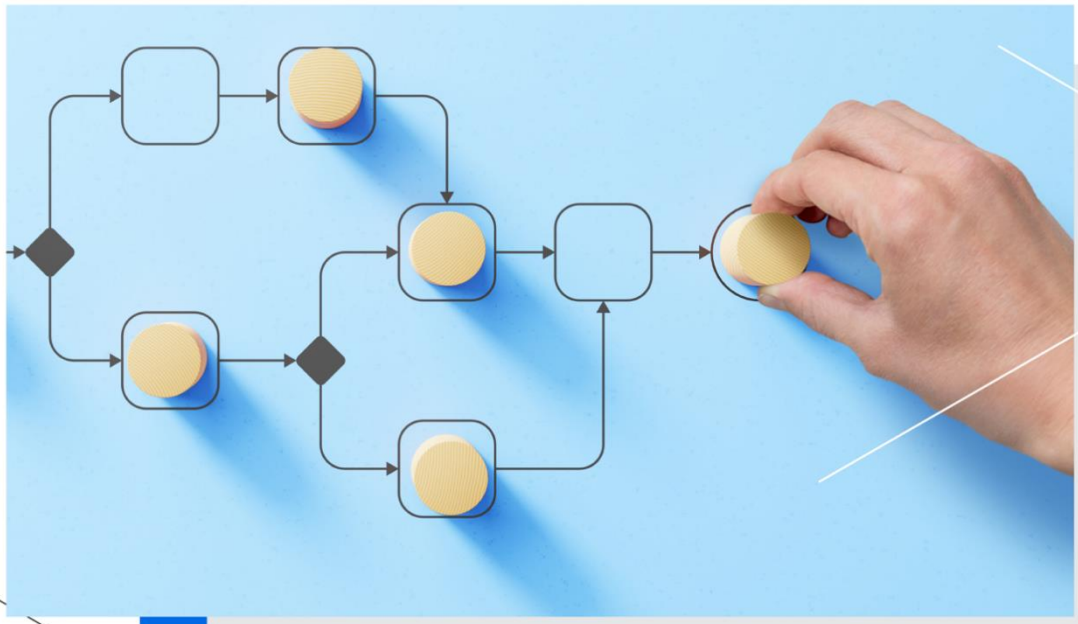
telelink business services



Speak Up
Policy

tbs.tech | simplify the complex

Table of Contents

1. Purpose 2
2. Scope and application 2
3. Responsibilities 2
4. Terms and definitions 3
5. How to Speak Up 4
6. After Speaking Up 5
7. Protection of reporting persons 6
8. False and malicious allegations 6
9. Personal data privacy 7

Change Control 8

1. Purpose

Telelink Business Services Group (for short: "TBSG" or "the Company") is committed to respecting and complying with all applicable laws and regulations in the markets where it operates, while demonstrating open and accountable management, conducting its business with honesty and integrity, and upholding the highest standards in order to protect the interests of its employees and business associates.

The purpose of this policy is to ensure that all employees and business associates of the Company understand how and when to submit signals of violations (confirmed or reasonably suspected), and are protected effectively against any kind of retaliation arising from submitting the signal.

2. Scope and application

This Policy is written in accordance with the European Union's Directive 2019/1937 of 23 October 2019, as well as the respective national laws on whistleblowers' protection across all jurisdictions in which TBSG conducts its business, and covers violations related to various areas, including public procurement, financial services, environmental protection, and information privacy.

This Policy applies equally and with equal weight to all potential, current and former employees, individual contractors, contingent workers, and interns of Telelink Business Services Group, including for the employees of each company in which Telelink Business Services Group controls more than fifty percent (50%) of the voting shares, regardless of the country in which the business is conducted.

Furthermore, this policy applies to all external parties and business associates of the company.

3. Responsibilities

The Company has appointed the members of the **Governance, Risk and Compliance Team** to be responsible for the management of signals of violations as function that will receive, register, and handle the signals.

The members of the **Governance, Risk and Compliance Team** are reporting to the Executive Director of TBSG. Questions about this policy should be addressed to the **Governance, Risk and Compliance Team**.

4. Terms and definitions

"Violation" means unethical or inappropriate behavior, malpractice or illegal practices within the areas[1] of (but not limited to):

- public procurement, financial services, products and markets
- prevention of money laundering and terrorist financing
- product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, and public health
- consumer protection, protection of privacy and personal data, and security of network and information systems.

"Information on violations" means information, including reasonable suspicions, about actual or potential violations, which occurred or are very likely to occur in the organization in which the reporting person works or has worked or in another organization with which the reporting person is or was in contact through his or her work, and about attempts to conceal such violations.

"Signal / to submit signal" means the oral or written disclosure of information on violations.

"Reporting person" means a natural person who submits a signal and discloses information on violations acquired in the context of his or her work-related activities.

"Person concerned" means a natural or legal person who is referred to in the submitted signal and disclosure as a person to whom the violation is attributed or with whom that person is associated.

"Work-related context" means current or past work activities through which, irrespective of the nature of those activities, persons acquire information on violations and within which those persons could suffer retaliation if they reported such information.

"Retaliation" means any direct or indirect act or omission which occurs in a work-related context, is prompted by submission of signal of violations, and which causes or may cause unjustified detriment to the reporting person.

"Initial review" means the analysis of the received information in a signal for the purpose of determining whether the signal falls under the scope of this policy, gives grounds to be considered plausible, contains all the necessary information required in a signal, whether it is

[1] Directive - 2019/1937 - EN - eu whistleblowing directive - EUR-Lex (europa.eu)

appropriate to conduct an in-dept investigation and whether it is necessary to report the signal externally to the respective authorities.

"Internal Investigation" means the process of gathering evidence, reviewing documents, conducting interviews, and examining all circumstances surrounding the alleged violation to determine the appropriate follow-up actions.

"Follow-up" means any action taken by the recipient of a signal to address the alleged violation, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure.

"Feedback" means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up.

5. How to Speak Up

Telelink Business Services Group enables all employees and business associates to make an informed decision on how to submit signals of violations. Such signals may be submitted in writing and/or verbally.

The communication channels through which employees and business associates can submit signals are:

- Speeki platform.
- Via email at ethics@tbs.tech
- In written to the address of the Company, to the attention of the Ethics Commission: Complex Garitage park, Building 1, Floor 4, 2 "Donka Ushlinova" Str., Vitosha area, 1766 Sofia, Bulgaria.
- Via phone call to the following number: +359 2 970 4099
- Via private meeting with representatives of the Governance, Risk and Compliance Team, in cases when the reporting person requests such.

All signals, regardless of the initially used submission channel, are logged in the Speeki platform (for short: "Speeki") for tracking and follow-up purposes.

Any reporting person who submits a signal per this Policy must:

- Disclose information in good faith.
- Have good reasons to believe that the information is correct.
- Not act maliciously or knowingly make false allegations.
- Comply with the law on personal data protection.

Additionally, the reporting person must be prepared to provide the following information:

- Full name, phone number & email address of the reporting person.
- Full name & job title/position in the company of the person concerned (if they are known).
- Specific details of the violation, or of the possibility that such violation will be committed.
- Location where the violation was committed or may possibly be committed.
- Period when the violation was committed.
- Description of the violation and the circumstances surrounding it, as far as these are known to the reporting person.

While Speeki enables anonymous submission of signals, it is important to note that initiating further investigations into anonymous signals may vary for the different local legislations. For Bulgaria proceedings are not initiated based on anonymous signals.

6. After Speaking Up

In order to protect reporting persons and to ensure that the persons concerned are given fair trial, an initial review will be carried out to determine whether it is appropriate to conduct an in-dept investigation and, if so, what form it should take and what type of experts should be involved.

The actions after a signal of violation is received may include:

- Investigation by the Governance, Risk and Compliance Team and / or the Legal Team, supported by other experts within the Company, as appropriate.
- External reporting to the respective competent / law enforcement authorities.

Once a signal of violation is received, the Governance, Risk and Compliance Team will confirm the receipt of the reporting person's signal within **seven days** via the Speeki platform's tools of confidential communication (or via the ethics@tbs.tech email in instances where the initial signal was not submitted via Speeki) as applicable data protection laws allow and, where applicable, will:

- Guide the reporting person on what further steps should be taken.
- Inform the reporting person whether an additional investigation will be carried out.
- Indicate whether the violation will be reported externally to the respective authorities.

The extent of contact between the Governance, Risk and Compliance Team and the reporting person will depend on the nature of the signal, any possible difficulties and the clarity & completeness of the information provided. If necessary, the reporting person may be required to provide additional information.

Follow-up feedback will be provided to the reporting person **no later than three months** from the confirmation of receipt of the signal. Final results of the conducted internal investigation, including information regarding the remedial actions that have been undertaken, will be provided upon conclusion of the internal investigation.

An internal investigation may lead to a report to the relevant law enforcement authorities.

7. Protection of reporting persons

All Telelink Business Services Group employees and business associates who submit signals about confirmed or suspected violations in good faith and in accordance with this Policy will not be subject to any retaliation or adverse consequences.

Telelink Business Services Group employees and business associates will not endure retaliation, discrimination, or disciplinary action (e.g., through threats, isolation, demotion, prevention of progress, transfer, dismissal, bullying, victimization, or other forms of harassment).

All reporting persons may receive legal protection when they provide the information necessary to detect violations falling within the scope of this policy.

In the case of intentional and deliberate submission of signals containing false or misleading information, the reporting person may not benefit legal protection.

Telelink Business Services Group applies all necessary measures to safeguard the identity of reporting persons.

Employees and business associates who submit signals anonymously are also subject to legal protection if they are subsequently identified and retaliated against.

8. False and malicious allegations

Malicious allegations must not be made with the knowledge that they are false. Allegations that are not made in good faith are an abuse of the Speak Up process and as such, Telelink Business Services Group will consider them serious disciplinary violations that may lead to disciplinary action, as permitted by law.

In case the reporting person has received the information about the submitted signal by committing a crime, they bear criminal responsibility according to the applicable local legislation.

In the case of acquisition or access to information which constitutes a criminal offense, criminal liability must continue to be handled by the applicable national law.

9. Personal data privacy

When it comes to processing personal data of reporting persons, persons concerned, or any other involved individuals, Telelink Business Services Group will process only the data required for the purposes of the Speak Up process, as per the established by the Company data protection policies and rules, and to the extent permitted by the applicable data protection legislation.

TBSG applies the necessary organizational and technical security measures to ensure legal and secure investigations and to guarantee that personal data is processed in accordance with the applicable data protection laws and regulations. All signals made under this Policy will be fully treated as confidential, insofar as this is consistent with conducting a full and fair investigation.

Personal data will be processed for the purposes of handling signals of violations and conducting further investigations, if necessary, and in any case only to the extent that is legally permissible and necessary.

The personal data processed will include any information obtained through the Speak Up channels, including the name and contact details of the reporting person (unless the signal is anonymous) and any other provided information in connection with their work in Telelink Business Services Group. The data processed may include personal data relating to violations.

Relevant personal data processed for the purposes specified in this Policy will be **retained for a period of 5 years** after the internal investigation has been concluded.

In instances where a signal of violation has led to criminal, civil, labor and/or administrative proceedings, all records regarding this signal, including the processed personal data, will be retained as long as necessary and legally required.

Change Control

Document Prepared/Updated by

Revision	Date	Name, Surname, Position
01	13.01.2022	Madlena Bozhilova, Business Process Architect
02	12.03.2024	Georgi Gaytandzhiev, Risk and Compliance Expert

Change control

Revision	Date	Change description
01	13.01.2022	New Document
02	12.03.2024	Policy Update according to the Second issue of Bulgaria's Whistleblowers' protection law

Current version

Date of approval	Approved by (Name, Surname, position)
13.03.2024	Ivan Zhitiyanov, CEO