TELENET PROCUREMENT
RESPONSIBLE SUPPLIER CODE OF CONDUCT

VERSION CONTROL:

Date	Owner	Version comments
October 2024	Telenet Procurement	V1

TABLE OF CONTENTS

I. INTRODUCTION

At Telenet, we are committed to being Belgium's leading provider of connected entertainment and business solutions, supported by reliable fixed and mobile networks. We believe technology has the power to improve lives, and we continuously innovate to deliver cutting-edge digital services, easy-to-use business solutions, and a superior customer experience.

As part of the Liberty Global Group, the world's largest international TV and broadband company, Telenet is dedicated to driving innovation and empowering people across Europe, Latin America, and the Caribbean to embrace the digital age.

As a key player in Belgium's telecommunications and media sectors, we conduct business ethically, responsibly, and lawfully. Our focus on sustainable growth balances operational excellence with social responsibility. We expect our suppliers to maintain equally high standards in business conduct, quality, sustainability, and human rights. This Supplier Code of Conduct defines these expectations.

Sustainability is integral to our strategy. We operate with fairness, transparency, and responsibility, adhering to high corporate governance standards while addressing social, economic, and environmental impacts. The products and services we procure must meet the same ethical and sustainability standards that apply to our own offerings.

Given our significant annual procurement of goods and services, we are committed to making ethical, environmental, and social considerations central to our procurement process. This Supplier Code of Conduct outlines Telenet's expectations for responsible sourcing, aiming to minimize any negative impact throughout the supply chain.

The Code provides guidance on policies, regulations, and legal requirements, detailing supplier obligations concerning social, environmental, and ethical compliance. It promotes fair working conditions and responsible management of these issues across Telenet's supply chain.

We support our suppliers in meeting these standards and encourage alignment with international best practices. Suppliers with over 250 employees are encouraged to seek certification to relevant standards, such as ISO 9001, ISO 45001, ISO 14001, ISO 27001, ISO 22301, ISO 50001, and SA 8000.

II. SCOPE

The principles in this Supplier Code of Conduct apply to all procurement and supply chain activities involving Telenet Group entities. Adherence to these principles is a key obligation in Telenet's contractual agreements, and suppliers are responsible for ensuring their application throughout their supply chains.

The term "Supplier" includes all officers, employees, contractors, subcontractors, and agents, where applicable. "Telenet Group" refers to the relevant contracting entity, as well as any parent, subsidiary, joint venture, or affiliate that benefits from the goods and services provided.

Suppliers must comply with all applicable laws, regulations, and standards in the countries where they operate, and must also promote these principles across their own supply chains, including subcontractors and partners.

This Supplier Code of Conduct is embedded in Telenet's General Purchase Conditions and forms part of all contractual agreements. Affiliates, partners, or joint ventures within Telenet Group may have additional Supplier requirements. By accepting this Code, Suppliers agree to comply with any additional policies that apply to other Telenet Group entities.

Purchasing activities are guided by this Supplier Code of Conduct, which sets clear sustainability standards for all Suppliers. Telenet will monitor compliance through a risk-based due diligence process.

III. UPDATES

This Responsible Supplier Code will be periodically updated and revised to reflect changes in laws and regulations, as well as Telenet's policies and standards. The most current version is available online here and, unless stated otherwise, will be effective when posted. We expect Suppliers to keep themselves informed as to any changes to this Responsible Supplier Code and to visit the Telenet Website regularly to keep themselves up to date. Compliance with this Responsible Supplier Code shall be each Supplier's responsibility.

IV. KEY PRINCIPLES

The Telenet Group depends on its Suppliers and all parties within their supply chains to uphold the Key Principles outlined below and to implement, manage, and maintain the necessary processes to ensure compliance:

1. International labour practice and standards

Telenet is committed to the highest labor standards across its supply chain, ensuring fair treatment and dignity for all workers. We expect our Suppliers to uphold these standards, applying internationally recognized labor practices in all locations.

Suppliers must comply with international conventions and treaties as well as relevant labor laws. This includes compliance with regulations on working hours, wages, benefits, and overtime. Suppliers must ensure fair treatment, prohibit forced labor, child labor, and discrimination, and provide safe working conditions and freedom of association.

2. Contracted labour

- Telenet requires Suppliers to comply with international standards and local laws governing contracted labor. All workers employed through third-party contractors must receive the same rights, protections, and benefits as direct employees.
- Contracted workers must have transparent employment agreements that clearly outline their roles, responsibilities, compensation, and working conditions. Suppliers must ensure that contracted labor is voluntary, free from coercion, and not subject to exploitation or forced labor.
- Suppliers must also ensure that third-party contractors adhere to the same labor standards. Regular audits must be conducted to ensure compliance with legal and ethical requirements. Non-compliance will be treated as a serious breach of this Code.

3. Child labour

- Telenet enforces a zero-tolerance policy on child labor and expects all Suppliers to comply with international labor standards, including the ILO Convention on the minimum age for employment. Suppliers must not engage in or support child labor in any form.
- The minimum employment age must comply with local laws and be no less than 15 years or the age at which compulsory schooling ends, whichever is higher. If local laws permit employment for those aged 15-18, Suppliers must ensure that the work does not endanger their health, safety, or education.

- Suppliers must verify employee ages through proper documentation and ensure that third-party contractors also comply. Violations of child labor policies will be treated as serious breaches, potentially resulting in immediate corrective action or termination of the business relationship.

4. Forced labour

- Telenet prohibits all forms of forced, bonded, or involuntary labor across its supply chain. Suppliers must ensure that all work is voluntary and free from coercion, threats, or exploitation.
- Suppliers must not engage in or benefit from forced labor, including bonded labor, debt servitude, human trafficking, or modern slavery. Employees must be free to leave their jobs with reasonable notice and retain possession of their personal documents. Deposits or security payments as conditions of employment are strictly forbidden.
- Suppliers must have procedures to prevent, detect, and address any instances of forced labor in their operations and supply chains. Breaches will be treated as severe violations, leading to immediate corrective action or termination of the business relationship.

5. Working hours and wage

- Telenet requires Suppliers to comply with all laws, regulations, and industry standards regarding working hours, wages, and benefits. Employees must be fairly compensated in line with legal requirements, industry benchmarks, and collective agreements, where applicable.
- Working hours must not exceed legal limits, including overtime, which should be voluntary, paid at premium rates, and not a substitute for regular employment. Employees must receive rest breaks, days off, and holidays as per local law.
- Wages must meet or exceed the legal minimum, and where no laws exist, they must be sufficient to cover basic needs. Payments must be made regularly, on time, and in full, with no unlawful deductions.
  Suppliers must provide clear, written information on employment conditions, including wage breakdowns and hours worked. Pay transparency is crucial, and unfair deductions are strictly prohibited.

6. Freedom of association

- Telenet requires Suppliers to respect workers' rights to freely associate, organize, and bargain collectively in line with local laws. Workers must be able to join unions without fear of retaliation or harassment.
- Suppliers must foster open communication, allowing employees to voice concerns and engage in collective bargaining without discrimination or disciplinary action.
  Where local laws limit these rights, Suppliers must provide alternative channels for workers to express concerns and negotiate working conditions.

7. Discrimination

- Telenet requires Suppliers to treat all workers fairly and equally, without discrimination based on race, gender, age, sexual orientation, ethnicity, religion, disability, or any other protected status.
- Suppliers must maintain a workplace free from discriminatory practices in hiring, compensation, promotion, and other employment decisions, ensuring that merit and performance are the sole criteria for advancement.
  Harassment, abuse, and intimidation in any form are prohibited. Suppliers must actively prevent and address any instances of harassment or discrimination in the workplace.

8. Fair treatment, Diversity and Inclusion

- Suppliers must uphold principles of fair treatment, diversity, and inclusion by treating all employees with dignity and respect. This includes strictly prohibiting any form of harassment, abuse, coercion, or inhumane treatment, whether physical, verbal, psychological, or sexual.
- To foster a safe and respectful working environment, Suppliers are expected to implement effective procedures to prevent and address harassment. Employees must be able to raise concerns without fear of retaliation, ensuring an atmosphere of trust and mutual respect.
- Disciplinary practices must be fair, transparent, and aligned with international standards. Practices such as corporal punishment, threats, or coercion are strictly prohibited. By promoting fair treatment, diversity, and inclusion, Suppliers contribute to a healthy, productive, and equitable workforce.

9. Community Engagement

- Suppliers are encouraged to engage with local communities, considering the social, economic, and environmental impacts of their operations and making positive contributions.
- Suppliers should build sustainable relationships with local stakeholders, addressing community needs through initiatives like local employment, education, and environmental stewardship.
- Operations must respect the rights and cultures of affected communities, fostering long-term, mutually beneficial outcomes.
- Telenet encourages Suppliers to support initiatives that enhance community well-being and align with UN Sustainable Development Goals.

10. Healthy and Safe Work Environment

- Suppliers must ensure a safe and healthy working environment, complying with all health and safety laws and industry standards.
- Proactive measures must be taken to prevent accidents, injuries, and health risks, including regular safety assessments, proper training, and the use of protective equipment. Safety policies should address industry-specific hazards.
- Suppliers must have emergency preparedness and response procedures, including evacuation plans, first aid, and access to emergency services.
- Promoting physical and mental well-being is essential for a productive workplace. Telenet expects Suppliers to continuously improve health and safety practices.

V. OUR ETHICAL STANDARDS

At Telenet, we uphold the highest ethical standards in all our business operations. Our Ethical Principles guide how we conduct business, interact with stakeholders, and make decisions, fostering a culture of integrity, transparency, and accountability.

We expect our Suppliers to embrace these principles, ensuring responsible business practices that comply with all applicable laws. By adhering to these standards, Suppliers contribute to an environment of fairness, honesty, and respect for human rights.

The following principles outline the ethical standards Suppliers must observe in all dealings with Telenet and their broader business activities.

1. Ethical and Legal Principles

- Telenet expects Suppliers to conduct business with the highest ethical standards, ensuring transparency, lawfulness, and good faith in all activities.
- Suppliers must act with integrity in all operations, including financial practices, reporting, and fair competition. Legal compliance is mandatory, and Suppliers must proactively address potential legal and ethical risks.
- Suppliers must avoid corrupt practices, including bribery, fraud, and insider trading. Telenet has a zero-tolerance policy for violations and expects Suppliers to uphold the same commitment to ethical standards. Suppliers must also ensure compliance with all applicable international, EU, and US sanctions and must not engage in transactions or interactions with individuals, entities, or organizations subject to such sanctions. Any breach of these obligations will be treated as a serious violation of Telenet's ethical and legal requirements.

Failure to meet legal standards may result in sanctions or termination of business with Telenet. Suppliers must integrate ethical decision-making into daily operations and strategies, ensuring that all practices promote fairness, respect, and sustainability. They are responsible for maintaining internal controls to ensure compliance with ethical and legal standards.

Suppliers should implement systems to monitor compliance, manage risks, and promptly address any violations. Any actual or potential breaches must be reported to Telenet immediately.

2. Anti-corruption and bribery policy

- Telenet enforces a zero-tolerance policy on corruption, bribery, and unethical behavior. Suppliers are strictly prohibited from offering, receiving, or soliciting bribes or improper payments in any dealings with Telenet or its partners.
- Suppliers must comply with all relevant anti-corruption laws, including the UK Bribery Act (for Suppliers in UK) and the US Foreign Corrupt Practices Act (FCPA) (for Suppliers in the US). These Suppliers must ensure transparency and accurately record all business transactions, avoiding any gifts or benefits that could influence decision-making.

Bribery includes offering anything of value to influence a decision, while ***Corruption*** involves dishonest or unethical behavior for personal or business gain. Suppliers must not engage in bribery, facilitation payments, kickbacks, or improper influence.

- Suppliers are responsible for ensuring their agents, intermediaries, and partners comply with anti-corruption laws, conducting due diligence to prevent corrupt practices. Political contributions or donations intended to secure business advantages are prohibited.
- Suppliers must implement controls, risk assessments, and monitoring to prevent and detect bribery or corruption. Regular audits should ensure compliance with anti-corruption laws, and Suppliers must align with Telenet's Anti-corruption Policy.

Failure to comply may result in severe consequences, including contract termination, legal penalties, and reputational damage. Suppliers should provide regular training and ensure all employees and partners are aware of anti-corruption policies.

3. Conflict of interest

- Suppliers must make objective business decisions free from conflicts of interest, which occur when personal, financial, or other factors compromise business integrity.

- Suppliers must disclose any actual or potential conflicts of interest involving Telenet, including relationships, financial interests, or other ties that could improperly influence decisions.
- Suppliers should have policies to identify, manage, and mitigate conflicts of interest, ensuring impartiality in all dealings with Telenet.

Conflicts of interest may arise from personal relationships, financial interests, outside employment, gifts, or third-party interests. Suppliers must avoid actual, potential, or perceived conflicts when conducting business with Telenet, ensuring decisions are made solely in Telenet's best interest.

- Suppliers must report any conflicts to Telenet, who will work with the Supplier to resolve the issue. This may involve recusing individuals, implementing safeguards, or, if necessary, terminating the business relationship.
- Suppliers are prohibited from failing to disclose conflicts, attempting to influence Telenet employees through gifts or hospitality, or engaging in conflicting business practices. Suppliers must maintain accurate records of conflicts and how they were resolved, and Telenet reserves the right to audit these records.

Failure to comply with Telenet's conflict of interest policy may result in contract termination, legal action, or exclusion from future business opportunities. Suppliers must proactively manage and mitigate conflicts of interest, regularly reviewing operations and relationships to ensure compliance.

4. Insider Trading

Insider trading occurs when non-public, material information is used to buy or sell securities, or is shared with others ("tipping"). Suppliers and their employees must not engage in these practices.

- Suppliers must not engage in or facilitate insider trading. Such actions are illegal and unethical.
- Suppliers must ensure that employees, contractors, and representatives with access to confidential information do not use it for personal gain or disclose it for trading purposes. Clear policies must be in place to prevent insider trading.

- Suppliers must treat all non-public information as confidential and safeguard it from unauthorized access. Sharing this information with third parties, including family or friends, is prohibited unless expressly authorized by Telenet or required by law.

Engaging in insider trading may result in:

  - Termination of the Supplier's contract with Telenet.
  - Civil or criminal penalties, including fines and imprisonment.
  - Damage to the Supplier's reputation and exclusion from future business opportunities.

- Suppliers must have internal policies to prevent insider trading and ensure that their personnel are trained on relevant laws and ethical conduct.

5. Transparency and Accountability

Suppliers must conduct their business with transparency and accountability, ensuring accurate, complete, and accessible records of their operations, financial activities, sustainable performance and supply chain management.

- **Accurate Record Keeping:** Suppliers must maintain clear, detailed records of business transactions, including financial data and supply chain activities, and provide them to Telenet for review upon request.

- **Disclosure of Conflicts of Interest:** Suppliers must promptly disclose any conflicts of interest that could affect compliance with this Code or compromise their impartiality in dealings with Telenet.
- **Risk Identification and Reporting:** Suppliers must identify and assess risks related to compliance, including supply chain, environmental, or regulatory risks, and communicate these risks to Telenet in a timely manner. Telenet expects Suppliers to also support Telenet in their due diligence, reporting and risk management efforts by timely sharing additional relevant information upon request.
- **Audit and Compliance:** Telenet may request audits to verify adherence to this Code. Suppliers must cooperate fully, providing access to relevant records and personnel.

Failure to uphold these principles may result in contract termination or other legal actions.

6. Gifts and hospitality policy

Suppliers must engage in business practices that reflect integrity, transparency, and adherence to ethical standards. Gifts, hospitality, or benefits offered to Telenet employees must not influence business decisions or create unfair advantages.

- **Permissible Gifts and Hospitality:** Any gifts or entertainment provided to Telenet must be modest, infrequent, and in line with customary business practices, complying with Telenet's Gifts and Hospitality Policy and applicable laws.
- **Prohibited Practices:** The following are strictly forbidden:
  - Offering gifts or hospitality during tenders or negotiations to influence outcomes.
  - Providing cash, gift cards, or vouchers.
  - Any offering that creates a conflict of interest or compromises the judgment of a Telenet decision-maker.
  - Offering extravagant travel, accommodation, or hospitality.

Failure to comply may result in immediate termination of the business relationship and legal consequences.

7. Diversity and Ethical Sourcing in the Supply Chain

Telenet is committed to promoting diversity, inclusion, and ethical practices across its entire supply chain. We expect our Suppliers to mirror this commitment by fostering a diverse workforce and sourcing materials and services in a manner that respects human rights, promotes fair labor practices, and adheres to the highest ethical standards.

- **Promoting Diversity:** Suppliers are encouraged to implement inclusive hiring, culture and employment practices that reflect the diversity of the communities in which they operate. This includes providing equal opportunities regardless of gender, race, ethnicity, disability, sexual orientation, religion, or any other characteristic protected by law. Suppliers should also aim to engage and support diverse businesses, including small enterprises, minority-owned, women-owned, and socially responsible businesses.
- **Ethical Sourcing Practices:** Suppliers must ensure that all materials, goods, and services are sourced in a responsible and ethical manner. This includes adhering to internationally

recognized standards for labor, environmental sustainability, and human rights throughout the supply chain. Suppliers should verify that their own Suppliers and subcontractors uphold similar ethical sourcing standards.

- **Fair Labor Practices:** Telenet expects Suppliers to maintain fair labor practices in compliance with all applicable laws and regulations, including those related to wages, working hours, health and safety, and the prevention of forced, bonded, or child labor. Suppliers must not tolerate any form of exploitation or abuse in their operations or supply chains.

- **Environmental Sustainability:** Suppliers are encouraged to implement sustainable sourcing practices that minimize environmental impact. This includes reducing waste and greenhouse gas emissions, conserving energy and natural resources, minimize harmful substances or physical impact to the environment, and sourcing materials from Suppliers who prioritize environmental sustainability. Suppliers should strive to align with international environmental standards, such as ISO 14001, where applicable.

- **Supply Chain Transparency:** Suppliers must maintain transparency in their sourcing practices and provide Telenet with clear documentation that demonstrates ethical sourcing and fair labor practices throughout their supply chains. Telenet reserves the right to request audits or assessments of Suppliers' sourcing practices to ensure compliance with this Code of Conduct.

Failure to adhere to these principles of diversity and ethical sourcing may result in the termination of the business relationship, and Telenet reserves the right to take appropriate legal action if necessary.

8. Responsible Corporate Governance

Telenet is committed to promoting diversity, inclusion, and ethical practices throughout its supply chain. We expect our Suppliers to support these values by fostering a diverse workforce, upholding human rights, and adhering to ethical standards.

- **Fair Labor Practices:** Suppliers must maintain fair labor practices, comply with laws related to wages, working hours, and safety, and prevent forced, bonded, or child labor.

- **Environmental Sustainability:** Suppliers should adopt sustainable sourcing practices, reducing waste and greenhouse gas gases, conserving resources, minimizing overall impact on the environment via substances or physical changes, and aligning with international environmental standards such as ISO 14001.

- **Supply Chain Transparency:** Suppliers must ensure transparency in their sourcing practices, providing documentation to demonstrate ethical sourcing and fair labor standards. Telenet may request audits to verify compliance.

Failure to adhere to these principles may result in termination of the business relationship and legal action.

9. Whistleblowing procedures

Telenet values integrity and ethical conduct throughout its supply chain. Suppliers are expected to establish effective whistleblowing procedures that allow employees, contractors, and third parties to report misconduct without fear of retaliation.

- **Confidential Reporting Channels:** Suppliers must provide secure, confidential channels for reporting unethical behavior, fraud, or violations of the Supplier Code. These channels should be accessible and encourage prompt reporting.

- **Protection Against Retaliation:** Whistleblowers must be protected from retaliation. Suppliers must implement protective measures to ensure individuals can report misconduct in good faith without fear of retaliation.
- **Investigation Procedures:** Suppliers must establish clear processes to investigate whistleblower complaints impartially and promptly. Investigations should be conducted by independent teams to avoid conflicts of interest.
- **Timely Action:** After an investigation, Suppliers must take appropriate actions, including disciplinary or corrective measures. Whistleblowers should be informed of the outcome, in line with data protection laws.
- **Awareness and Training:** Suppliers must communicate whistleblowing policies to all employees and contractors, providing regular training to ensure understanding of reporting rights and protections.
- **Record Keeping and Transparency:** Suppliers should maintain confidential records of whistleblower complaints and investigations and provide them to Telenet upon request. Significant incidents must be reported to Telenet.

Telenet expects Suppliers to promote a culture of transparency and accountability, where individuals feel empowered to report misconduct without fear of retaliation.

VI. ENVIRONMENTAL RESPONSIBILITY

At Telenet, we are committed to safeguarding the environment for future generations by reducing the environmental impact of our operations and those of our Suppliers. We view business success and environmental responsibility as integral components of our long-term strategy for sustainable growth.

Telenet values partnerships with Suppliers who prioritize sustainability and demonstrate a commitment to continuously improving their environmental performance. Together, we aim to drive meaningful change and foster a culture of environmental stewardship across the supply chain.

We expect our Suppliers to adopt environmentally responsible practices by ensuring full compliance with all applicable environmental laws and regulations. Additionally, Suppliers are encouraged to seek innovative solutions and employ best available techniques to minimize their ecological footprint. Suppliers must also support Telenet's due diligence, reporting, and risk management efforts by promptly providing relevant information when requested.

1. Specific Environmental Expectations

- **Address Climate Change:**
  - Mitigate climate change in line with the UN Paris Climate Agreement and the EU Green Deal to limit global warming to 1.5°C. Suppliers must publicly commit to achieving net-zero emissions by 2050 at the latest and comply with applicable Telenet Group policies, such as sustainable travel practices.
  - Prevent potential Telenet Group service disruptions due to climate change effects (e.g., heatwaves, floods, wind loads) by addressing vulnerabilities in their own operations and supply chains.
- **Energy Efficiency and Decarbonization:**

- Reduce overall energy consumption and eliminate the use of fossil fuels in their operations through publicly committed targets.

- **Sustainable Resource Management:**
  - Use resources sustainably by adopting circular economy practices that reduce waste, maximize material repurposing, and optimize resource efficiency.
  - Adopt eco-design principles, eliminate single-use products, and minimize environmental impact throughout the entire lifecycle of delivered products and services.
- **Biodiversity Protection:**
  - Minimize environmental impact and actively contribute to the protection of biodiversity, which is vital for healthy ecosystems, human well-being, and economic stability.
  - Protect ecosystems by reducing pollution, conserving water, and controlling emissions to prevent soil degradation, water contamination, and air pollution.
- **Data Sharing for Sustainability:**
  - Enhance Telenet's sustainability insights by providing data on specific environmental impacts, such as greenhouse gas (GHG) emissions, for Supplier products and services.

2. General Supplier Obligations

All Suppliers must:

- **Manage Hazardous Waste:**
  - Handle hazardous waste responsibly, ensuring compliance with all applicable laws and regulations, while striving to reduce hazardous material usage.
- **Restrict Harmful Substances:**
  - Comply with all laws, regulations, and customer requirements regarding the prohibition or restriction of specific substances.
  - Identify and manage hazardous chemicals and materials, especially those listed as Substances of Very High Concern (SVHC) under the EU REACH Regulation, to ensure safe use, recycling, and disposal. The use of such substances must be avoided wherever possible and minimized if avoidance is not feasible.
- **Obtain and Maintain Permits:**
  - Obtain, maintain, and keep current all necessary environmental permits, approvals, and registrations (e.g., for waste management and transportation).
- **Prevent Conflict Minerals:**
  - Ensure supply chains are free from conflict minerals (e.g., tantalum, tin, tungsten, and gold). Suppliers must verify that these materials are not sourced from regions where their extraction finances armed conflict or human rights abuses, particularly in conflict-affected areas such as the Democratic Republic of Congo (DRC).

3. Consequences of Non-Compliance

Failure to meet these environmental commitments and obligations may result in the termination of the Supplier relationship and potential legal consequences.

VII. TECHNOLOGY, PRIVACY, AND INFORMATION SECURITY

We recognize the importance of safeguarding technology systems, protecting personal and sensitive data, and maintaining the highest standards of information security. In this respect, we expect our Suppliers to share these commitments and adhere to robust policies that ensure the privacy, security, and integrity of all data and technological assets involved in their relationship with Telenet.

We also expect Suppliers to safeguard and only make proper use of information or assets that we share with them and abide by all information protection and privacy laws that apply to their relationship with Telenet Group. Respecting and protecting the Privacy rights of Telenet Group customers and other consumers, Telenet Group employees, officers, directors and other parties with whom Telenet Group does business, is important to building and maintaining trust.

Failure to comply with Telenet's standards for technology, privacy, and information security may result in:

- **Termination of the Supplier relationship**.
- **Legal and financial consequences**, including liability for damages caused by a data breach or security incident.
- **Exclusion from future business opportunities** with Telenet and its affiliates.

Suppliers are expected to take immediate corrective action in response to any breach or security incident and ensure that such incidents do not occur in the future.

1. Compliance with Data Privacy Laws

Suppliers must comply with all applicable data protection and privacy laws, including but not limited to the **EU General Data Protection Regulation (GDPR)** and other relevant laws in the jurisdictions in which they operate. This includes

ensuring the lawful processing of personal data, respecting the rights of data subjects, and taking appropriate steps to protect the confidentiality and integrity of personal data. Supplier shall process Personal Data always in accordance with the Data Protection Laws and provisions of any agreements between Supplier and Telenet Group, including Data Processing or Data Sharing Agreements, as applicable. In particular, when acting as a Processor, Supplier shall process Personal Data only in accordance with Telenet Group's instructions and never for its own purposes, and shall not transfer any Personal Data to third parties without Telenet Group's prior approval

- **Data Minimization**: Suppliers should only collect, process, and retain the minimum amount of personal data necessary to achieve legitimate business purposes. When acting as a Processor, Supplier shall process Personal Data only in accordance with Telenet instructions and never for its own purposes and shall not transfer any Personal Data to third parties without Telenet Group's prior approval.
- **Lawful Basis**: Suppliers must ensure that they have a lawful basis for collecting and processing personal data, such as consent, legitimate interest, or contractual necessity, as required under applicable data protection laws.

- **Data Subject Rights**: Suppliers must respect the rights of individuals (data subjects) to access, correct, delete, and restrict the processing of their personal data, as mandated by applicable privacy laws.
- Supplier shall not process Personal Data outside the European Economic Area without Telenet's prior approval and shall comply with applicable legislative requirements and guidelines regarding international transfers of Personal Data, including, where applicable, conducting a transfer impact assessment and implementing any necessary measures to ensure an essentially equivalent level of protection to the Personal Data transferred outside the European Economic Area.

2. Information Security Standards

Suppliers must implement and maintain robust information security measures to protect data from unauthorized access, theft, loss, destruction, or compromise. This includes adopting industry-recognized standards for information security, such as **ISO 27001** or equivalent.

- **Access Controls**: Suppliers must establish secure access control mechanisms to ensure that only authorized personnel can access confidential or sensitive information. Multi-factor authentication, encryption, and role-based access controls should be employed to safeguard data.
- **Data Encryption**: All sensitive data, including personal and business-critical information, must be encrypted both in transit and at rest using strong encryption standards.
- **Security Audits and Testing**: Suppliers are encouraged to conduct regular security audits, penetration tests, and vulnerability assessments to identify and mitigate security risks.
- **Incident Response**: Suppliers must establish and maintain an incident response plan to address security breaches or data incidents in a timely manner. The plan should include procedures for containment, investigation, reporting, and remediation.

3. Data handling and Storage

Suppliers are required to handle, store, and transmit data in a manner that protects its confidentiality, integrity, and availability.

This includes:

- **Data Retention**: Suppliers must only retain personal and sensitive data for as long as necessary to fulfill legitimate business purposes or as required by applicable laws. Suppliers must securely delete or anonymize data once it is no longer needed.
- **Secure Data Storage**: Data must be stored in secure environments that prevent unauthorized access, modification, or destruction. Cloud storage services and data centers used by Suppliers must comply with relevant security standards and certifications.
- **Data Backup and Recovery**: Suppliers must maintain secure and regular backups of critical data to ensure its availability in the event of a data loss or system failure. Backup procedures should include offsite storage and disaster recovery planning.
- **Privacy by Design and Default:** Suppliers are required to incorporate privacy by design and by default into their products, services, and processes. This means that privacy considerations must be integrated into the development of any technology or service from the outset, ensuring that data protection principles are adhered to by default.

  - **Designing for Security:** Systems and services provided by the Supplier must be designed with robust security features to protect data from breaches or unauthorized access.
  - **Minimizing Data Exposure:** Suppliers must ensure that their systems and processes minimize data exposure, for example, by limiting the amount of data collected, anonymizing data where possible, and employing data masking techniques.

- **Protection of Confidential and Proprietary Information:** Suppliers must protect all confidential and proprietary information belonging to Telenet or its customers. This includes trade secrets, financial data, intellectual property, business plans, and any other non-public information that could harm Telenet's interests if disclosed.
- **Non-Disclosure:** Suppliers must not disclose confidential information to unauthorized third parties, including competitors, without Telenet's prior written consent. Confidentiality agreements should be in place with all employees, contractors, and third parties who may have access to Telenet's confidential information.
- **Third-Party Data Sharing:** When sharing confidential information with third parties (e.g., subcontractors), Suppliers must ensure that these third parties comply with the same data security and confidentiality requirements.
- **Return or Destruction of Data:** Upon the termination of the business relationship or the completion of services, Suppliers must return or securely destroy all confidential information and data in their possession, as required by Telenet.

4. Reporting Security Breach

Suppliers must promptly notify Telenet of any actual or suspected data breach or security incident that may compromise the confidentiality, integrity, or availability of data or systems. The notification should include:

- **Details of the breach**: A description of the nature and scope of the breach, the data affected, and any potential impact on Telenet or its customers.
- **Immediate actions taken**: The steps taken to contain the breach, mitigate its impact, and prevent further data loss or damage.
- **Remediation plan**: A plan for full remediation of the breach and steps to prevent similar incidents in the future.

Suppliers must fully cooperate with Telenet in the investigation of security incidents and breaches and take any necessary corrective actions to address vulnerabilities or security gaps.

5. Technology Usage and Innovation

Suppliers are expected to use technology responsibly and align with best practices for innovation and digital transformation. This includes:

- **Ethical Use of Technology**: Suppliers must ensure that technology is used in a way that respects privacy, security, and human rights. The development and use of artificial intelligence, big data, and other advanced technologies must be conducted ethically and transparently.
- **Sustainable Technology**: Suppliers are encouraged to adopt energy-efficient and environmentally sustainable technologies in their operations, particularly in data centers and hardware production.

- **Open Communication**: Suppliers must maintain open communication with Telenet regarding technology advancements, innovations, and any potential risks or concerns that may arise from the use of new technologies.

6. Training and Awareness

Suppliers must provide regular training to employees, contractors, and subcontractors on information security, data privacy, and responsible technology use. This training should cover:

- **Understanding Data Privacy Laws**: Ensuring that personnel understand and comply with GDPR, data protection regulations, and industry-specific privacy requirements.
- **Security Awareness**: Training employees on recognizing and preventing security risks, such as phishing attacks, malware, and social engineering.
- **Handling Confidential Information**: Educating personnel on the proper handling, storage, and sharing of confidential and proprietary information.

VIII. COMPLIANCE

Telenet Group expects Suppliers to fully comply with all applicable laws, regulations, and international standards, as well as the Key Principles outlined in this Responsible Supplier Code. Adherence to these principles is essential to ensure alignment with Telenet's commitment to social and environmental responsibility, maintaining transparency, integrity, and trust in all business dealings.

Key principles include:

- **Adherence to Laws:** Suppliers must comply with all local and international laws, including labor, environmental, health and safety, and anti-corruption laws. Staying informed of legal changes is essential.
- **Regulatory Compliance:** Suppliers must ensure that their products, services, and practices meet all regulatory requirements, including maintaining necessary licenses and certifications.
- **Environmental and Safety Laws:** Suppliers must follow environmental protection and safety regulations, properly handling hazardous materials and reducing emissions while maintaining a safe work environment.
- **Product Safety:** Suppliers must ensure that all products meet safety standards and consumer protection laws, including labeling, packaging, and quality requirements.
- **Fair Competition:** Suppliers must comply with competition and antitrust laws, avoiding practices like price-fixing, market allocation, or bid rigging.
- **Data Protection:** Suppliers must follow data protection laws, such as GDPR, implementing measures to protect personal data and notify Telenet of any breaches.
- **Anti-Bribery Laws:** Suppliers must comply with anti-bribery and anti-corruption laws, ensuring no improper payments or bribes are involved.
- **Trade Compliance:** Suppliers must adhere to export control, sanctions, and customs laws, ensuring their supply chain complies with international trade regulations.
- **Documentation:** Suppliers must maintain accurate compliance records and report any violations or breaches to Telenet immediately.

- **Training:** Suppliers must provide training to employees on relevant legal requirements and maintain ongoing compliance programs to mitigate risks.

By following these principles, Suppliers help Telenet uphold ethical business practices. Failure to comply may result in termination and legal consequences.

Compliance with the Responsible Supplier Code will be evaluated by Telenet Group in accordance with the Telenet's Supplier risk screening procedure. This process also enables Telenet Group to assess the improved sustainability performance of Suppliers and to help them to improve by implementing suggested corrective actions.

If Supplier declines Telenet Group's risk screening and monitoring requests, or if Supplier fails to comply with this Responsible Supplier Code, this may affect Telenet Group's ability and willingness to continue business relations with the relevant Supplier.

IX. ACKNOWLEDGMENT

By engaging in business with Telenet, Suppliers acknowledge and agree to adhere to the principles outlined in this Supplier Code of Conduct.

We are committed to partnering with Suppliers who share our values and commitment to ethical business conduct, sustainability, and social responsibility. Together, we can ensure that our business relationships are built on trust, respect, and integrity.

X. ENGAGEMENT AND COMMUNICATION

Telenet Group will communicate these Key Principles externally to all business partners, Suppliers, and potential business partners.

Telenet Group will aim to work with Suppliers, where appropriate, to share best practices on responsible supply chain management.

XI. RESPONSIBILITIES

Suppliers should appoint a relevant point of contact to ensure adherence to the Key Principle outlined in this document.

XII. RAISING CONCERNS AND SEEKING GUIDANCE

To report questionable behavior or potential violations of the principles outlined in the Supplier Code of Conduct, Suppliers and third-party partners are encouraged to raise concerns regarding the adherence to and enforcement of these standards by Telenet Group's Suppliers. Reports can be submitted through the Telenet Compliance Portal.

Reports can be made anonymously through the Portal and will be kept confidential to the extent possible.