SINGLE USE SUPPORT.

PIONEERING BIOPHARMA

SINGLE USE SUPPORT

CODE OF CONDUCT

Content

Dear Employees, Business Partners,
and Stakeholders,

At Single Use Support GmbH, our reputation and success are built on trust — trust from our customers, our partners, and from each other. This trust is earned every day through the decisions we make and the way we conduct our business.

Our Code of Conduct is more than a set of rules; it reflects our shared values and principles. It applies to everyone who represents or works with Single Use Support – employees, suppliers, contractors, and business partners. It provides clear guidance on acting with integrity, respecting one another, and complying with the laws and standards that govern our industry.

We expect all of you to read this Code carefully, apply it in your daily work, and speak up if you see something that does not align with our values. Doing the right thing is everyone's responsibility, and your voice matters.

By maintaining our dedication to the highest ethical standards, we will continue to foster a community that maintains Single Use Support as a company trusted and respected by our customers and employees.

Darren Verlenden
Chief Executive Officer
Single Use Support GmbH

Purpose & scope

Purpose

The purpose of this Code of Conduct is to:

- Define the ethical principles and legal standards that guide all actions and decisions at Single Use Support GmbH.
- Promote a culture of integrity, transparency, and accountability across the organization.
- Protect the company's reputation, ensure compliance with applicable laws, and maintain the trust of customers, partners, and stakeholders.
- Provide clear guidance for employees and third parties on how to handle ethical dilemmas and compliance-related questions.

Scope

- This Code applies to **all employees**, including permanent, temporary, and contract staff, as well as **executive leadership**.
- It also applies to **business partners, suppliers, contractors, consultants,** and **any third parties** acting on behalf of Single Use Support.
- Compliance with this Code is **mandatory**, regardless of role, seniority, or location.
- In case of conflicts between this Code and local laws, the stricter standard applies.

All employees are expected to:

- Integrate the principles of this Code into their daily work.
- Seek guidance from Compliance or Legal when in doubt.
- Report any suspected violations promptly through the available channels.

Our goals & values

Our goals

- **Customer Delight:** Create value for customers through agility, reliability, and continuous improvement.
- **Growth through Innovation:** through collaboration with our customers, we innovate high value differentiated solutions to the Biopharma market.
- **Quality:** Deliver high quality solutions and services to our customers to the standards they expect.
- **Sustainability:** Integrate environmental and social responsibility into all business processes.
- **Compliance & Integrity:** Ensure adherence to laws, regulations, and ethical standards in every decision.

Our core values

- **Integrity:** We act honestly, reliably and ethically even when no one's watching.
- **Respect:** We treat colleagues, customers, and partners with dignity and fairness.
- **Transparency:** this makes mutual trust possible.
- **Diversity & Inclusion:** We embrace different perspectives and foster an inclusive workplace.
- **Courage:** We are not afraid to make bold investments to anticipate and shape the future.
- **Environmental Awareness:** We minimize our ecological footprint and promote sustainable practices.

Example

When facing a tight deadline, we never compromise on product quality or safety standards to speed up delivery. Our commitment to integrity and quality comes first.

Legal & ethical foundations

Our commitment

- We conduct all business activities with **integrity, transparency, and in full compliance** with applicable laws and regulations.
- We align with internationally recognized standards, including:
- **UN Global Compact Principles** (human rights, labor, environment, anti-corruption).
- **OECD Guidelines for Multinational Enterprises.**
- **We categorically reject:**
  - **Bribery, corruption, fraud, money laundering,** and any unlawful practice.
  - We expect the same commitment from all **business partners, suppliers, and third parties** acting on our behalf.

How we ensure compliance

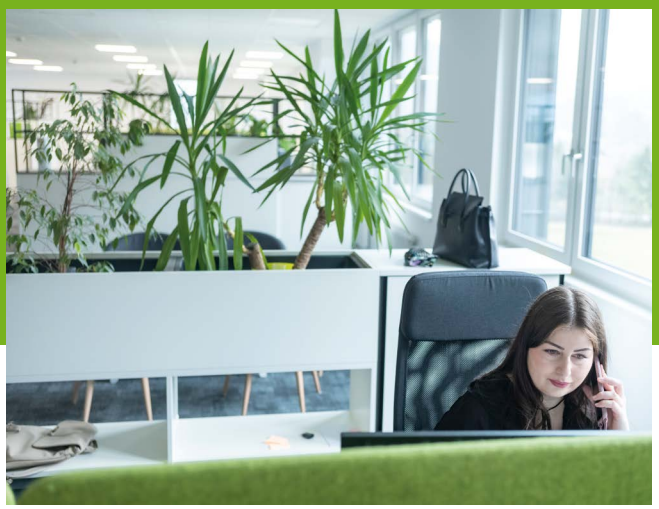
- **Internal Controls:** Policies, procedures, and approval processes to prevent misconduct.
- **Risk Assessments:** Regular evaluations of high-risk areas (e.g., anti-bribery, data protection).
- **Training & Awareness:** Mandatory compliance training for all employees.
- **Reporting Channels:** Secure and anonymous options for reporting concerns without fear of retaliation.

Our responsibilities

- Know and follow all applicable laws, regulations, and company policies.
- Avoid any activity that could lead to illegal or unethical behavior.
- Seek guidance from Compliance or Legal when in doubt.
- Report any suspected violations immediately.

Example

If a supplier suggests an “informal payment” to speed up customs clearance, you must refuse and report the incident to Compliance immediately.



Speaking up, reporting & non-retaliation

Our commitment

- We encourage an **open speak-up culture** where employees feel safe to raise concerns without fear of retaliation.
- Reporting suspected violations helps protect our company, colleagues, and stakeholders.

Non-retaliation

- **Strict prohibition of retaliation:** Any form of punishment, harassment, or disadvantage against someone who reports a concern in good faith or participates in an investigation is forbidden.
- Violations of this principle will result in disciplinary action.

Reporting channels

- **Direct reporting:** Speak to your manager, HR, or Compliance.
- **Anonymous reporting:** Use the secure whistleblowing system SPEAK-UP - Power Apps.
- **Email:** speak-up@singleusesupport.com.
- Reports can be made in **good faith** without fear of negative consequences.

Investigation process

- All concerns are reviewed promptly and fairly.
- Investigations may involve interviews, document reviews, and cooperation with authorities if required.
- Outcomes and corrective actions are communicated where appropriate.

Confidentiality & anonymity

- All reports are treated **confidentially** to the extent permitted by law.
- Anonymous reports are accepted and investigated with the same diligence.

Example

If you suspect a colleague is accepting improper gifts from a supplier, you can report it anonymously via the whistleblowing system. You will not face retaliation for raising the concern in good faith.

Conflicts of interest

A **conflict of interest (COI)** occurs when personal interests—financial, family, or otherwise—interfere, or appear to interfere, with the best interests of Single Use Support GmbH. Even the appearance of a conflict can damage trust and must be avoided.

Our obligations

- **Disclose** any actual or potential COI immediately to your manager and Compliance.
- **Avoid** situations where personal interests could influence professional judgment.
- **Recuse** yourself from decisions where a conflict exists.
- Follow any mitigation measures set by Compliance or Management.

Examples of conflicts

- Holding a financial interest in a supplier or competitor.
- Hiring or supervising a family member or close friend.
- Accepting gifts or hospitality that could influence business decisions.
- Engaging in outside employment or consulting that competes with Single Use Support.

Example

You are involved in selecting a new supplier for critical components. One of the bidding companies is owned by your cousin. Even if you believe you can remain objective, this situation creates a perceived conflict of interest. You must disclose this relationship to Compliance and remove yourself from the decision-making process.

Anti-bribery & anti-corruption (ABAC)

Single Use Support GmbH enforces a zero-tolerance policy against bribery, corruption, facilitation payments, and any form of improper advantage. These practices are strictly prohibited for all employees, managers, and third parties acting on our behalf.

What is prohibited?

- **Bribes:** Offering, giving, requesting, or accepting anything of value to influence a decision.
- **Kickbacks:** Returning a portion of contract value to secure business.
- **Facilitation Payments:** Small payments to speed up routine government actions.
- **Improper Advantages:** Any benefit intended to gain an unfair business advantage.

Gifts, hospitality & business courtesies

Allowed (with conditions):

- Modest, infrequent gifts or hospitality that are lawful, transparent, and have a legitimate business purpose.
- Example: A branded pen or a coffee during a business meeting.

Never acceptable:

- Cash or cash equivalents (e.g., gift cards, vouchers).
- Lavish travel, entertainment, or accommodations.
- Anything offered during tenders, negotiations, or regulatory inspections.

Approval & logging:

- All gifts and hospitality above the defined threshold must be **pre-approved** and recorded in the **Gifts & Hospitality Register.**
- Thresholds and approval workflows are defined in the **Gifts & Hospitality Standard.**

Third parties

- We are responsible for the actions of agents, distributors, consultants, and other intermediaries acting on our behalf.
- Due diligence is mandatory before engagement.
- Contracts must include **anti-bribery clauses** and allow audits.

Political & charitable contributions

- **Political donations:** Prohibited unless explicitly approved by Executive Management and compliant with law.
- **Charitable donations/sponsorships:** Must have a legitimate purpose, undergo due diligence, and be transparent.

Examples of violations

- Offering a government official an expensive watch to speed up an approval process.
- Accepting a luxury weekend trip from a supplier during a tender process.
- Paying a small “fee” to a customs officer to release goods faster.
- Hiring a consultant without due diligence who then bribes on our behalf.

Fair competition & antitrust

Single Use Support GmbH is committed to maintaining a fair and lawful marketplace. We strictly adhere to all applicable competition and antitrust laws. These laws are designed to protect free and fair competition for the benefit of customers, suppliers, and society.

What is prohibited?

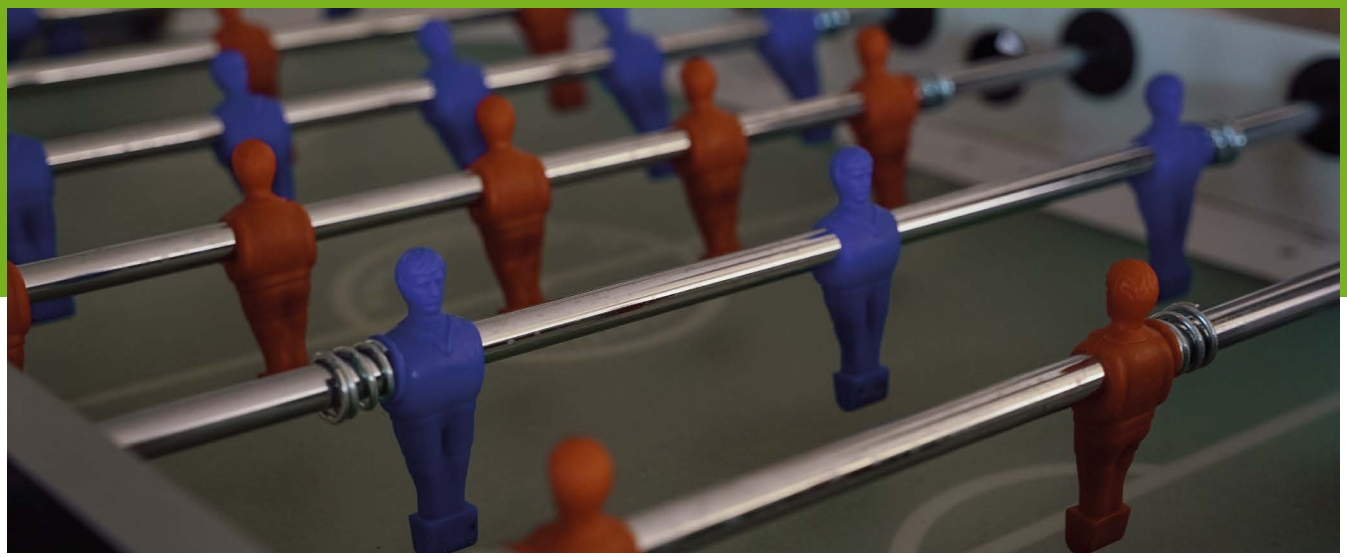
- **Price-fixing:** Agreeing with competitors to set or influence prices.
- **Market or customer allocation:** Dividing markets, territories, or customers with competitors.
- **Bid rigging:** Coordinating bids to manipulate tender outcomes.
- **Exchange of sensitive information:** Sharing non-public data such as pricing, costs, or strategic plans with competitors.
- **Group boycotts:** Agreeing with others to refuse to deal with a particular supplier or customer.

Our responsibilities

- Never discuss prices, costs, margins, or future business strategies with competitors.
- Avoid informal meetings or industry events where sensitive topics could arise.
- If a competitor attempts to discuss prohibited topics, **stop the conversation immediately,** leave the meeting, and report the incident to Compliance.
- Document any such occurrence and keep accurate notes.

Examples of violations

- Two suppliers agreeing to “rotate” winning bids for tenders.
- Competitors agreeing to set minimum prices for a product.
- Sharing future pricing plans during an industry conference.



Trade compliance

Single Use Support GmbH complies with all applicable **export control laws, customs regulations, and economic sanctions.** These rules govern the transfer of goods, services, software, and technology across borders.

Our responsibilities

- **Screening:** Verify that customers, suppliers, and partners are not on restricted or sanctioned party lists.
- **Licensing:** Obtain required export licenses before shipping controlled goods or technology.
- **End-use & end-user checks:** Ensure products are not used for prohibited purposes (e.g., weapons development) or by restricted entities.
- **Recordkeeping:** Maintain accurate documentation of export transactions for the legally required period.

Examples of violations

- Shipping controlled components to a country under embargo without a license.
- Providing technical data to a foreign national without proper authorization.
- Ignoring red flags such as unusual routing or requests for dual-use items.

Accurate records, fraud & money laundering

We maintain **complete, accurate, and timely records** to ensure transparency and compliance with financial and legal obligations.

Our responsibilities

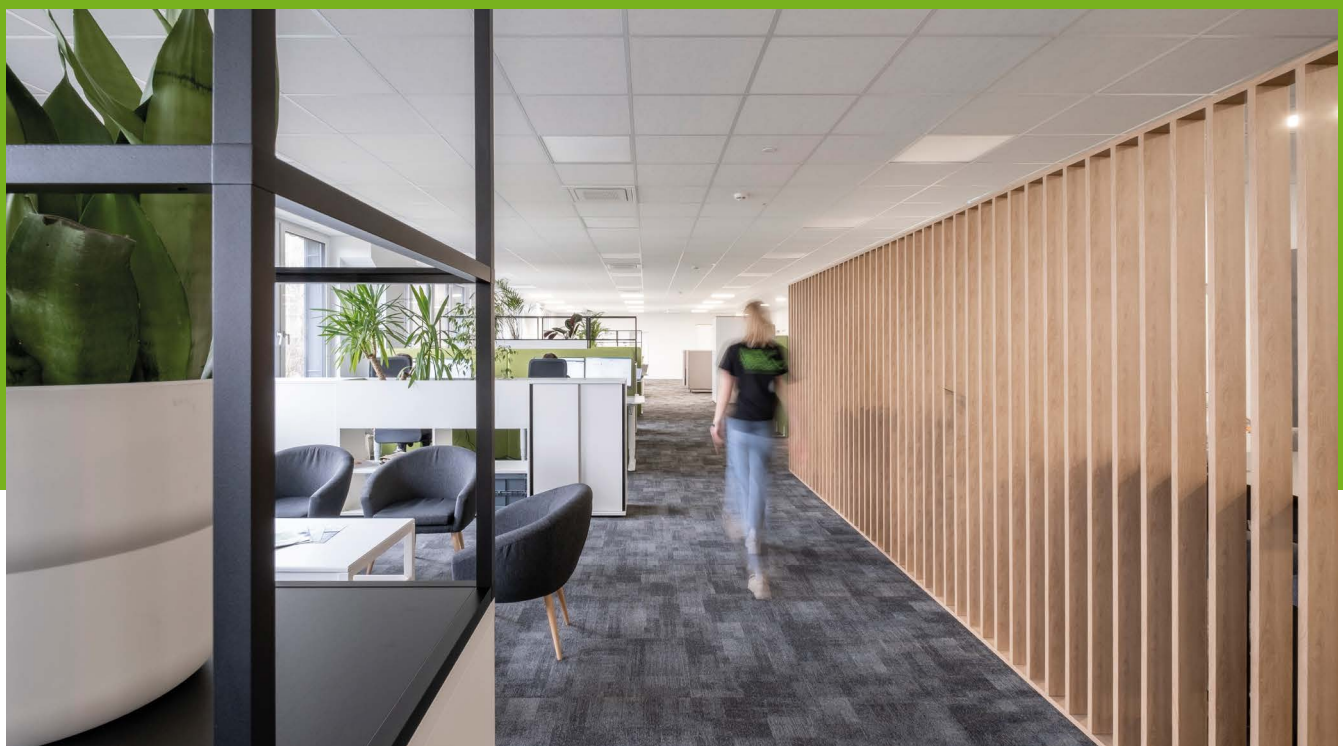
- Never falsify, alter, or mischaracterize financial or operational records.
- Ensure all transactions are properly documented and approved.
- Report any suspicious activity or irregularities immediately to Compliance or Finance.

Anti-money laundering (AML)

- Be alert to **red flags**, such as:
  - Payments from or to unrelated third parties.
  - Requests for cash transactions or unusual payment methods.
  - Complex structures with no clear business rationale.
- Conduct **due diligence** on customers and partners to prevent involvement in money laundering or terrorist financing.

Examples of violations

- Creating false invoices to hide improper payments.
- Accepting payments from an unverified offshore account.
- Splitting transactions to avoid approval thresholds.



People & workplace standards

Human rights, diversity & non discrimination

- We respect and promote human rights in all operations and across our value chain.
- We prohibit discrimination based on ethnicity, gender, religion, belief, disability, age, sexual orientation, or any other protected characteristic.
- Harassment, bullying, and intimidation are strictly forbidden.
- We support freedom of association and fair working conditions.

Health, safety & environment (HSE)

- Safety is everyone's responsibility.
- Follow all EHS guidelines, use PPE (Personal Protective Equipment), and comply with cleanroom protocols.
- Report hazards, incidents, and near misses immediately.
- Management ensures risk assessments, training, and continuous improvement.

Examples

1. Making jokes about someone's ethnicity or gender identity is harassment and will not be tolerated.
2. If you notice a chemical spill in a cleanroom, stop work, alert your supervisor, and follow the spill response procedure.

Data protection, information security & technology

Privacy & data protection

- We comply with the **General Data Protection Regulation (GDPR)** and all applicable data protection laws.
- Collect, process, and store personal data only for legitimate business purposes and with appropriate legal basis (e.g., consent, contract, legal obligation).
- Apply **data minimization** (only collect what is necessary) and **purpose limitation** (use data only for the stated purpose).
- Respect data subject rights (access, rectification, erasure, portability).
- Report any **data breach** immediately to the Data Protection Responsible.

Information security

- Protect confidential information, trade secrets, and intellectual property.
- Use **strong passwords**, enable **multi-factor authentication (MFA)**, and never share login credentials.
- Store sensitive documents in approved systems; avoid using personal devices or unauthorized cloud services.
- Report phishing attempts or suspicious emails immediately to IT Security.

Examples

1. Do not share customer or employee personal data via unsecured channels (e.g., personal email or messaging apps).
2. If you receive an email asking for login credentials, do not respond—report it to IT Security.

Responsible use of artificial intelligence (AI)

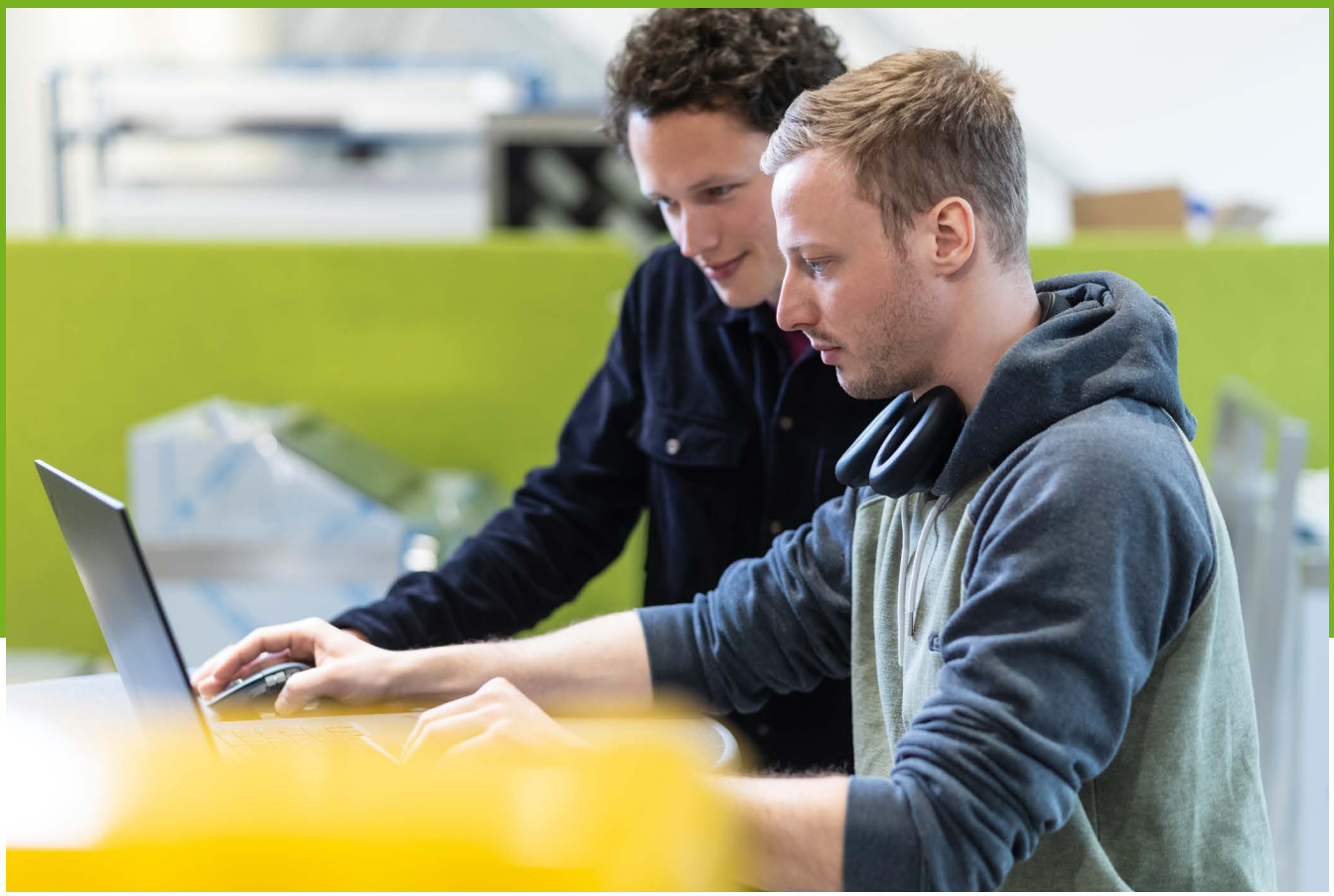
- Use AI tools only if **approved by IT and Compliance.**
- Do not input **confidential or personal data** into AI systems unless explicitly permitted and safeguarded.
- No **automated decision-making** with legal or significant effects on individuals without human oversight and prior assessment.
- Ensure AI use complies with **data protection, security, and ethical standards**.

Intellectual property & confidentiality

- Protect Single Use Support intellectual property (patents, trademarks, copyrights, trade secrets).
- Respect third-party IP rights; do not use unlicensed software or materials.
- Execute NDAs where appropriate and mark confidential documents clearly.
- Report suspected IP infringement immediately to Legal.

Examples

1. Do not upload internal contracts into a public AI chatbot for analysis
2. Do not copy competitor product designs or use images without proper licensing.



Sustainability & responsible supply chain

Environmental responsibility

We are committed to reducing our environmental footprint by:

- Minimizing energy and water consumption.
- Reducing waste and promoting recycling.
- Using environmentally friendly materials and technologies.

Employees should actively consider the environmental impact of their decisions and suggest improvements where possible.

Social responsibility

- We uphold and promote human rights across our operations and supply chain.
- We prohibit child labor, forced labor, and any form of exploitation.
- We foster diversity, inclusion, and equal opportunities for all employees.
- We expect suppliers and partners to adhere to the same standards and include these requirements in contracts.

Economic sustainability

- We aim for long-term financial stability and responsible growth.
- Decisions should balance short-term objectives with long-term value creation and risk management.
- We invest in innovation and quality to ensure resilience and competitiveness.

Supply chain due diligence

- Apply **risk-based due diligence** to suppliers, especially in high-risk regions or industries.
- Monitor compliance with human rights, environmental, and ethical standards.
- Take corrective actions in cases of non-compliance, up to and including termination of the business relationship.

Examples

1. Choose digital documentation over printing whenever possible to reduce paper waste.
2. Reject any supplier that cannot demonstrate compliance with labor standards.

Communications & social media

External communications

- Only authorized spokespersons (e.g., PR, Marketing, Executive Management) may speak on behalf of Single Use Support GmbH.
- All media inquiries must be directed to the Communications Department or designated contact.
- Do not disclose confidential or proprietary information in any external communication.

Social media use

Employees are free to use social media in a personal capacity but must:

- Clearly state that opinions are personal when discussing industry topics.
- Never share confidential information, trade secrets, or internal documents.
- Avoid posting content that could harm the company's reputation or violate laws.

Do not use company logos or branding without prior approval.

Professional conduct online

- Be respectful and professional in all online interactions.
- Do not engage in arguments or negative discussions about competitors, customers, or colleagues.
- Report any social media crisis or negative publicity to the Communications team immediately.

Examples

1. If a journalist contacts you for a comment on company performance, do not respond directly—forward the request to the Communications team.
2. Posting a photo from inside a cleanroom on your personal Instagram account is prohibited because it may reveal sensitive processes.

Training, awareness & acknowledgement

Mandatory training

- All employees must complete **mandatory compliance and ethics training** (e.g., via LENA) within the specified deadlines.
- Training covers key topics such as anti-bribery, data protection, health & safety, and Code of Conduct principles.
- Refresher courses are required periodically or when significant policy changes occur.

Manager responsibilities

- Managers must ensure their teams complete all required training on time.
- They should actively promote a culture of compliance and lead by example.

Acknowledgment

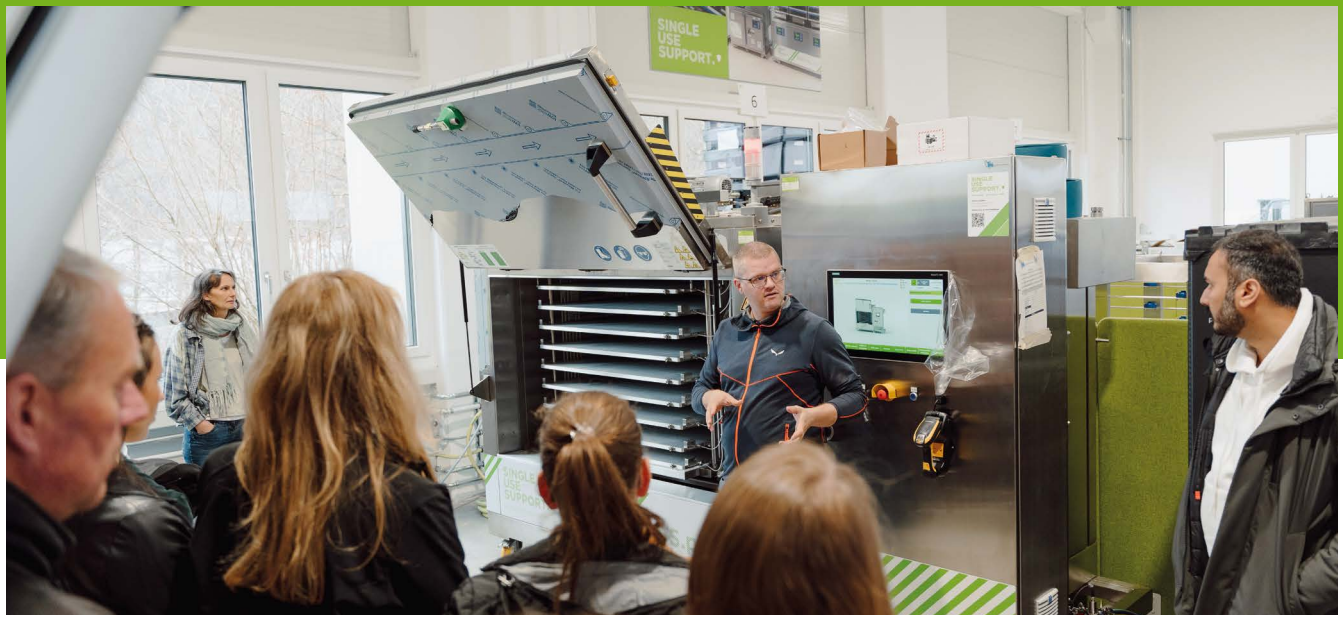
- Employees must **acknowledge receipt and understanding** of this Code and related policies annually.
- Acknowledgment is documented and stored for audit purposes.

Awareness & communication

- The Code and related policies are available on the company intranet and in onboarding materials.
- Regular communication (e.g., newsletters, workshops) reinforces awareness of compliance obligations.

Example

If you receive a notification to complete an anti-bribery training module, you must finish it by the deadline. Failure to do so may result in disciplinary action.



Roles & responsibilities

All employees

- Read, understand, and comply with this Code and all related policies.
- Complete all mandatory compliance and ethics training on time.
- Act with integrity in all business dealings and report any suspected violations promptly.
- Seek guidance from Compliance or Legal when in doubt.

Managers and leaders

- Lead by example and demonstrate commitment to ethical behavior.
- Foster a **speak-up culture** where employees feel safe to raise concerns without fear of retaliation.
- Ensure team members complete required training and understand compliance obligations.
- Monitor for potential risks (e.g., conflicts of interest, unethical practices) and escalate issues as needed.

Compliance team

- Own and maintain the Code of Conduct and related compliance policies.
- Provide advice, training, and tools to support compliance across the organization.
- Monitor adherence through audits, risk assessments, and reporting mechanisms.
- Investigate reported concerns promptly and fairly, and recommend corrective actions.

Legal department

- Advise on legal and regulatory requirements affecting the business.
- Support compliance with competition law, trade regulations, data protection, and intellectual property.
- Assist in drafting and reviewing contracts to ensure compliance clauses are included.

Data protection responsibles

- Oversee compliance with GDPR and other data protection laws.
- Conduct Data Protection Impact Assessments (DPIAs) where required.
- Handle data subject requests and maintain records of processing activities.

EHS (Environment, Health & Safety)

- Develop and maintain safety standards and environmental guidelines.
- Provide training and resources to ensure a safe workplace.
- Investigate incidents and implement corrective measures.

Example

If an employee suspects a violation of the Code, they must report it. The manager ensures the concern is escalated to Compliance, which investigates and recommends actions, while Legal provides guidance on regulatory implications.

Investigation, consequences & enforcement

Investigations

- All reported concerns are taken seriously and investigated promptly, fairly, and confidentially.
- Investigations may include interviews, document reviews, and cooperation with external authorities if required.
- Employees are expected to **fully cooperate** with investigations and provide truthful information.
- Retaliation against anyone participating in an investigation is strictly prohibited.

Consequences for violations

Breaches of this Code, company policies, or applicable laws may result in:

- Disciplinary action, up to and including termination of employment.
- Termination of contracts with third parties.
- Civil or criminal liability, including fines or imprisonment where applicable.

The severity of consequences depends on the nature and impact of the violation.

Corrective actions

In addition to disciplinary measures, corrective actions may include:

- Additional training or coaching.
- Process improvements or policy updates.
- Enhanced monitoring or audits.

Documentation

All investigations and outcomes are documented and retained in accordance with legal and regulatory requirements.

Example

If an employee is found to have accepted a bribe from a supplier, the company will terminate the employment and may report the case to law enforcement authorities.

Governance, monitoring & review

Governance structure

- The **Compliance Team** owns and maintains the Code of Conduct and related policies.
- **Executive Management** provides oversight and ensures adequate resources for compliance.
- **Legal, HR, EHS, and IT Security** collaborate to implement and enforce relevant sections of the Code.

Monitoring & auditing

Compliance with this Code is monitored through:

- **Internal audits** and spot checks.
- **Risk assessments** for high-risk areas (e.g., anti-bribery, data protection, supply chain).
- **Whistleblowing reports** and investigation outcomes.

Key metrics (KPIs) include:

- Training completion rates.
- Number and resolution time of reported incidents.
- Audit findings and remediation status.

Reporting to management

- Compliance reports are submitted to **Executive Management** and, where applicable, to the **Board or Audit Committee.**
- Significant breaches or systemic risks are escalated immediately.

Review & continuous improvement

The Code is reviewed at least annually or when:

- There are significant legal or regulatory changes.
- Internal audits or investigations reveal gaps.
- Business operations expand into new jurisdictions.

Updates are communicated to all employees, and revised versions are distributed via the intranet and training platforms.

Example

If a new EU regulation on AI governance comes into effect, the Compliance Team updates the Code and related policies, informs employees, and provides targeted training.

At-a-glance – One-page summary

This quick reference guide summarizes the core principles of our Code of Conduct. When in doubt: **Stop – Think – Ask (Manager, Compliance, Legal).**

Our core principles

- **Integrity first:**
  Act honestly, fairly, and in compliance with laws and company values.
- **Zero tolerance:**
  No corruption, no discrimination, no retaliation.
- **Speak up:**
  Use internal channels or the anonymous whistleblowing system.

Do's

- Report concerns or violations immediately.
- Disclose conflicts of interest (e.g., family ties to suppliers).
- Keep accurate and complete business records.
- Use approved tools for data processing and AI.
- Wear PPE in all safety-critical areas.
- Treat everyone with respect and without discrimination.

Don'ts

- No bribery, kickbacks, or facilitation payments.
- No price-fixing or sharing sensitive information with competitors.
- No sharing of confidential data via unsecured channels.
- No posting internal information on social media.
- No use of AI systems for confidential data without approval.

Reminder:

"If you are unsure, ask before you act."