

Compliance Management System - EuroTeleSites Group

-

Whistleblowing Policy

Whistleblowing Policy - Updates:

Edition	Update by	Issue date	Updated chapters	Cause of update
1.0	Compliance Officer - Guillaume Dubois	04/11/2024	Creation of the document	First edition

Approval

Approved by: Management Board



Table of Contents

- 1. Introduction and background 3
 - 1.1 General..... 3
 - 1.2 Validity Area 4
- 2. EuroTeleSites Whistleblowing Policy 5
 - 2.1. Possible ways to report a concern: 5
 - 2.2. Receipt of whistleblowing reports..... 6
 - 2.3. Processing of whistleblowing reports..... 6
- 3. Whistleblower protection 8
 - 3.1. Reporting retaliation 8
 - 3.2. Protection against retaliation 8
 - 3.3. Investigation of reported retaliation 8

1. Introduction and background

1.1 General

At EuroTeleSites, we make a conscious choice to commit ourselves to the highest standards of integrity towards all our stakeholders. Only by following an honest, fair, and transparent way to conduct our business we are able to fulfill our vision to provide the sustainable foundation for the digital transformation.

Integrity has a central place in our values. We consider that the right results can only be obtained by going the right way and that integrity is more important than short term business success. In this matter, it is everybody's responsibility to always act ethically and in compliance with applicable laws and regulations.

Our Compliance Management System (CMS)

In order to ensure integrity and trustworthiness within EuroTeleSites Group, we have implemented a CMS designed to work effectively by using the 3 pillars: prevent, detect and react.

Prevent: we implement relevant compliance guidelines that are fixing clear rules for all stakeholders, also in our purchasing process regarding right business conduct from our suppliers and other business partner. We conduct a yearly compliance risk assessment to identify risks and potential for improvement, define measures to effectively manage those risks and proceed to regular reviews on it.

Detect: we implement permanent and periodic controls and audits to be able to detect compliance cases or problems. The [whistleblowing platform](#) is also a central part of the detection process. Each stakeholder can help us strengthen our compliance by signaling violations of laws and rules.

React: each detected case is then duly investigated by Compliance Office. If a violation is confirmed, we discipline such deliberate, unlawful misconduct consistently, regardless of the rank or position of the person involved. Also, business partners have to expect appropriate consequences in case of breach of contractual compliance obligations or violations of anti-corruption laws.

Whistleblowing

Misconduct and violations of conduct standards have serious consequences not only for the individual as a person, but also for the entire company. For this reason, misconduct cannot be tolerated. Managers have a special role model function in this regard. We are committed to ensure that the company fosters a culture where our employees and all stakeholders are encouraged to report concerns without fear of retaliation.

“Whistleblowing” means any report that raises concerns about possible violations, unlawful or irregular conduct or behavior, including omissions, which fail to comply with national or

European Union laws and regulations, thereby potentially harming the public interest or undermining the integrity of the EuroTeleSites Group.

We put great value on confidentiality and guarantee the anonymity and protection of the whistleblower, the reported person and of any further persons involved in the report (e.g. “facilitators”, family members, colleagues, etc.) in accordance with applicable legislation. Thus, any whistleblower can choose to send us a report anonymously.

EuroTeleSites will not retaliate and will not tolerate any retaliation against an individual for raising good-faith and genuine concern or for participating in the investigation of any report. Any person who retaliates against a whistleblower, threatens any such retaliation, or is involved in any such conduct may be subject to disciplinary action, up to and including termination of employment or any kind of contractual relationship with EuroTeleSites Group.

1.2 Validity Area

This Policy applies to all current and former employees, customers, suppliers, and any other stakeholders and sets out EuroTeleSites approach to managing the whistleblowers’ reports and to protecting and supporting individuals who report potential misconduct.

This Policy is valid in its current form for EuroTeleSites AG and all its subsidiaries.

1.3 Legal Basis

EuroTeleSites whistleblowing system is in line with the EU Whistleblowing Directive as well as the Austrian Whistleblower Protection Act (HinweisgeberInnenschutzgesetz). National legal requirements may extend or limit some provisions of this Policy and in such case, the national legal requirements shall prevail over the provisions of this Policy.

1.4 Purpose

The purpose of this Policy is to promote and facilitate whistleblowing, as well as to provide guidelines for the process of transmitting, receiving, managing and filing whistleblowing reports.

This document aims mainly to:

- clarify that any stakeholder may make reports;
- define the minimum requirements for a report to be processed by the Compliance Office;
- identify the roles and responsibilities, as well as the principles and general rules governing the process, including the procedures for managing the investigation and the protection of the whistleblower and the reported person, in compliance with the legislation on the protection of personal data;
- define the maximum timeline for processing a report and communication with the whistleblower.

2. EuroTeleSites Whistleblowing Policy

Information provided by honest employees is one of the most effective ways of exposing misconduct in the company and is therefore an appropriate measure to expose serious risks at an early stage within EuroTeleSites Group.

Any employee, but also any other person concerned, can report a violation or suspected violation of legal provisions, EuroTeleSites Code of Conduct and internal guidelines. We encourage reporting if a person has knowledge of, or reasonable grounds to believe, in light of the circumstances and the information available to them at the time of reporting that the matters reported by them are true. Nothing negative will happen to honest whistleblowers who have provided information to the best of their knowledge. This also applies to tips that are not covered by local whistleblower protection laws.

Potential whistleblowers may approach the Compliance Office to seek guidance and support on:

- whether a potential report would be covered by this Policy;
- which reporting channel may be best for communicating the relevant information;
- which alternative procedures are available if the information does not qualify for whistleblowing;
- advice and guidance on protective measures that may be applicable following the reporting, or on any other question related to this Policy.

2.1. Possible ways to report a concern:

As internal whistleblowers, you may approach your direct manager for initial support. If a manager receives a whistleblower report, only the Compliance Office must be immediately notified of this report in written via email to compliance@eurotelesites.com, otherwise the report must be kept confidential. Alternatively, whistleblowers may address their concern directly to the compliance office (email to: compliance@eurotelesites.com).

Information can also be provided through the EuroTeleSites Group [whistleblowing platform](#) in written or by using the voice recording functionality. The details will be investigated and verified confidentially and by persons committed to confidentiality.

If you wish, you can remain completely anonymous. In this case, please observe the option to set up an electronic mailbox in the [whistleblowing platform](#) so that you can remain in contact with the Compliance Office anonymously during the investigation. But please keep in mind that it may be more difficult to investigate an anonymous report due to difficulty in obtaining specific details and/or answers to follow-up questions.

In case the potential report concerns the Head of Audit & Compliance, or the EuroTeleSites CFO as direct supervisor of the Compliance Office, whistleblowers can send the report to our Ombudsman (wkklaw - Wess Kux Kispert & Eckert Rechtsanwalts GmbH, Himmelpfortgasse 20/2, 1010 Vienna), that confidentially receives and processes reports about suspected violations/irregularities via email at eurotelesites@wkklaw.

Alternatively, information can also be provided to local competent authorities in accordance with the statutory provisions while maintaining the legal protection of whistleblowers.

2.2. Receipt of whistleblowing reports

The whistleblowing report must meet certain minimum requirements in order to be processed and for Compliance Office to be able to carry out the subsequent investigation of the events that have occurred, when necessary.

Specifically, the report must contain the information detailed below:

1. Identification and contacts of the whistleblower unless they choose to remain anonymous.
2. A description, as solid as possible, of detailed events that occurred, whenever possible:
 - The company in EuroTeleSites Group concerned by the report.
 - The kind of breach of legislation and/or other internal regulations.
 - Dates of occurrence of the events described above (as accurate as possible).
 - Persons allegedly involved.
 - Details about the reported wrongdoing which will be the basis for opening an investigation by Compliance Office.
 - The whistleblower relationship to EuroTeleSites.

The Compliance Office can start the evaluation, investigation and resolution of the reports, only if they contain the minimum requirements detailed in this section.

Whenever possible, we recommend providing documents, witnesses, or any evidence, in whatever format, to support the report of the facts that have occurred. Providing such elements is very important in order to facilitate the gathering of evidence on the reported facts and to conduct the investigation promptly and effectively.

2.3. Processing of whistleblowing reports

After receiving a new whistleblower report, the Compliance Office 1/ confirms formally the reception of the report at least within the legal deadline of 7 days, 2/ analyzes the information transmitted by the whistleblower to assess roughly the characteristics and the plausibility of the information regarding the reported violation or wrongdoing. If those elements are not sufficient, the Compliance Office may contact the whistleblower to requires further elements, information, explanations or evidence.

After this first analysis, and within max. 7 days, the Compliance Office decides if an investigation have to be performed or not. An investigation will not be conducted if the information transmitted by the whistleblower are obviously false, significantly insufficient or clearly not represent a case of violation. Oppositely, if the facts and evidence are sufficiently clear to demonstrate a violation, an internal investigation may be not necessary.

The internal investigation is then handled by the function “Internal Audit” (which is in the same department at EuroTeleSites Group). Internal Audit acts under mandate of the Management Board and received authorization to launch an internal investigation from the Management Board. If a member of the Management Board is involved in the report of the whistleblower, Internal Audit receives authorization to launch internal investigation from the Chairperson of the Supervisory Board. In urgent case (evidence may be deleted...), Internal Audit can launch

internal investigation without authorization. Authorization shall then be gathered ex-post. The principle of independent investigation in the interest of the company integrity shall prevail against other principles (e.g. principle of respect of internal decision process...).

Internal Audit conducts the internal investigation by using mainly two ways: 1/ gathering information and evidence, 2/ interviewing concerned persons.

1/ Based on the EuroTeleSites' Internal Audit Charter, Internal Audit disposes of general right for full, free and unrestricted access to any and all data, IT-systems, physical properties of the company. Access to information useful to the internal investigation cannot be denied. All requested information has to be provided in a truthful and complete manner within a reasonable period of time. Internal Audit is committed to require and safeguard only data necessary and useful in the context of the internal investigation. Data and information are saved with very restrictive access right (only employee from Internal Audit have access).

2/ Also based on the EuroTeleSites' Internal Audit Charter, Internal Audit has full right to inquire employees and management to carry out its activity. All employees and management are requested to assist Internal Audit in accomplishing their audit tasks. This can be as witnesses as well as reported persons. Internal Audit informs the reported persons about the accusations against them so that they can defend themselves in time. Reported persons are informed that they can require the support of a person from the work council during the interview. Interviews in the context of internal investigation are subject to detailed minutes containing the questions of Internal Audit and the answers given by the interviewee and are signed by both parties.

Depending on the involved level, Internal Audit may require support from the local management or legal expert (regarding matters of languages or national laws).

After analyzing all available information and evidence, Internal Audit decides independently and consciously upon the end of investigation and the conclusion to give to the alleged violation. Internal Audit writes a report for each case of internal investigation containing the whistleblower reported information, the performed investigating activities, the facts as Internal Audit can reasonably present them objectively and a conclusion on the case. An ad hoc compliance committee, involving HR, Legal and the Compliance Office decides on measures to take given the conclusion of Internal Audit (incl. disciplinary measures). The Compliance Office only recommends measures but does not take part in the decision-making. The report is transmitted to the member of the Management Board concerned, which decides alone on forwarding to other persons and/or local level. In case of serious evidence of violation of laws representing criminal offences, the Compliance Office with the Head of Legal and the company external legal counsel assesses and decides about indictment (incl. self-indictment). The prevailing objective is to avoid the most possible negative consequences for EuroTeleSites Group.

Data protection

We collect and process personal data within the framework of this Policy in accordance with European and national data protection regulations, in particular the General Data Protection Regulation (GDPR).

Whistleblowers are informed of the processing of their personal data when registering a new report on the [whistleblowing platform](#), if they did not choose to remain anonymous. Whistleblowers are entitled to access, rectify and (in certain circumstances) block their data by contacting the Compliance Office, as it is responsible for investigating their report.

Personal data which are manifestly not relevant for the handling of a specific report, shall not be collected or, if accidentally collected, shall be deleted without undue delay.

Data is usually stored until the follow-up activities related to the result of the investigations are completed. It may be stored longer in case of legal disputes of criminal proceedings, but in any case, no longer as allowed by applicable legal requirements.

3. Whistleblower protection

The Compliance Office is responsible for the operational implementation of whistleblower protection. Whistleblowers can turn to this department if they feel they have been adversely affected by any form of (perceived) disadvantage as a result of the whistleblowing. Whistleblower protection does not apply if knowingly incorrect information is provided to the detriment of the company or its employees.

3.1. Reporting retaliation

Whistleblowers who believe that they have been victims of retaliation or have valid reasons to believe that they are exposed to a risk of retaliation, should immediately report the matter to the Head of Internal Audit & Compliance via email at compliance@eurotelesites.com or through the [whistleblowing platform](#) (choose “retaliation” category). Alternatively, the report can be made to the Ombudsman (wkklaw - Wess Kux Kispert & Eckert Rechtsanwälts GmbH Himmelfortgasse 20/2, 1010 Vienna), that confidentially receives and processes reports about suspected violations/irregularities via email at eurotelesites@wkklaw.at.

A person who submits a complaint of retaliation must establish the respective facts with information or documentation in support of the complaint. A complaint of retaliation shall be treated as strictly confidential and will not interfere with the investigation of the reported allegation of misconduct unless the retaliation constitutes a form or an attempt of obstruction.

It shall be up to the individual who has allegedly committed the retaliation act to prove that there is no causal link between the whistleblowing report and the alleged retaliation act, i.e. that the act is not a retaliation against the Whistleblower.

3.2. Protection against retaliation

When a whistleblower can reasonably demonstrate that he is threatened with retaliation or retaliated against because of the reported information, the Head of Internal Audit & Compliance shall provide appropriate assistance to secure their protection. Should the retaliation or the threatened retaliation come from the Head of Internal Audit & Compliance, the Head of HR shall provide appropriate assistance to secure the whistleblower's protection. The Head of Internal Audit & Compliance shall assess the circumstances of the case and may recommend to the Management Board or local General Manager, as applicable, that temporary and/or permanent measures be adopted to protect the whistleblower and mitigate the possibility of retaliation and consequences of retaliation.

3.3. Investigation of reported retaliation

Based on the reported retaliation, only when receiving information backed by facts and/or documents (e.g.: removing the whistleblower from its position, written threats, restricting the whistleblower's access to previously available information/premises) an investigation can be launched. The Head of Internal Audit & Compliance shall assess the matter without undue

delay and may launch an inquiry. Whistleblowers shall not lose protection if their reports cannot be substantiated.

If an investigation finds that an employee of EuroTeleSites has committed an act of retaliation, that employee shall be subject to disciplinary proceedings. The relevant Group company shall also consider adopting any other measures necessary to remedy the retaliation.

The whistleblower shall be informed in writing (by the same way of communication in which the info about retaliation was received by Compliance Office) of the measures to be adopted, if any.

Abusive, false or malicious allegations, particularly if they are based knowingly on false or misleading information, may also lead to disciplinary and criminal proceedings, as applicable.