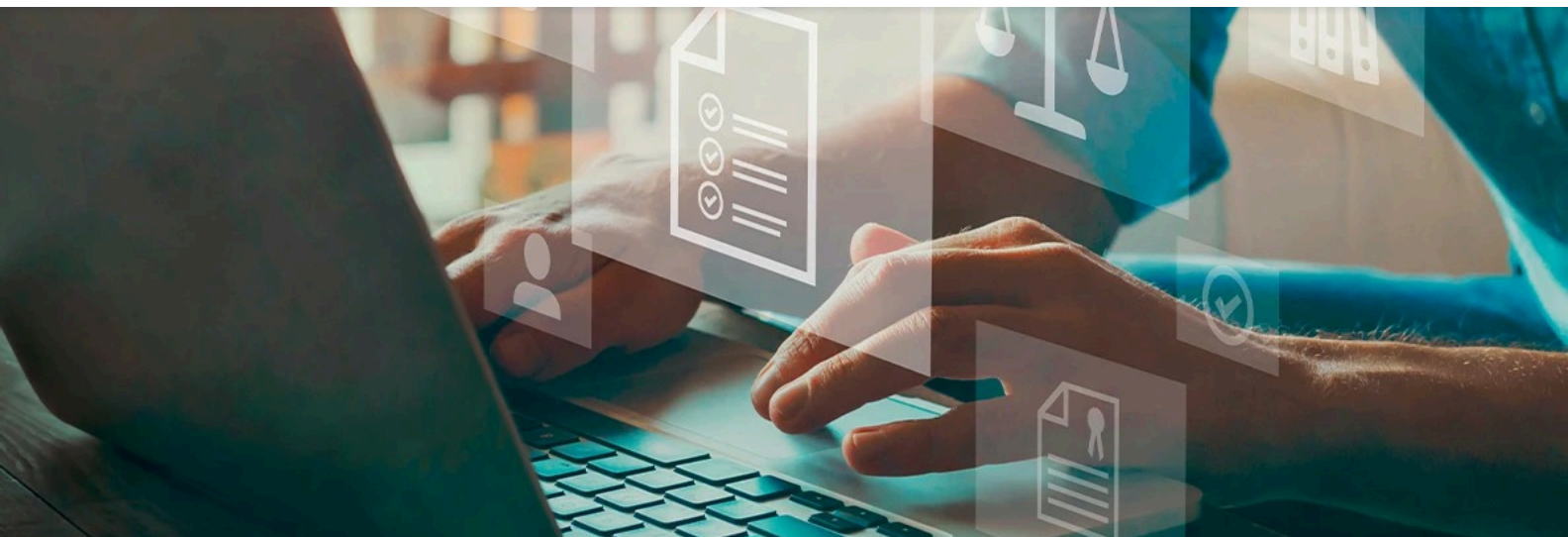




Compliance and Responsibility

17	Compliance Management System
18	Whistleblower System and Reporting Channels
19	Training
20	Compliance Auditing for Business Partners
21	Periodic Risk Analysis
21	Data Protection and Information Security

With its company values of integrity, collaboration, courage, and excellence and the principles of the Group-wide [KION Group Code of Compliance](#) (KGCC), KION is responding to the demanding expectations of the capital market, customers, employees, and other stakeholders.

As part of KION, STILL shares these values and is committed to ensuring complete compliance with all legislation, regulations, and codes of conduct. The comprehensive compliance management system of STILL is based on the KGCC, which sets out guidelines for ethical, value-driven, and lawful business conduct.

The KGCC also provides a binding framework for interactions between colleagues, as well as with customers, business partners, and the public.

As a German business, KION GROUP AG is primarily subject to German law. At the same time, KION must comply with any national legislation in force at its sites around the world. In cases where national law differs from German law, the KGCC defines the appropriate course of action. The Group's compliance and legal departments are also available as the designated point of contact for all legal questions. The KGCC is published in 24 languages and is updated as necessary – including with topics and new priorities – in order to best reflect the prevailing legal and business situation. External parties can view the KGCC on the KION website.

Compliance Management System

The compliance management system is continually reviewed and refined to ensure it remains fit for purpose. It is based on the IDW PS 980 auditing standard developed by the Institute of Public Auditors in Germany (IDW). Under the system, the Group audit department conducts regular audits and ad-hoc checks to ensure that compliance standards are being upheld across the KION GROUP AG and its consolidated subsidiaries.

The Group is explicitly committed to combating all forms of bribery and corruption. To this end, KION pursues a prevent-detect-respond approach with the ongoing objective of preventing misconduct, identifying it, and addressing it promptly with appropriate countermeasures.

In addition to the rules of conduct and anti-corruption provisions of the KGCC, further detailed requirements can be found in topic-specific guidelines. These include the anti-bribery and anti-corruption policy, the policy on avoiding conflicts of interest, and the donations and sponsorship policy.

In the reporting year, no confirmed cases of bribery or corruption were identified.

Number of Confirmed Corruption Cases in 2025

0

2024: 0, 2023: 0



Whistleblower System and Reporting Channels

Reports of actual or suspected unlawful or inappropriate behavior can be submitted in various ways – in person, by telephone, by mail, by email, or via an online form. All employees – as well as external stakeholders – have the opportunity to report potential compliance violations around the clock, including anonymously if they so wish. For this purpose, a [whistleblower tool](#) and a hotline operated by an external provider are available, which allow contact to be made in writing or by telephone.

The whistleblower system is designed on a global basis, but is adapted to local circumstances as far as possible. The integrated case management system is designed to ensure that all incoming information is reviewed and that each individual case is processed systematically in line with the provisions in the EU Whistleblowing Directive. The system guarantees confidentiality and protection against retaliation.

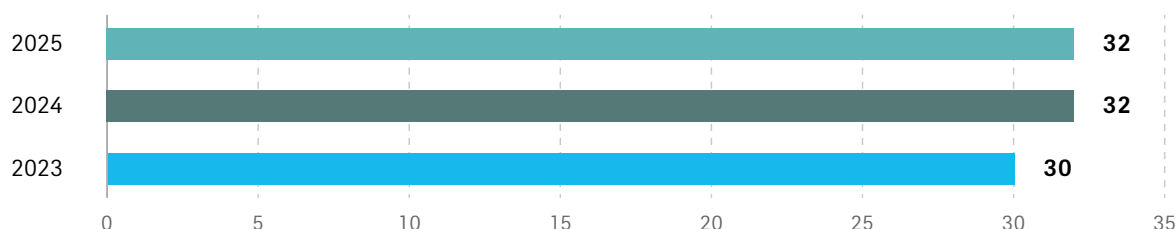
The KION Compliance Committee is a cross-functional body made up of managers from the Corporate Compliance, Internal Audit, and Legal departments. This committee oversees the processing of reports of potential breaches and related investigations and confers on sanctions in the case of identified compliance violations.

The Compliance Committee at STILL in Germany provides employees with another independent point of contact that they can turn to when seeking advice or reporting potential violations. Anyone that experiences or observes any form of discrimination or harassment can report this behavior to their designated committee – including in complete confidence. Similar contact points are also available at sites across the EMEA region in line with relevant national regulations. Compliance representatives are in place in all countries where STILL operates and can be contacted at any time.

To encourage use of the whistleblowing system, employees are regularly updated about the various reporting channels via the intranet and mandatory compliance training.

All reported suspected cases are systematically reviewed. Investigations are initiated if the information is deemed credible. Disciplinary action is taken in all cases where misconduct is identified. If necessary, the compliance management system is also updated to prevent further breaches in future.

Number of Reports Submitted via Whistleblower System



Training

In addition to clear compliance policies, STILL also offers extensive information, advice, and training. The compliance officers and representatives of STILL work hard to ensure that the company's staff are kept fully up to date at all times about compliance matters and understand the importance of upholding the company's values. On joining KION, all new employees are required to complete mandatory training in the [KION Group Code of Compliance](#), either online or in person in the case of staff without access to a work PC. Employees who are exposed to particular compliance risks due to their role, including sales and procurement staff, also attend regular in-person training sessions on specific topics.

Training Provided on Topics Relating to Business Ethics

- Classroom training (KION Group Code of Compliance, anti-corruption, anti-discrimination, conflicts of interest, data protection, whistleblower protection, speak-up culture)
- E-learning course: KION Group Code of Compliance
- E-learning course: Avoiding Corruption in KION – the General Principles of the ABC Policy
- E-learning course: Professional Conduct at KION – Promoting a Respectful Working Environment
- E-learning course: Preventing Money Laundering and Fraud at KION
- E-learning course: Avoiding Conflicts of Interest at KION
- E-learning course: KION – Preventing Anti-Competitive Practice
- E-learning course: General Data Protection
- E-learning course: Information Security Employee Awareness Training
- E-learning course: Role of Unconscious Bias in the Workplace
- E-learning course: Speak up – We're Listening

The aim is to provide all KION employees with regular training on the most important topics (anti-corruption, avoiding conflicts of interest, antitrust and competition law, anti-money laundering, whistleblower protection, data protection, IT security/information security, and human rights). Changes to legislation or internal regulations are incorporated into the training courses, as are further insights from the Compliance Management System.

Percentage of Total Workforce that Received Training on Topics Relating to Business Ethics

2025	2024	2023
77%	91%	79%

Compliance Auditing for Business Partners

Before KION enters into a new business relationship, external business partners must be audited and relevant documentation secured. The audit process establishes and verifies the financial background of the potential business partner and identifies any arguments against entering into a business relationship, e.g., the business appears on a sanction list or is the subject of negative reporting. If doubts arise, the Group may decide not to enter into a business relationship with this partner. External partner audits at KION are, wherever possible, conducted on the basis of a risk assessment.

The basic audit is conducted using the business partner tool, which is maintained by Corporate Compliance and designed to check customers and suppliers against compliance watch lists. Corporate Compliance is responsible for running these checks, assessing the results, and taking any necessary action. For external sales partners where the potential for corruption is higher – such as dealers, importers, distributors, agents, and integrators – the responsible compliance officer will conduct a multi-stage due diligence assessment prior to commencing a new business relationship. In addition to identifying potential risks in the relevant country based on subindices from reputable international organizations, this assessment obtains information from the sales partners via due diligence questionnaires, through audits conducted using the business partner tool, and/or via external due diligence providers. The results of the due diligence assessment are subsequently communicated to the responsible teams – e.g., the Management Board – along with any recommended actions, such as tighter contractual terms including a right to audit clause and additional monitoring of payment streams.

Percentage of High-Risk Business Partners Subject to a Due Diligence Process with Regard to Corruption in 2025

100%

2024: 100%, 2023: 100%



Periodic Risk Analysis

KION conducts an annual systematic risk analysis to identify and evaluate corruption and bribery risks throughout the Group. Money laundering, tax compliance, cyber security, and human rights risks are also assessed, as are the risks of non-compliance with competition laws. Non-financial risks that arise on an ongoing basis are also screened, evaluated, and managed. Based on the results of this analysis, the Group devises suitable actions to eliminate any weaknesses in the relevant processes and control mechanisms. Key factors used in the risk analysis include the corruption perception index for the respective country, the size and structure of the local procurement or sales organization, and any contacts with public officials.

Percentage of Sites Where an Internal Audit or Risk Assessment Related to Business Ethics Was Conducted in 2025

100%

2024: 100%, 2023: 100%



Data Protection and Information Security

Data protection and information security are both top priorities at STILL and are governed by policies that apply to the whole of KION. While the Data Protection Policy regulates technical and organizational measures to protect personal data, the Information Security Policy ensures the confidentiality, integrity, and availability of information and thus protects KION against related attacks. There are also a series of Group-wide operating agreements and mandatory standards in place covering topics such as IT security in the workplace and the management of IT systems, email, and internet usage. Samples and templates to facilitate the day-to-day handling of personal data and sensitive business information are also available. The Operating Units are each responsible for implementing the central requirements of these policies and standards. Staff members responsible for data protection and the coordination of data protection activities in the individual subsidiaries report to their respective senior management team. At Group level, the Group Data Protection Officer reports to the Chief Compliance Officer, and the Chief Information Security Officer of KION reports to the Chief Information Officer, who reports to the Executive Board of KION GROUP AG.

Protecting sensitive personal data is an important responsibility, so secure and effective processes and systems have therefore been put in place to protect this information and ensure compliance with the relevant legislation. All staff are given training and receive regular updates via the Group intranet to ensure that they understand and remain up to date with basic data protection principles, their reporting obligations, and the Group-wide compliance reporting system.

The number of attacks on companies' global IT infrastructure has increased significantly due to organized crime and industrial espionage. Various technical and organizational measures have been implemented with the aim of protecting the data of KION from unauthorized access, misuse, and loss. This includes continuously checking for vulnerabilities in the entire IT and operational technology infrastructure. Regular training on IT security issues, global anti-phishing campaigns, a monthly video series published on the Group intranet, and protection guidelines for the IT infrastructure also contribute to IT security.

Information Security Management System

The Information Security Management System (ISMS) of KION is designed to ensure that sensitive information remains protected. The ISMS is based on the standards set out in ISO 27001 (for the establishment, implementation, maintenance, and continuous improvement of documented information security management processes) and applies across the Group. A documentation policy describes the requirements for information security.

KION regularly analyzes potential or existing threats to its information security. Where these risk analyses identify an IT security risk or deviation from KION security standards, the risk is described and appropriate courses of action are defined. The residual risk is also assessed and, on this basis, the risk owner decides whether or not to accept this risk. Residual risks continue to be reassessed on a regular basis and the decision to accept them reaffirmed. The Group audit department conducts regular IT audits, including information security checks.

The KION divisions that develop and operate the cloud-based fleet management systems are certified in accordance with ISO 27001. At STILL, this applies to STILL GmbH in Hamburg. The KION headquarters in Frankfurt am Main, the STILL headquarters including production site in Hamburg, and the STILL branches in Hamburg, Berlin, and Hanover are certified according to the TISAX® standard. TISAX® is a cross-company assessment and exchange mechanism for information security in the automotive industry. It is designed to ensure the security, integrity, and availability of data required for manufacturing processes and vehicle operations. As part of the assessment, various safeguards were demonstrated, such as information security standards, standard operating procedures, security concepts, and key performance indicators.

In preparation for the NIS 2 Directive (Network and Information Security Directive 2), additional locations and companies were brought into the scope of the ISMS. Furthermore, the focus is now also on maintaining the high level of information security that has been established and on the smooth functioning of the system's components in day-to-day operations. Among other things, this includes regular internal audits and checks, information security risk management, the planning and implementation of improvements, regular assessment of the information security of service providers and suppliers, as well as other measures.

Number of Confirmed Information Security Incidents in 2025

0

2024: 0, 2023: 1

