



Stellar Code of Conduct

Preamble

STELLAR is a German teleport service provider specialized in connecting America to the Middle East, Africa and Asia providing turnkey satellite and fiber based communication solutions.

However, Stellar operates two so-called teleports in Germany and Cyprus with more than 80 large antennas and a global fiber network ring with nine PoP locations (Points of Presence). With its global coverage, Stellar is the most important partner for bi-directional IP and digital TV distribution platforms as well as customized bandwidth access services.

Stellar commits to comply with a service performance based on transparent value structure. The fundamental values include to protect human dignity, respect for legality and for the law as well as our commitment to guarantee our contractual obligations in full.

To guarantee these values the company management commits to actively put these values into practice and to support them with an open and transparent company culture. This includes the active participation of our employees and partners.

As a global service provider of specialized technical services, Stellar is aware of the risks related to commercial operations. Currently, the main challenge for us is the integrity and availability of our systems, the handling of sensitive data and the compliance with legal standards. We meet these challenges with our conscious entrepreneurial risk management and our Compliance Management System (CMS).

Stellar is a global provider of communication services via satellite and fiber optic

Stellar is a value-based company

We promote a strong and transparent corporate culture

Stellar consider and minimize all possible risks continuously

Aims of the Code of Conduct

This Code of Conduct is a binding commitment to comply with the rules for commercial operations of the Stellar Group. Currently, this includes the Stellar Professional Communications Systems GmbH and its subsidiaries Stellar DBS GmbH (Data Broadcast Services), Stellar BBS GmbH (Broad Band Services) and Stellar Cyprus Ltd.

Hereafter in this CoC we use the word “we” for Stellar and its company group.

The following rules bind the company management as well as the employees, partners, service providers and suppliers. For our customers, this CoC serves as a means of expressing our understanding of compliance and as a demand to assure rigorous compliance with the established rules.

We make this CoC available for all our customers, our associates and for the general public (via our website).

The adherence to this Code of Conduct is intended to avert damages to our company, to our customers, and all those to whom the company feels committed to. This includes, in particular, damages caused by infringements, corruption/bribery, damage of information processing systems, data abuses or improper usage of our system landscapes.

We do not provide services for purposes, which are recognizable of criminal, extremist or terrorist nature. Infringement caused by using our services are not tolerated. In any case, the customer is liable for the contents of the data transferred. For this reason, we strongly request our customers to comply with this guidelines.

The integrity and availability of our systems

High availability and integrity of our systems and services is the essential part of our company values. We are conscious of this fact. Being aware that information processing systems can be disrupted by technical malfunctions or criminal onslaughts, we make all necessary efforts to preserve the integrity and the availability of our systems.

We achieve this by using a continuous Technical Risk Management, with the adherence of technical standards and the creation of an effective Information Management System.

The responsibility for integrity and availability of our systems lies with our Chief Information Officer (CIO). The CIO is responsible to the company management and reports directly to the company management. We

This Code of Conduct applies to the entire Stellar Group

We do promote and request all our partners to comply with this code of conduct actively

We counteract corruption, bribery, forbidden financial transactions and misuse of our IT systems

We do not tolerate terrorist, extremist and criminal activities or ambitions

High availability and integrity of our systems and services is the essential part of our company values.

perform regular internal and external audits to verify the compliance with standards.

Should we determine that our technical systems are disrupted or compromised by criminal activities, we will do everything we can to clarify the situation. If necessary, we will act in cooperation with national authorities.

We have establishing rules to handle information technology systems and provide our employees with binding guidelines in order to avoid IT risks. Our key principles include the securing of our premises against unauthorized access, segmentation and strengthening of our IT infrastructure and a concerted right and role concept.

In the case that we must allow access for third parties to our systems, we require them to comply with our IT standards and check for their compliance regularly.

Loyal, motivated employees

Our most important resource is the knowledge, skills and commitment of our employees, branding Stellar as your trusted partner in the field of high-end telecommunications technology.

It is not only our fiber that is diverse. We benefit from our international team and foster its diversity. To ensure sustainability and quality, we invest time in our employees' skills and training and believe in each employee's potential to achieve great things. We know that the success of our business is entirely dependent on our people. In addition, we invest in our employee`s physical health by promoting healthy diets and physical activities.

We are proud of our diverse team and its commitment.

We are aware that our high technical level, our continuous availability und and our orientation to the requirements of our customers can only be achieved with qualified and motivated employees. For this purpose and deeply convinced, we promote the qualification and identification of our team.

We motivate our employees to speak openly about potentials for optimization. Each employee is able to contact the company management directly, if violations against this Code of Conduct are suspected. We are convinced that an open communication culture offers the most effective protection - we demand all of our employees to live this culture.

We guarantee the availability and security of our system by clear responsibilities and standards

We reduce IT risks by compliance with binding standards

Physical security

Segmentation of networks

Risk-based user concepts

Motivated, loyal and healthy employees have made Stellar successful

We train our employees and we do everything in order to promote a constructive and loyal team structure

We place a great importance on an open communication culture, which offers the most effective protection for our company and our customers

To support this “team spirit” and to keep it in perfect condition, the following binding rules must be observed by all our employees:

Respect for our company values

All employees of the company are committed to a value-based management. They recognize every individual’s dignity and rights and respect their political views and religion. Discrimination of individuals or of whole groups for ethnic, political, religious, sexual or other reasons constitute a serious infringement of our value-based self-image (company culture). Unfavorable treatment or disrespect of others due to the gender, the age, disability or for reasons of descent or origins are irreconcilable with our self-image. All employees will make efforts to prevent the renunciation of this fundamental principles and to speak up for the respect of the above-listed principles.

The company management and the employees prohibit any form of criminality and violations against legal provisions and requirements. Offences and infringements are incompatible with this value-based corporate management.

Prevention of corruption by employees of high integrity

Employees are prohibited from holding out the prospect of any personal advantages for third parties, providing benefits to third parties or receiving benefits for their own actions from customers and suppliers.

If there is reason to suspect that third parties expect personal benefits or offer personal benefits, all employees are obliged to contact company management. This shall also be the case if benefits should be conferred to another person or group (indirect corruption).

We consistently sensitize and train our employees on the basis of an individual and group-specific risk analysis and provide all necessary action strategies for an effective prevention of corruption.

We are keenly aware that personal problems (i.e. liabilities, divorces, grief) or dissatisfaction in a professional context (i.e. conflicts, career ambitions etc.) might favor corruption. In order to take this problems seriously and to find ways and solutions together, we actively encourage our employees to contact the Chief Compliance Officer or the company management in personal matters as early as possible.

The respect for human dignity and non-discriminatory dealings are part of our very strong values

We commit ourselves to political, religious and ideological neutrality

We ostracize every kind of corruption, bribery and corruptibility, and we guarantee the independence of our corporate decisions

Acceptance and presentation of gifts

We are critical of acceptance of individual gift by employees, even if it is accepted in common business practices.

Our employees shall not accept any presents. This applies in particular if the value of the presents exceeds EUR 30.00 and if these gifts are considered to be influencing business decisions and processes. Services, benefits, credit notes etc. are treated in the same way.

The same rules apply to invitations. We are aware that certain employees need to establish and maintain contact with customers. For this purpose business invitations to customers are acceptable. Management provides individual regulations to these employees and reserves the right to deny actions. For all other employees invitations to events or business meals etc. are not allowed.

The principles established above also apply to the presentation of gifts to business partners and invitations for business partners. We take pride in our products and services and not in giveaways.

The size of our company enables us to react to individual issues sensibly. In case of doubt, all employees can contact the Compliance Chief Officer or ask the company management for an assessment.

Careful handling with company property and confidence of our customers

We know that the success of our business is entirely dependent on the availability and integrity of our technical systems. In order to protect our technical communication network of high quality, all our employees are obliged to handle company property carefully. This also requires regular internal audits of our technical security precautions used to protect our properties. Our employees speak proactively about vulnerabilities in security systems and make use of identified optimization potentials conscientiously. All employees are aware of this responsibility.

Sustainable corporate processes

Our commercial operations are based on risk-based, transparent and reliable corporate processes. We set the same standards for our employees as for our corporate activities.

We owe our commercial success to our services, not our gifts or gratuities.

We established clear rules for invitations, acceptance and presentation of gifts or gratuities

We handle carefully and consciously with our company property, protecting the company values and requirements of our customers

Our commercial operations are subject to circumspect and responsible action

Risk-based management

Before entering into new business relations, we perform an obligated risk-based Due Diligence Check. For this purpose we compare information required with information of sources available for the public. This includes:

- Internet research for known fraudulent conduct
- Calibration against sanctions lists (embargoes and terrorist lists)
- Information from commercial data (especially commercial register etc.)

In case of doubts about the integrity and reliability of business partners, in conjunction with this documented process, the Chief Compliance Officer and the company management must be notified. They decide on next steps.

Such basic checks are repeated once a year. In addition, further checks can be conducted if the type of commercial relationship requires further detailed investigations.

Contracts with a volume of less than EUR 1.000.00 are excluded from this regulation.

Compliance with provisions on sanctions and money laundering prevention

Before starting new contractual relationships or continuing existing contractual relationships, we, as a global service provider, make sure that we do not make payments to persons, groups, companies or organizations, which are subject to German, European or international sanctions.

For this purpose, we regularly verify if the above mentioned group is on the publicly available EU or UN sanctions list.

This will be covered by regularly sensitization and training of our commercial departments. All employees of this department are expected to contact the Chief Compliance Officer or the company management directly in case of suspicious facts for fraudulent payments.

Prevention of corruption

Stellar ensures compliance with national and international regulations related to preventing active and passive corruption, bribery etc. For that reason, we do not make payments or provide services to public officials, privileged persons, decision-makers from public bodies, politicians or similar people or groups of persons, with intention of favoring commercial developments.

“One who commits themselves should examine”

We make sure, that we do not maintain business contacts to persons or companies, which have attracted adverse attention as a result of wrongful conduct in the past

We make sure that we do not make payments to persons or groups, which are subject to German, European or international sanctions.

We do not make payments or provide services to politically exposed persons, public officials or other decision-makers

All employees are obliged to take an anti-corruption training annually. In addition, employees with risk functions (sales, accounting, sales force in risk locations etc.) receive a qualification for regulatory compliance. These risk functions are defined by the Chief Compliance Officer.

In addition, we will not tolerate fraudulent activities from third parties on behalf of the company, as referred to in the previous subsection.

Dealing with government authorities

The trustworthy cooperation with government authorities is one of our major concerns. Due to the fact that our business model involves business relations with governmental actors, we carefully weigh the opportunities and risks involved before concluding the contract.

We deal objectively and respectfully with public officials and representatives of national organizations. It is important to us to avoid any concerns about our corporate integrity and to prevent any acts which could be interpreted as corrupt activities.

If we receive any notification that our systems are abused for transmitting contents that may be hateful, terroristic or criminal, we will contact the German authorities. The same shall apply if we assume that our systems are compromised by third parties.

Suspicious of corruptions, disloyalty, embezzlement, wrongful competition and/or abuses of our systems in general will be subject to legal evaluation and criminal proceedings.

Compliance with market conditions

In full awareness of our high quality services, we will refrain from any activities which could expose ourselves to the suspicion of abuse. This includes, beside a responsible management, our strict rejection of cartelization, price agreements, or other influences on the market.

Data protection and data security

As a company and communication provider, we are conscious of the importance of data protection and data security. We ensure the protection of data entrusted to us and all other personal data relating to customers, employees, suppliers etc. We check compliance with data protection regulations by annual audits.

We deal respectfully and professionally with politically exposed persons, public officials or other exposed persons

We support government agencies and cooperate with them responsibly

We do not engage in competitive agreements or create market-dominating monopolies

We ensure the protection of data entrusted to us and we regard the full protection of personal data

We ensure the integrity and technical security of the data entrusted to us by effective, technological and organizational IT security measures. Our employees actively identify and address vulnerabilities and optimization potentials. At regular team meetings, we evaluate all findings obtained and improve our procedural and technical security measures.

Data protection audits and IT security audits guarantee compliance with our data protection and integrity concept

Environment protection and occupational safety

As a value-based company, we are aware of our ecological responsibility. We comply with applicable environmental requirements and refrain from any activity which could lead to environmental pollution. At our locations, we check the environmental impact and protection at regular intervals.

We take our ecological responsibility seriously

Beside the strict observance of environment protection, our primary concern is to ensure the protection of our employees and providers from moral and physical damages or other damages. We regularly train our staff in occupational safety. For this purpose, we provide all necessary documents and information and promote any activities, which ensure a healthy working life.

We promote and require safety at work

Compliance Management System

The company management appoints a Chief Compliance Officer (CCO), who will have responsibility for updating and implementation of the code of conduct. The Chief Compliance Officer reports to the company management regularly and directly.

Our Compliance Chief Officer assumes responsibility for the implementation of the Compliance Management System

The CCO decides on all interpretation issues concerning this Code of Conduct. For this purpose, CCO may call on the expertise of third parties, if required. Once a year, the Chief Compliance Officer initiates an external audit of the Compliance Management System, the data protection audit and the IT security audit.

Each employee is free to ask questions related to the interpretation of this Code of Conduct at any time. Each employee reports abuses and contributes to this continuous development of the Compliance Management System. For this purpose, we make use of the regular team meetings as well as of annual compliance trainings and anti-corruption trainings.

Each employee reports abuses and contributes to the implementation of this code of conduct actively

The Compliance Officer will follow up with any information suggesting a violation of the Code of Conduct.

If a certain circumstance makes it necessary, the Compliance Officer ensures the protection of whistleblower confidentiality. The auditing

findings have to be documented by the Compliance Officer. If necessary, he will call an outside consultant for this purpose.

Violations of the Code of Conduct can result in employment, civil or criminal consequences. The management decides solely about consequences. The Compliance Officer prepares the facts of the case for the decision-making process.

Implementation of the Code of Conduct

This Code of Conduct will be put into effect on March 1st, 2017. This Code of Conduct shall be evaluated once a year and updated as necessary. The evaluation is conducted by the end of the third quarter of each calendar year. Responsibility for the evaluation lies with the Chief Compliance Officer.

*Violations of this Code of Conduct
and other actions that are
detrimental to his company are
consequently prosecuted*