Speak Up Policy

Table of Contents

1. Purpose

Telelink Business Services Group (for short: TBSG or the Company) is committed to demonstrate open and accountable management and to conduct its business with honesty and integrity and upholding the highest standards in order to protect the interests of its employees and business associates, and the community in which we work. The company is also commited to respecting and complying with all applicable laws and regulations in the markets in which we operate.

The purpose of this policy is to ensure that all employees and external parties of the company understand how and when to report breaches, such as unethical or inappropriate behavior, malpractice or illegal practices withouth being penalised in any way, and what type of behavior should be reported.

The policy follows the principles and requirements for internal and external reporting of breaches and the respective high level protection of the persons reporting breaches under the Directive (EU) 2019/1973 of the European Parliament and of the Council of 27 October 2019 on the protection of persons who report breaches of Union law.

2. Scope and application

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 **Business Process Management Team** to be responsible for the management of whistleblowing alerts as function that will receive reports with information on breaches. If necessary, they may require additional information and will further provide feedback. The members of the Business Process Management team are reporting to the Executive Director of Telelink Business Services Group.

All matters concerning this Policy will be consulted with a **Senior Legal Adviser** and **HR Director** when applicable.

Questions about this policy should be addressed to the **Business Process Management Team**.

4. Terms and definitions

"Breaches" means unethical or inappropriate behavior, malpractice or illegal practices within the areas of public procurement, financial services, products and markets, and 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, public health, consumer protection, protection of privacy and personal data, and security of network and information systems, breaches affecting the financial interests of the Union, breaches relating to the internal market, Union competition and aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

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

"Report" or **"to report"** means, the oral or written communication of information on breaches.

"Reporting person" (whistleblower) means a natural person who reports or publicly discloses information on breaches 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 report or public disclosure as a person to whom the breach is attributed or with whom that person is associated.

"Facilitator" means a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential.

"Internal reporting" means the oral or written communication of information on breaches within a legal entity in the private or public sector.

"External reporting" means the oral or written communication of information on breaches to the competent authorities.

"Public disclosure" or **"to publicly disclose"** means the making of information on breaches available in the public domain.

"Work-related context" means current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches 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 internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.

"Follow-up" means any action taken by the recipient of a report or any competent authority, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, 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.

"Competent authority" means any national authority designated to receive reports and give feedback to the reporting person, and/or designated to carry out the duties provided for in this Directive, in particular as regards follow-up.

5. How to Speak Up

Telelink Business Services Group enables all employees to make an informed decision on how to report violations. Such reports may be done in writing - anonymously or not anonymously.

The communication channels through which employees can submit signals are:

- Speeki platform.
- Through email at ethics@tbs.tech.
- In written to the address of the Company to the attention of the Ethics Commission.

Any employee who reports a violation as per this Policy must:

- Disclose information in good faith;
- There are good reasons to believe that the information is correct;
- Does not act maliciously or knowingly make false allegations;
- Complies with the law on personal data protection.

After the report has been submitted, it will be directed only to the function responsible for management of such signals.

6. After Speaking Up

In order to protect persons and those suspected of the alleged infringement, an initial investigation will be carried out to determine whether it is appropriate to conduct an investigation and, if so, what form it should take and what type of experts should be involved.

Further, the actions after reporting a breach may include:

- Investigation by the Business Process Management team and / or the Legal Department, supported by others within the Telelink Business Services Group, as appropriate.
- External reporting to the respective competent/ law enforcement authorities.

Once a breach has been reported, the Business Process Management team will confirm the receipt of the whistleblower's report within seven days in a way indicated by the sender, as applicable data protection laws allow and, where applicable, will:

- Guide how the whistleblower should handle the case;
- Inform the whistleblower whether an initial review of the case will be carried out;
- Indicate whether or not an additional investigation will be carried out.

Feedback will be provided to the whistleblower no later than three months from the confirmation of receipt of the alert.

The extent of contact between Telelink Business Services Group and the whistleblower will depend on the nature of the reported issue, the possible difficulties and the clarity of the information provided. If necessary, Telelink Business Services Group will seek additional information from the whistleblower.

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

7. Protection of whistleblowers

All employees who report concerns and / or suspicions in good faith in accordance with this Policy will not be subject to any retribution or adverse consequences. Telelink Business Services Group employees will not endure retaliation, discrimination or disciplinary action (eg through threats, isolation, demotion, prevention of progress, transfer, dismissal, bullying, victimization, or other forms of harassment).

All employees may receive legal protection when they provide the information necessary to detect an infringement falling within the scope of this policy.

In the case of intentional and deliberate submission of false or misleading information, the employee may not benefit legal protection.

Employees who report anonymously are also subject to legal protection if they are subsequently identified and retaliated against.

8. False and malicious allegations

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

In case the whistleblower has received the information about the violation by committing a crime, he bears 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

Telelink Business Services Group will process employees' personal data only required for the purposes of this Policy as per the established by the Company data protection policies and rules and to the extent permitted by the applicable data protection legislation.

The Company applies the necessary organisational and technical security measures to ensure legal and secure investigations and to guarantee that personal data is processes in accordance

with the applicable data protection laws and regulations. All reports 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 submission of breach report and further investigation, 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 whistleblowing channels, including the name and contact details of the whistleblower (unless the whistleblower is anonymous) and any other provided information in connection with their work in Telelink Business Services Group. The personal data processed may include personal data relating to offenses.

Relevant personal data processed for the purposes specified in this Policy may be stored for as long as necessary and legally permitted (but no longer than one calendar year after closure of the investigation and resolving of the breach).

Personal data processed in connection with a report of a breach that does not lead to further investigation or that is unfounded will be deleted immediately.

Change Control

Prepared / Updated current version

Revision	Date	Name, Surname, position
01	13.01.2022	Madlena Bozhilova, Business Process Architect

Change control

Revision	Date	Change description
01	13.01.2022	New Document

Current version

Approved by (Name, Surname, position)	Ivan Zhitiyanov, Chief Executive Director
Date of approval	16.05.2022