach must address potential risks from regulatory non-compliance, reputational loss and opportunities for business growth through operational and product stewardship.

5. Protection and Security of Digital Resources and Technologies

5.1 Data Protection & Information Security

Suppliers are required to protect confidential and proprietary information, including personal data, from unauthorized access, destruction, use, modification, and disclosure. This protection must be implemented through appropriate physical and electronic security measures.

Suppliers must:

- Adhere to all applicable data and technology laws, including but not limited to data protection laws (e.g. the EU's General Data Protection Regulations (GDPR), EU Data Act and the California Consumer Privacy Act (CCPA)) and cybersecurity laws (e.g. NIS2 Directive and implementing regulations in the EU, data breach notification laws in the US, etc).
- Train their employees on information security and data protection best practices, and
- Conduct regular security audits and risk assessments.

In the event of any unauthorized use of assets, potential unauthorized access, or compromise of systems or data, suppliers must immediately notify the Northern Data Group in line with contractual requirements. Prompt reporting allows for swift action to mitigate potential risks and damages.

5.2 Intellectual Property

We expect our suppliers to respect and comply with all relevant laws concerning intellectual property rights, including patents, copyrights, trademarks, and protection against intellectual property disclosure. Suppliers must safeguard the intellectual property rights of all parties by exclusively using lawfully acquired and licensed information technology and software. Furthermore, they are obligated to use such software, hardware, and content strictly in accordance with the terms outlined in their associated licenses or usage agreements. This commitment to intellectual property protection extends to all aspects of the supplier‘s operations and interactions with Northern Data and other entities.

5.3 Cyber Security

Suppliers shall implement robust measures to safeguard and protect all information and assets entrusted to them. This protection must be comprehensive, guarding against cyber intrusions, unauthorized access, use, modification, disclosure, or destruction. It is the supplier‘s responsibility to ensure that all data and systems related to Northern Data ,s operations are secure and protected from potential cyber threats or breaches.

Suppliers must implement controls consistent with NIS2 requirements where applicable, or follow equivalent internationally recognized cybersecurity standards, including:

- Incident reporting to Northern Data within 24 hours (early warning)
- Supply-chain cybersecurity controls to ensure subcontractors follow appropriate cybersecurity measures
- Multi-factor authentication
- Secure encryption standards
- Secure software development methodologies
- Documented security policies, risk assessments, and continuous monitoring of systems

5.4 Artificial Intelligence Ethics

If Northern Data is supplied with software containing embedded AI capabilities, these capabilities must comply with all relevant local laws governing ethical and responsible AI. Suppliers must ensure that any AI systems provided to Northern Data comply with the EU Artificial Intelligence Act (Regulation (EU) 2024/1689). This includes risk classification (Prohibited, High-Risk, Limited-Risk, Minimal-Risk) with examples, conformity assessments for high-risk AI systems, transparency obligations for AI systems interacting with humans, and prohibition of manipulative or exploitative AI practices

Suppliers are required to commit to ethical practices in artificial intelligence when developing or deploying AI solutions. This commitment must include:

- **Transparency:** ensuring that AI decision-making processes are clear and understandable
- **Fairness:** addressing bias and fostering equitable outcomes for diverse user groups
- **Accountability:** accepting responsibility for the actions and consequences of AI systems
- **Privacy protection:** safeguarding personal data involved in AI applications
- **Social responsibility:** considering the wider societal impacts of AI technologies.

In the absence of applicable local laws, suppliers should have a documented AI policy based on recognized international guidelines, such as the EU AI Act, the Institute of Electrical and Electronics Engineers (IEEE), the Organization for Economic Co-operation and Development (OECD), or the Council of Europe.

6. Reporting Channel

Prevention is best; however, if something does go wrong, we count on you to “Speak Up”. If something doesn’t feel right, look right, or sound right, it probably is not right. We expect you to report any suspected violation of this Supplier Code, as well as any breach of laws or regulations, including those related to improper conduct, human rights, or environmental concerns, as soon as you become aware of it. Reports can be made confidentially and, if preferred, anonymously through our Whistleblowing System at any time on our website. We understand that reporting an issue requires courage. Northern Data has a zero-tolerance policy for any form of retaliation against individuals who raise concerns in good faith. Likewise, we do not tolerate personal attacks or false accusations directed at any individual.