Whistleblowing Policy
TTTech Group

tttech.com

Purpose of this policy

TTTech Group is strongly and unconditionally committed to complying with all applicable laws and regulations. We are also committed to identify any misconduct within the company as quickly as possible, to resolve it and to take necessary remedial actions.

We expect our employees to act in accordance with our quality principles while performing professional duties. All acts, processes and decisions must comply with the applicable laws, standards and other requirements.

In order to maintain these high standards, we encourage every employee to speak up in case they witness or suspect any unlawful, unethical or inappropriate conduct, processes or incidents. We have established a whistleblowing-system, which allows employees, suppliers and customers, thus generally all business partners to report such cases easily and confidentially.

We as TTTech are committed to protect any employees who act as whistleblowers. At the same time, we are determined to prevent the willful dissemination of false and/or malicious accusations. The provisions of this policy will guide whistleblowers in submitting reports and ensure that such reports are investigated thoroughly and with due regard for confidentiality and anonymity. Whistleblowers are not to be sanctioned in any way for information provided in good faith.

Although employees are encouraged to report misconduct, the usage of the implemented whistleblowing system is voluntary. Without exception, the reports serve solely to uncover and remedy misconduct and breaches of laws described in more detail below, but under no circumstances to control employees.

Executive Board

GEORG KOPETZ
CEO

MANFRED PRAMMER
COO

WERNER KÖSTLER
CPO

1. General provisions

1.1. TTTech aims to simplify the process of submitting a report and to assure utmost protection for whistleblowers. The whistleblowing system allows whistleblowers to report breaches, unlawful or unethical conduct within the corporate environment without having to fear any kinds of repercussions. Reporting such incidents helps us as a company to prevent compliance-risks from materializing.

1.2. This policy describes the usage and handling of the whistleblowing system.

2. Scope of this policy

This whistleblowing policy is applicable to individuals with current or prior professional connection with TTTech Group which comprises TTTech Computertechnik AG and all subsidiaries in which TTTech Computertechnik AG holds directly or indirectly at least 50 % of the shares (hereinafter referred to as "Subsidiaries").

It is applicable to all employees (workers, apprentices and if applicable, temporary workers), applicants as well as interns and members of an administrative, management or supervisory body at all corporate locations. Furthermore, the whistleblowing policy is applicable to suppliers and customers, thus all business partners.

3. Reporting breaches

3.1. The usage of the whistleblowing system is voluntary. Whistleblowers may also contact the Compliance Officer ("CO") or the Compliance Representative ("CR") to report breaches.

3.2. The whistleblowing system serves as a tool to report breaches in an easy, confidential and if desired anonymous way. Breaches which may be reported shall concern any areas as defined in the EU-Whistleblowing-Directive (Directive (EU) 2019/1937), in the national (depending on the employee's jurisdiction) whistleblowing laws and in the Code of Conduct. Breaches concerning the following areas are in any case subject to this policy and may therefore be reported using the whistleblowing system:

- Public Procurement
- Financial services, financial products, financial markets and prevention of money laundering and terrorism financing
- Product safety and product conformity
- Traffic safety
- Environmental protection
- Radiation and nuclear safety
- Food and feed safety, animal health and welfare
- Public health
- Customer protection
- Protection of privacy and personal data and security of network and information systems
- Prevention and foreboding of criminal offenses according to §§ 302 to 309 of the Criminal Code (StGB) such as
  - Bribery/Corruption
  - Inappropriate relationships with business partners
  - Violations of antitrust laws
  - Collusion in bidding procedures
  - Abuse of a market-dominating position
  - Abuse of official authority
  - Acceptance of advantage / granting of advantage
  - Acceptance of advantage to influence / granting of advantage to influence
  - Prohibited intervention
  - Forbidden acceptance of gifts
- Property crimes
  - Fraud
  - Breach of trust
  - Theft
  - Tax evasion
  - money laundering and terrorism financing
- Misconduct in payment transactions
  - Financial/economic sanctions and embargoes
- Breaches of privacy and data protection laws, confidentiality rules or IT security rules
  - Breaches of provisions regarding network and information systems
  - Disclosure of confidential information or trade secrets
  - Breaches of confidentiality obligations

If reports are submitted which do not refer to the areas defined above (eg non-illegal or non-unethical circumstances such as wishes regarding contractual arrangements, etc), they will be deferred back to the whistleblower with a corresponding note that no investigation will take place in the matter. If such a report is made anonymously and the whistleblower has not made use of the option to open an anonymous "mailbox" in the system, the report will simply be deleted.

Reports regarding circumstances which do not concern the areas above but are likely to trigger a (legal) duty to act on behalf of TTTech or may be subject to a different procedure (eg harassment) will be forwarded to the responsible internal department (eg HR) with due confidentiality.

4. Ways to submit a report

Communicating openly is the basis of a compliant corporate environment. Thus, witnessed or suspected breaches may be reported and subsequently resolved. TTTech's Executive Board therefore encourages all employees to speak up in such a case using the following options. Any other ways of reporting which are already established remain in place.

4.1. Reporting to the CO/CR

Whistleblowers may report to the CO/CR. Reports to the CO/CR may be submitted in writing (e.g. via e-mail) or orally (personally or by phone).

4.2. Submitting a report using the whistleblowing system

Additionally, employees may use the whistleblowing system to submit a report. Reports can be submitted anonymously upon the whistleblower's request. The whistleblowing system is accessible around the clock. The system also allows for communication between the whistleblower and the person processing the report. This provides a secure electronic communication platform for submitting reports.

The process is as follows: At first, only the CO/CR can read and process the report. The CO/CR is obligated to maintain confidentiality regarding any information received. The whistleblower may – even in the case of an anonymous report – set up a mailbox in the whistleblower system to enable queries and a dialog with the CO/CR. IP addresses, time stamps and metadata of the whistleblower are not recorded; technical traceability is thus impossible.

5. Content of the report

To allow for efficient processing of any reports, the report shall contain all relevant facts of the alleged breach. It is especially important to comprehensively describe the matter, place, time, or duration of the breach as well as information regarding all involved persons and affected legal entities, business areas or departments.

6. Reporting in good faith

Any employee who reports misconduct must act in good faith and have reasonable cause to believe that the breach reported constitutes a violation of applicable laws, regulations or internal policies. Any allegation found to be malicious or knowingly false will result in disciplinary action up to and including the termination of employment, as well as consequences under the law on damages. Bullying and denunciation will not be condoned nor accepted.

7. Confirmation of receipt

Within seven days of submitting the report the whistleblower will receive a note from the CO/CR confirming the receipt of the report. Such confirmation may not be issued if the whistleblower's anonymity prevents this.

8. Internal investigations and further actions

8.1. Every submitted report will be investigated, unless the report does not contain any factual information. The CO/CR will carry out a first relevance check or a preliminary examination of the report. Depending on the type of reported breach the CO/CR will carry out further investigations to resolve the matter. If needed, the CO/CR may consult with third party experts, which are subject to confidentiality provisions.

8.2. Within three months of having received the report, the whistleblower will receive one of the following feedbacks:

- a The reported information has been considered unsubstantiated and/or irrelevant to begin with the investigation because it does not refer to a (possible) breach; or
- b Investigations have been initiated or which follow-up actions have been taken; or
- c The report concerns to another process or department (e.g. HR).

If the investigations are at that time still ongoing, further feedback will be provided to the whistleblower after they have been completed or discontinued.

8.3. Depending on the outcome of the internal investigation TTTech can take appropriate corrective and/or sanctioning measures to the extent required.

Confidentiality and protection of whistleblowers

9.1. Independently of the chosen way to submit a report, whistleblowers may decide for themselves whether they remain anonymous or disclose their identity. In either case strict confidentiality regarding both the whistleblowers' identity and content of the message is guaranteed.

9.2. The content and subject matter of the report as well as involved parties will be kept strictly confidential towards any persons which are not involved in receiving the report, conducting the investigation or, if necessary, deciding on follow-up measures. Disclosing whistleblowers' identity may become necessary under exceptional circumstances; this is the case if the reported matter becomes the subject of an official investigation or court proceedings and the parties involved must be subpoenaed. In addition, disclosure of the identity of whistleblowers as well as the report is required if TTTech is legally obligated by any law or if TTTech is requested to do so by a public authority.

9.3. TTTech assures every whistleblower, who reports a breach of the Code of Conduct, laws, regulations or internal policies in good faith that they are protected against any sorts of retaliation and other adverse consequences. Employees who retaliate against a whistleblower face legal and disciplinary actions, up to the termination of employment.

10. External reporting channels

11.1. This policy encourages everyone of TTTech's employees to speak up if they suspect or witness potential breaches within TTTech to enable timely investigations and corrective actions.

11.2. It is hereby noted that there are also external reporting channels which may be used by whistleblowers. A list of respective authorities may be found in annex 1 to this policy [authorities of all jurisdictions].

11. Data protection

The information provided will be handled in accordance with the GDPR and the DSG. Details e.g. on the processing of personal data and access to personal data can be found in the privacy policy for the whistleblower system.

12. Contact Person

Compliance Offer (CO):

Veronika Benes, LL.M. (NY)
veronika.benes@tttech.com
+43676 84 93 72-4258

Compliance Representative (CR):

Elisabeth Krenn
elisabeth.krenn@tttech.com
+43676 84 93 72-4068

ANNEX 1 - External reporting channels [authorities of all jurisdictions].

Austria:

- Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung: https://www.bak.gv.at/
- Abschlussprüferaufsichtsbehörde (aufgrund des Abschlussprüfer-Aufsichtsgesetzes)
- Bilanzbuchhaltungsbehörde (aufgrund des Bilanzbuchhaltungsgesetzes)
- Bundeswettbewerbsbehörde (aufgrund des Wettbewerbsgesetzes)
- Finanzmarktaufsichtsbehörde (aufgrund des Finanzmarkaufsichtsbehördengesetzes)
- Geldwäschemeldestelle (aufgrund des Bundeskriminalamt-Gesetzes)
- Notariatskammern (aufgrund der Notariatsordnung)
- Rechtsanwaltskammern (aufgrund des Disziplinarstatuts für Rechtsanwälte und Rechtsanwaltsanwärter)
- Kammer der Steuerberater und Wirtschaftsprüfer (aufgrund des Wirtschaftstreuhand-berufsgesetzes)

Finland:

- Office of the Chancellor of Justice

Germany:

- Bundesamt für Justiz
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (auf Grund des Finanzdienst-leistungsaufsichtsgesetzes)
- Bundeskartellamt (auf Grund des Hinweisgeberschutzgesetzes)

Czech Republic:

- Ministry of Justice

Italy:

- National Anti-Corruption Authority (ANAC)