Governance

Governance, compliance and ethical principles – data protection and information security – human rights and sustainable supply chain management

We align our actions with legal requirements, take data sovereignty into account, and integrate human rights and sustainability standards into our procurement processes.

Total number of corruption cases in 2025:

0

Fines or other sanctions due to data protection breaches or security incidents in 2025:

0

Review of all potential high-risk suppliers using self-assessments on ESG aspects:

100%

Governance, compliance and ethical principles

We act in accordance with all applicable laws, social guidelines and our values.

Strategy

Reliability, integrity, and transparency form the basis of our actions

Responsible corporate governance is our guiding principle – our governance provides the framework for acting responsibly, sustainably, and in line with our values. Sustainability is firmly anchored in all business areas; guidelines and control mechanisms ensure **integrity, reliability, and transparency**. They ensure that environmental, social, and compliance standards are systematically integrated into management processes, provide clear guidance for all employees, and establish binding rules.

We act **ethically and in accordance with the law**. We consistently prevent corruption and unfair business practices, maintain the integrity of the corporate culture at O_2 Telefónica, and ensure the implementation of data protection and compliance standards. In doing so, we protect our reputation, the **trust of our stakeholders**, and the foundation for long-term business success.

Policies

Live with integrity and act in accordance with the rules

Our Responsible Business Principles document the ethical foundations and are the binding code of conduct at O_2 Telefónica – also on sustainability issues such as human rights, climate responsibility or responsible use of digital technologies.

With our Guideline Anti-Corruption, which is based on the **UN Convention against Corruption**, national criminal law, and **OECD Guidelines**, we clearly commit to **zero tolerance** for bribery and unfair business practices. At the same time, our Policy Compliance Organisation defines the structure of our **compliance management system**, including internal structures, roles, and responsibilities to prevent legal violations, claims for damages, and reputational damage. Our antitrust prevention policy provides an overview of legal regulations and prohibited conduct; it is mandatory for all employees. Our policy on gifts and invitations ensures that we **minimise conflicts of interest**, while our training policy defines the training requirements so that all employees are familiar with and adhere to our standards.

As part of our responsible corporate governance, we rely on a **Business Continuity Management (BCM)** system certified according to ISO 22301. The BCM policy governs impact and risk analyses as well as emergency planning to ensure that critical business processes remain as resilient as possible, even in the event of disruptions. The BCM system is regularly audited, and external certification was reaffirmed in 2025. In addition, **IT Service Continuity Management (ITSCM)**, based on **ISO 27031**, ensures the **resilience** of our IT and network infrastructure. A standardised process for transparency and disaster recovery plans was established in 2025.

To actively cultivate our corporate culture and promote the highest standards regarding human rights, environmental protection, and integrity, we have established a **comprehensive whistleblower system**. This system allows for the reporting of concerns about human rights and environmental risks in accordance with the Supply Chain Due Diligence Act (LkSG), about corruption or fraud in accordance with the German Whistleblower Protection Act (HinSchG), and about internal regulations. The Whistleblowing Procedure transparently outlines how such reports can be submitted – anonymously or non-anonymously – to an independent ombudsperson. Reports can be submitted in 21 languages and can be made online, by mail, or by telephone. A dedicated human rights mailbox and a compliance mailbox are also available. The **Whistleblowing Procedure** protects whistleblowers by ensuring they do not suffer any disadvantages. Further information about our due diligence processes can be found in the chapter Human rights.

Targets

We had the following targets by the end of 2025:

- No **cases of corruption** within the company.
- More than 95% of our employees should have successfully completed the **training on the business principles**.

Performance

We remain true to our commitment

✓ In 2025, as in the previous year, we recorded 0 **cases of corruption** and thus achieved our target.

🕓 85.4% (2024: 94.7%) of employees successfully completed the **training on the company principles**. Thus, despite a continued good completion rate, we are below our target.

All key indicators and definitions can be found in our interactive KPI tool.

Actions

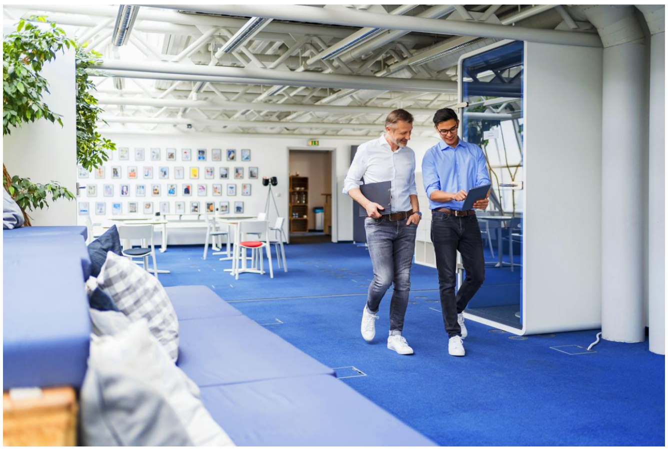
This is how we ensure integrity and ability to act

We are prepared for emergencies and disruptions: Our Business Continuity Management (BCM) and crisis management policy have established contingency plans. All critical data centres and core sites are geographically separated but synchronised and designed to operate autonomously for 48 hours. Mobile backup power systems, pumps, and air conditioning units are available for disaster situations. In addition, emergency offices are in place that maintain a satellite internet connection even during outages.

Knowledge creates security: Training on the Responsible Business Principles and human rights is mandatory for all employees and is repeated every three years, as is training on the German General Equal Treatment Act (AGG). The Responsible Business Principles training also covers corruption prevention, antitrust law, and ESG topics such as sustainable supply chain management, climate responsibility, the circular economy, and the responsible use of digital technologies. In addition, we offer voluntary intensive training on anti-corruption, which teaches the proper handling of gifts and invitations as well as the recognition of and response to bribery attempts.

The Senior Leadership Team confirms compliance with anti-corruption requirements annually as part of the Group-wide certification process. Business partners contractually commit to complying with corresponding anti-corruption clauses.

Promoting a speak-up culture and strengthening compliance awareness: We continuously monitor the legal situation and raise awareness of compliance and ethical conduct – through awareness campaigns, internal communication, and our whistleblowing system. Reports are treated confidentially and processed by a trained team. In this way, we foster the integration of ethical conduct into our corporate culture.



Business value

Legal certainty, digitally conceived

We are digitising legal and compliance processes with legal tech tools, enabling audit-proof documentation for **transparency and continuity** – across departments and, in the future, cloud-based. This allows us to respond to legal inquiries faster, streamline processes, and improve **compliance documentation** for greater trust and security. Clear digital workflows reduce risks in data protection and legal processes. Business clients benefit from **enhanced data protection, reliable compliance**, and **accelerated response times**.

Next steps

We make compliance smart

We want to further digitise compliance processes – with **legal tech and self-service platforms** for certificates and audits for our business clients. Training will be supplemented by micro-learning and gamification.

Data protection and information security

We are committed to ensuring that our customers retain control over their data and can manage their digital lives autonomously.

Strategy

For the principle of data sovereignty

Protecting personal data and mitigating cyber risks are our highest priorities. We act in accordance with the law, transparently and proactively to build trust and contribute to a secure digital society.

Policies

We're playing it safe

We protect personal data based on recognized standards and applicable laws, such as the General Data Protection Regulation (GDPR).

The Telecommunications Act (TKG) and the **ISO 27001:2022 Information Security Management System**. The corporate data protection standard forms the basis of the data protection management system and aims to ensure that data is processed lawfully and protected according to the current state of the art. It is supplemented by internal guidelines such as the information security policy, the data protection incident policy, and the crisis management policy.

Our resilience framework describes the fundamental **security control objectives**, which we specify in guidelines and standards and from which we derive control requirements. The **effectiveness of information security measures** is regularly reviewed – including through internal and external audits, such as **ISO 27001** certification audits, internal audit reviews, and internal control assessments.

Specific internal guidelines and procedures govern how we deal with threats and vulnerabilities, and how we raise employee awareness of these issues. These guidelines form the basis for **robust security and data protection management**, ensuring both transparency regarding data usage and the responsible handling of information. Implementing information security also includes the technical and organizational protection of our network and IT systems. This approach is supported by the Cyber Fusion Center, which coordinates comprehensive protective measures against cyberattacks.

Targets

We had the following targets by the end of 2025:

- **No data protection breaches or security incidents** that result in fines or other sanctions.
- Increasing the **completion rate** of the "Information Security" training among our employees to over 90%.

Performance

Encouraging results

✓ As in the previous year, there were **no data protection breaches or security incidents** in 2025 that would have led to fines or other sanctions.

The completion rate for **information security training** in 2025 was 88.5% (2024: 89.6%), just below the target of over 90%. We further strengthened our employees' security awareness through numerous additional awareness measures supplementing the mandatory training.

All key indicators and definitions can be found in our interactive KPI tool.

Actions

Prevention, monitoring, response: our resilience triad

Minimising risks from the outset: We rely on the principle of "Privacy by Design and Default" to protect personal data as effectively as possible from the very beginning. By minimising data processing and access rights, we reduce potential attack surfaces.

Keeping security in focus: Our Cyber Fusion Center (CFC) is a central hub for improving cyber security. Here, systems and networks are continuously monitored, threats are identified, and incidents are handled quickly and in a coordinated manner. The Network Operations Center (NOC) provides additional support by monitoring network components to detect anomalies early and ensure the stability of our services.

Targeted skills development: Through mandatory and regularly updated training on data protection and information security, we strengthen our employees' awareness of current threats and regulatory requirements. In 2025, numerous additional measures covering various security topics were offered to address individual needs and further enhance security awareness.

Proactively addressing threats: In addition, we use Cyber Threat Intelligence (CTI) and the Threat Intelligence Programme to analyse the evolving threat landscape. This allows us to anticipate risks and initiate preventative measures to counter potential threats.

This three-pronged approach of prevention, monitoring, and rapid response strengthens the protection of digital infrastructure.

Prioritising data privacy: As a telecommunications provider, we process large amounts of mobility and usage data. The Data Anonymisation Platform (DAP) is a multi-stage process that anonymises this data. You can find more information about data protection here.

Business value

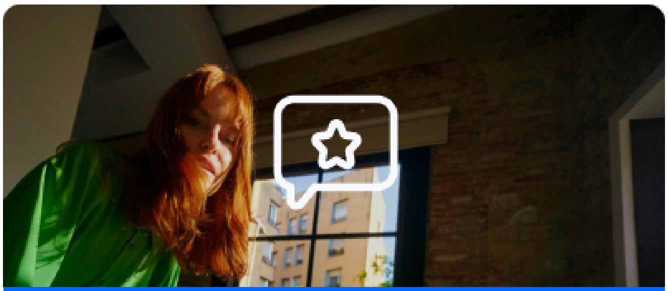
Keeping an eye on the dangers

Our **Threat Intelligence Programme** enables us to identify threats early and take preventative action. Attacker tactics and risks are continuously analysed, including in key areas such as 5G networks, IoT, ransomware, supply chains, cloud security, and social engineering. Emerging threats like AI-based attacks, malware trends, and phishing targeting business tools are also monitored. The programme delivers actionable insights for rapid decision-making, strengthens the **resilience of digital infrastructure**, and enhances the reliability of our services for our business customers.

Next steps

Certainly a good idea

As with compliance, we want to expand our AI-powered risk analyses and threat intelligence systems to **further optimise prevention**. The self-service platforms should also be usable for data protection requests and security certificates.



Business Impact Story: O_2 Telefónica enables secure network architectures for public administration

ekom21, an IT service provider for local authorities and public institutions in Hesse, uses our SD-WAN-based network architecture with integrated security functions to enable access to cloud services and technically secure the operation of sensitive applications.

→ Click here for the story: 'We needed a flexible and, above all, secure network solution.'

Human rights and sustainable supply chain management

We take sustainability criteria into account in our purchasing processes and are committed to environmental, social and human rights standards in the supply chain.

Strategy

Protect human rights, reduce risks

To effectively embed **respect for human rights** within our Group and in our own business activities, we employ a human rights due diligence process. This process implements the requirements of international frameworks, such as the UN Guiding Principles and the OECD Guidelines, as well as legal regulations, such as the German Supply Chain Act (LkSG). The six components of the process are described on the O_2 Telefónica human rights website. We have also established a **comprehensive supply chain management**. Read more about this online here.

Policies

We adhere to binding standards

In addition to the Responsible Business Principles, the Human Rights Policy defines the commitment to integrating international standards, such as the **UN Guiding Principles, the OECD Guidelines, and ILO Standards**, into our processes, as well as systematically identifying and appropriately mitigating human rights risks. It is complemented by the Commitment to Children's Rights, which focuses on the protection of children and young people and is based on the **UNICEF Principles on Children's Rights and Business Practices**.

The O_2 Telefónica Declaration of Principles on Respecting Human Rights explains our areas of action and reaffirms our **commitment to fair working conditions**. It sets out requirements for **preventing child and forced labour** as well as discrimination, supports the involvement of employee representatives, and explains the due diligence process as a key element for monitoring the implementation of these guidelines.

Our Supply Chain Sustainability Policy is a binding code of conduct for suppliers and applies to the procurement of products and services. It establishes clear **minimum environmental, social, and ethical standards**, including in particular human and labour rights, environmental and climate protection, integrity in business conduct, and data protection. Direct suppliers are required to contractually obligate their subcontractors to comply with comparable standards and regulations.

Our goal is to promote resilient and competitive supply chains together with our suppliers.

Targets

By the end of 2025, we pursued the following targets:

- Almost all of O_2 Telefónica's potential high-risk suppliers were reviewed using **self-assessments** regarding ESG aspects.
- The percentage of **resolved complaints** and reports on human rights issues is 100%.

Performance

Progress, but yet a need for action

✓ In 2025, the proportion of potential high-risk suppliers who had conducted an **ESG self-assessment** was 100% (2024: 78%).

✓ The percentage of **resolved reports and complaints** relating to human rights issues remained at 100%, same as the previous year.

All key indicators and definitions can be found in our interactive KPI tool.

Actions

Governance, risk management and transparency: this is how we implement responsibility

We act in accordance with applicable laws: Our human rights due diligence process enables us to identify human rights and environmental risks and violations at an early stage and to take appropriate measures to prevent, mitigate, or – if they have already occurred – to initiate remedial measures.

Handling of reports and complaints: Individuals, companies, and organisations can report human rights and environmental risks or violations. All relevant information can be found on our Whistleblowing Procedure website, which we further improved in 2025 by using easily understandable language and infographics for all stakeholders.

Monitoring in high-risk countries: As part of the Joint Alliance for CSR (JAC), Telefónica, S.A. Group conducts regular audits of its suppliers. These audits verify compliance with key social and labour standards, including fair working conditions with appropriate wages and working hours, as well as health and safety in the workplace. The audits also define necessary corrective actions to specifically address identified risks. As a subsidiary of Telefónica, S.A. Group, we are part of JAC and have direct access to the results of the supplier audits.

Collaboration with suppliers: Nearly 100% of the suppliers contracted in 2025 through the procurement system have committed to complying with the Supply Chain Sustainability Policy. In addition, as part of our annual risk analysis, we use standardised questionnaires for high-risk suppliers to capture the identified priority risks. In 2025, these risks included: inadequate wages, unequal treatment in employment, disregard for freedom of association and the right to collective bargaining, and inadequate health and safety in the workplace. Through dialogue with suppliers, we clarify our expectations regarding working conditions and job security.

Supplier monitoring: Through AI-supported screening, we identify risks and critical events in the value chain early on (see section Business value) and initiate measures as needed.

Review of internal processes and training: We continuously review governance structures and processes to improve transparency and human rights due diligence. Regular online training for employees and suppliers supports the implementation of the German Supply Chain Act.

Business value

For sustainable partnerships: real-time monitoring of the supply chain

We have further developed our AI-based supplier screening to assess supply chain risks transparently and efficiently. Using advanced AI models, we analyse information from news, social media, and trusted sources in more than 180 languages. This allows us to identify **potential human rights or environmental violations** early on and forward critical alerts to procurement in real time. Continuous adjustments based on user feedback ensure the quality of our risk identification.

By using AI-powered supplier monitoring, we aim for transparency and security in the direct supply chain. We contribute to supporting fair and environmentally friendly conditions in the production of goods and the provision of services, aim to **reduce failure and compliance risks,** and **strengthen ESG conformity**. In this way, we pursue the goal of developing suppliers into reliable partners and creating added value through trust and competitiveness.

Next steps

Consistently advancing human rights due diligence

We solve all reports and complaints responsibly, aim to maintain the rate of ESG self-assessments for high-risk suppliers to nearly 100%, and **further developing AI-supported systems for risk analysis**. In addition, we intensify awareness training for internal teams and suppliers to ensure the consistent implementation of international standards.