

WHISTLEBLOWER REPORT MANAGEMENT PROCEDURE

TECNIKABEL S.p.A.

Revised	Approved	Modified	Issue date
00	Board of Directors	First issue	2024

CONTENTS

1.	INTRODUCTORY REMARKS.....	2
2.	NORMS AND REGULATIONS	2
3.	PROCEDURE PURPOSE AND FIELD OF APPLICATION	3
4.	TERMS AND DEFINITIONS.....	3
5.	REPORTING METHODS AND CHARACTERISTICS	3
5.1	WHO CAN FILE A REPORT: THE WHISTLEBLOWER.....	3
5.2	ANONYMOUS REPORTS	4
5.3	SUBJECT OF A REPORT: WHAT CAN BE REPORTED?	4
5.4	HOW TO FILE A REPORT.....	5
6.	WHISTLEBLOWING REPORTING CHANNELS AND PROCEDURE	6
6.1	REPORTING CHANNELS	6
6.2	INTERNAL REPORTING CHANNEL: THE SESTANTE WEB PORTAL	6
7.	HOW TO MANAGE THE REPORT	7
7.1	PARTIES ENTRUSTED WITH MANAGING THE REPORTS	7
7.2	WHISTLEBLOWERS - INTERNAL WHISTLEBLOWING COMMITTEE	7
7.3	SAFEGUARDS AND RESPONSABILITIES OF THE WHISTLEBLOWER/REPORTER	8
8.	DISCIPLINARY SANCTIONS.....	10
9.	TRAINING AND INFORMATION.....	10
	OPERATING INSTRUCTIONS FOR THE	11
	“SESTANTE” WEB-BASED WHISTLEBLOWING PORTAL.....	11

1. INTRODUCTORY REMARKS

TecniKabel S.p.A. (hereinafter referred to as the Company) has set up an internal communication channel to file reports of actual or alleged violations. The reporting flow is carried out with the utmost respect for the person reporting the breach, their protection, and without fear of retaliation.

2. NORMS AND REGULATIONS

- ⇒ Directive 1937/2019.
- ⇒ Regulation 679/2016, or GDPR.
- ⇒ Italian Legislative Decree No. 24/2023, implementing European Directive No. 1937/2019 on whistleblowing. This decree repealed provisions provided for by Law No. 179/2017 for the public sector and Legislative Decree No. 231/2001 for the private sector.
- ⇒ Legislative Decree 231/01, dated 2001, governing the administrative liability of legal persons.
- ⇒ Draft guidelines on the protection of persons reporting breaches of European Union law and protection of persons reporting breaches of national law - Procedures for the submission and management of external reports - ANAC (National Anti-Corruption Authority).

3. PROCEDURE PURPOSE AND FIELD OF APPLICATION

The aim of this procedure is to:

- ✓ **Promote** a corporate culture based on transparency, accountability and integrity;
- ✓ **Establish and raise awareness** of the internal reporting channel of communication;
- ✓ **Define responsibilities for the whistleblowing management process**;
- ✓ **Illustrate the safeguards, or protection system, provided for the whistleblower in accordance with the law**;
- ✓ **Illustrate the sanctions system** provided for in the legislation against the Company and whistleblower.

The present procedure applies to TecniKabel S.p.A.

4. TERMS AND DEFINITIONS

WHISTLEBLOWER: An individual who files a whistleblowing report concerning alleged breaches in their work-related context.

BREACHES: Conduct, acts or omissions that are detrimental to the public interest or the integrity of a public administration authority or private-sector entity

WORK-RELATED CONTEXT: work or professional activities carried out in the past or present as part of relationships with the company through which (regardless of the nature of such activities) a person acquires information on breaches and within which context they could suffer retaliation in the event of a reports or public disclosure.

A REPORT: A concern raised by a whistleblower/reporter providing information on one or more breaches.

INTERNAL REPORT: A written or oral provision of information on breaches submitted through the internal reporting channel employed by the Company for this purpose.

EXTERNAL REPORT: the written or oral provision of information on breaches submitted through the external reporting channel (managed by ANAC).

PUBLIC DISCLOSURE: the publication of information on breaches either through the press or online (including social media) using means of dissemination with the potential to reach a wide audience.

JUDICIARY AUTHORITY REPORT: Possibility to file a complaint with the relevant national judiciary or audit authority concerning an alleged violation or breach in a private or public work-related context.

RETALIATION: Any conduct, or act or omission (even if only attempted or threatened) put in practice as a result of the report, which constitutes - or may constitute - either directly or indirectly, a tort against the reporter or the person who made the complaint or public disclosure.

ANAC: National Anti-Corruption Authority (<https://www.anticorruzione.it>)

FACILITATOR: An individual who assists a reporter during the reporting process, who works within the same work-related context and whose assistance must be kept confidential.

5. REPORTING METHODS AND CHARACTERISTICS

5.1 WHO CAN FILE A REPORT: THE WHISTLEBLOWER

The Company, in compliance with legislation in force, identifies the following as potential whistleblowers:

INTERNAL STAKEHOLDERS:	EXTERNAL STAKEHOLDERS:
<ul style="list-style-type: none"> • All employees, irrespective of their contractual status, role or function. • Persons performing administrative, management, business control, oversight, or representatives (senior figures), even if these roles are performed on a purely de facto basis. 	<ul style="list-style-type: none"> • Independent contractors and self-employed workers who provide goods or services or perform work on behalf of the company. • Volunteers and paid and unpaid workers on trial periods who perform work-related activities inside the Company. • Self-employed professionals, and external consultants who provide the Company with their services.
ADDITIONAL PERSONS ALSO COVERED BY WHISTLEBLOWER PROTECTION	
<ul style="list-style-type: none"> • Facilitators. • Persons sharing the same work environment, with fourth degree kinship relationships and with stable emotional ties to the whistleblower. • Work colleagues sharing the same work environment with a current relationship on a regular basis with the whistleblower (e.g. close friendship). • Bodies owned by the whistleblower, or bodies for which the whistleblower works, or bodies operating in the same work environment (the reason being, in such cases, to safeguard such bodies, for example, from retaliation of a commercial nature). 	

A report may be filed during a selection process or other pre-contractual activities, during a trial period, or after termination of a legal relationship.

This procedure refers to cases in which the whistleblower discloses their identity. The aim is to ensure that the persons involved are afforded the protection and safeguards provided for by the legislation, thereby guaranteeing the confidentiality of the personal details they have provided.

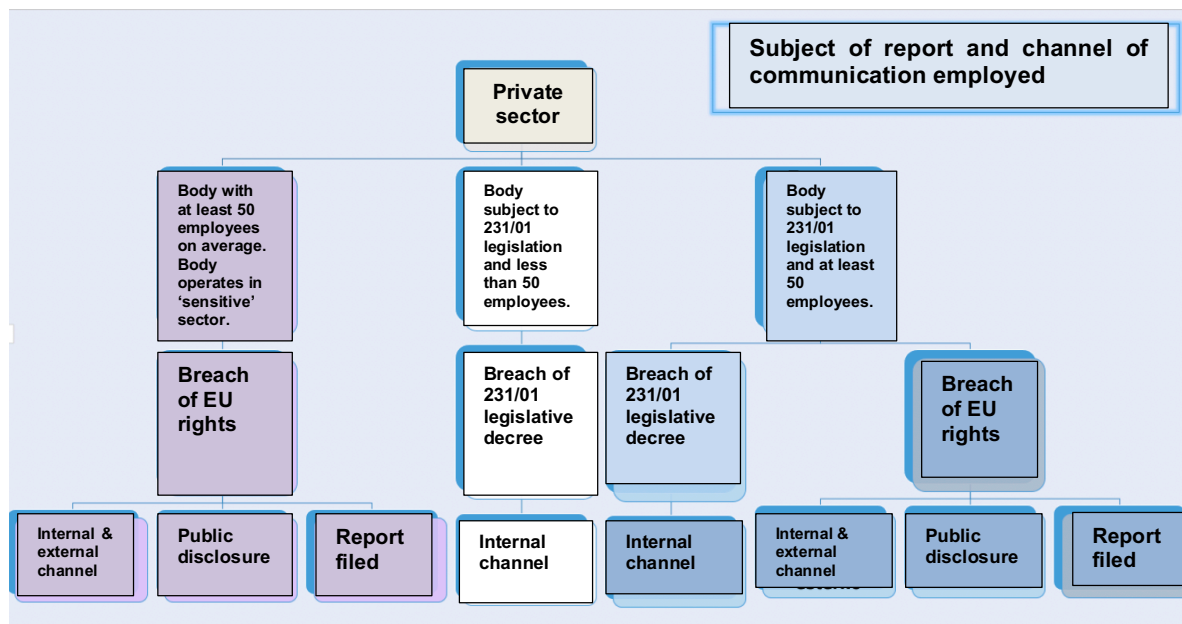
5.2 ANONYMOUS REPORTS

Anonymous reports shall be considered 'standard' reports, even if channelled through the internal channel of communications. Safeguards apply to an anonymous, subsequently identified, whistleblower who has reported to the ANAC that they have suffered retaliation.

In the case of an anonymous report, content is decisive in order to judge its admissibility and suitability to be taken into account. Therefore, only reports that are substantiated and accompanied by evidence shall be taken into due consideration.

5.3 SUBJECT OF A REPORT: WHAT CAN BE REPORTED?

The law differentiates between the various subjects of a report depending on the nature of the legal parties involved. The table below summarises what can be reported and through which channel:



Source: ANAC guidelines

Generally speaking, the report may concern any conduct covered by Legislative Decree 231/01, any alleged or ascertained breaches of Standard 231 or the Code of Ethics, or any offences considered relevant within the EU framework of competence and therefore affecting the financial interests of the European Union.

By way of example and without limitation, the report may concern::

- ⇒ **Active and passive corruption.**
- ⇒ **Behaviour aimed at obstructing controlling activities of oversight authorities (e.g. failure to produce documentation, submission of false or misleading information).**
- ⇒ **The promise, or the giving of money, goods or services, or other benefits with the intent to bribe suppliers or customers.**
- ⇒ **Unlawful tax, accounting and financial practices.**
- ⇒ **Tax fraud.**
- ⇒ **Violation of human rights.**
- ⇒ **Environmental, occupational health and safety offences.**
- ⇒ **Illicit use of personal data or blatant violation of privacy laws.**
- ⇒ **Breach of unfair competition or state aid regulations.**
- ⇒ **Breach of the Code of Ethics and corporate organisation, management and control regulations.**

Harassment, instances of workplace abuse and/or discrimination regarding gender, ethnicity, religious faith, or sexual orientation may all be reported in order to ensure that the health and dignity of workers, as well as the moral integrity and values of the Company are safeguarded.

5.4 HOW TO FILE A REPORT

Reports should preferably contain the following elements:

- ⇒ **A full description of the facts being reported.**
- ⇒ **If known, the circumstances (time and place) in which the ascertained or alleged breaches were committed.**
- ⇒ **Details (qualification, office, activity carried out) of the reported person in order to enable them to be identified.**
- ⇒ **Details of any witnesses or persons who can report on the facts detailed in the report.**
- ⇒ **Any attachments or documents that may validate the facts detailed in the report.**
- ⇒ **Any other information that may provide useful in order to support to alleged facts in the report.**

The following are also potential subjects of reports and are therefore admissible:

⇒ ***Details of retaliation that the reporter believes they have suffered as a result of a report.***

Alleged retaliation may also be the subject of a report. Retaliation must be communicated solely to ANAC. Union representatives are not permitted to notify ANAC of alleged retaliation on behalf of the reporting party.

The following instances are INADMISSABLE and excluded from the above list of admissible reports:

⇒ ***Personal grievances of the reporter, which concern exclusively their individual working relationships with colleagues or persons above them in the organisation.***

⇒ ***Conjecture, suspicions or hearsay.***

⇒ ***National security breaches.***

6. WHISTLEBLOWING REPORTING CHANNELS AND PROCEDURE

6.1 REPORTING CHANNELS

The legislative decree foresees potentially more than one channel of reporting:

Internal channel of communication	External channel of communication: ANAC	Public disclosure	File a police report
Reporting channel set up by the Company.	<p>The whistleblower may choose to report through ANAC when:</p> <ul style="list-style-type: none"> the internal reporting channel is not active or does not meet legal requirements (e.g. when it does not guarantee confidentiality). they have already filed an internal report without receiving a response. they fear that the report may give rise to the risk of retaliation. they fear that the breach may constitute an imminent or obvious danger to the public interest. 	<p>The whistleblower may report by public disclosure through the press, media, or social media, when:</p> <ul style="list-style-type: none"> they have already filed a report internally and/or to ANAC without receiving a response. they fear that the report may give rise to the risk of retaliation. they fear that the breach may constitute an imminent or obvious danger to the public interest. 	<p>Finally, the decree also grants the whistleblower the right to report unlawful conduct constituting a criminal offence directly to the national authorities.</p>

6.2 INTERNAL REPORTING CHANNEL: THE SESTANTE WEB PORTAL

The Company has set up a dedicated internal reporting channel for any potential whistleblowing.

The platform uses the customised SESTANTE web-based portal. This portal guarantees legal and regulatory compliance, including the processing, organisation and management of personal data, and privacy (Legislative Decree no. 196/2003 - Personal Data Protection Code; and EU Regulation 2016/679 on the protection of personal data).

The platform ensures effective, confidential communications by allowing all internal and external stakeholders to send reports to those internal persons who have been authorised to handle whistleblowing reports.

The platform can be accessed from the official Company website or at the following link:

<https://tecnikabel.software231.eu>.

Before filing a report, the whistleblower is asked to read a privacy statement regarding the processing of their personal data.

The reporter may choose to file a report and include personal details, or file a report completely anonymously by simply entering the subject of the report and the topic.

Once the report has been entered, the platform assigns it a unique **ticket code**. The reporter must make a note of this code, and keep it safe, as it allows them to check the status and progress of the report.

When the report has been filed, the reporter will receive either notification of receipt or notification directly on the platform itself.

The platform allows a person wishing to file a report, to make a written report.

Please refer to "**Operational Instructions for Using the Web Whistleblowing Platform**" for further details regarding the use of the platform.

The whistleblower may always request to be heard in person. The suggestion in this case, however, is to access the platform regardless, and file this request in the descriptive fields provided in order to track the request and maintain confidentiality.

7. HOW TO MANAGE THE REPORT

7.1 PARTIES ENTRUSTED WITH MANAGING THE REPORTS

ANAC Guidelines stipulate that the following persons may be entrusted with managing the internal reporting channel referred to in the previous paragraph:

- a. a person in the administration department/inside the organisation or body
- b. a dedicated office inside the administration department/a body with specifically appointed staff
- c. a third party

In the event the organisation decides to outsource reporting channel operations to an external third-party, it, however, remains responsible for following up the report, dealing with any ascertained breach, and providing feedback to the whistleblower. It is therefore always necessary for an organisation to appoint at least one internal contact person.

7.2 WHISTLEBLOWERS - INTERNAL WHISTLEBLOWING COMMITTEE

The Company has set up an internal whistleblowing committee which is responsible for receiving and handling whistleblowing reports. The Committee is composed of:

- **Diego Clerici - external consultant for General Affairs.**

The Committee has the task of analysing all reports received from the Company.

The Committee members are appointed as "persons authorised to handle personal data" according to legislation currently in force.

The person filing a report may choose to exclude one or more business functions from amongst those receiving the report.

7.2.1 HOW THE COMMITTEE MANAGES WHISTLEBLOWER REPORTS

The Committee makes a preliminary assessment/investigation of the report to check it meets the essential criteria for admissibility. In particular, the Committee checks:

- Whether or not the report falls within the subjective and objective scope of the law (who reported the breach, and what they reported).

- If there is suitable factual evidence or proof to justify further checks or investigation.
- That the report is accurate and provides well-founded evidence, and that the report is neither over-generalised nor defamatory;
- That any documentation attached to the report is relevant and consistent.

Once the Committee has assessed and approved the report as being admissible, it is required to carry out an investigation to follow up the report. This may include interviewing persons or obtaining documents that are relevant to the inquiry, but shall always comply with the strictest principles of impartiality and confidentiality.

In the event that the Code of Ethics, or the corporate organisation, management and control regulations have been breached, the Company Supervisory Board will also always be involved, and is bound to confidentiality. Other parties may be involved, subject to their agreeing to non-disclosure and signing the confidentiality agreement.

The Committee shall provide the reporter with feedback following the outcome of the investigation and no later than 3 months from the date of confirming receiving the report. If required, and suitably justified, the deadline may be extended to 6 months.

7.2.2 Filing and storing the report

All documents concerning the report are stored on the platform (digital archive) in compliance with data protection regulations.

Report documents are kept for a maximum of 5 years. Any personal data that is clearly not required for the purpose of processing the report will not be collected or immediately deleted if accidentally collected.

7.2.3 Reporting

The Committee is responsible for preparing an annual report of all whistleblower reports received during the period.

The document contains the status of each report (e.g. received, open, being processed, closed, etc.) and any action taken (corrective action and disciplinary measures), in full compliance with regulations governing confidentiality and the reporter's privacy.

The whistleblowing report is sent to:

- The company board of directors
- The statutory board of auditors;

7.3 SAFEGUARDS AND RESPONSABILITIES OF THE REPORTER

7.3.1 Safeguarding confidentiality

The identity of the whistleblower and of other persons involved (e.g. facilitator) is protected regardless of context once a report has been filed.

Disciplinary proceedings shall be taken against any breach of confidentiality, without prejudice to any further form of liability provided for by law. without prejudice to any other legal rights or remedies.

Exceptions to the protection of confidentiality:

The reporter has **expressed their consent** to disclose their identity to persons other than those authorised in advance.

In **criminal proceedings**, the identity of the reporter is kept secret according to Art. 329 of the Criminal Code only after the close of the preliminary investigation.

In the case of **disciplinary action brought** against an alleged author of a breach, the identity of the reporter may be disclosed to the accused person in order for them to defend themselves. Consent, however, must be granted by the reporter.

The personal data of the reporter, and any other persons who may be involved during the report management process, will be managed in full compliance with current legislation governing the protection of personal data, including EU Reg. 679/2016 ("GDPR") and Legislative Decree 196/2003.

In order to fulfil this requirement, the Company has carried out a Data Protection Impact Assessment (DPIA).

7.3.2. Safeguards from retaliation

The Company has adopted a strict anti-retaliation policy in order to comply fully with legal requirements. Retaliation in the ways described in the list below (illustrative, not exhaustive) will not be tolerated:

- ⇒ *Dismissal, suspension or equivalent measures.*
- ⇒ *Downgrading or failure to promote.*
- ⇒ *Change of duties, change of workplace, reduction in salary, change in working hours.*
- ⇒ *Suspension of training or any restrictions on access to training.*
- ⇒ *Demerit or bad references.*
- ⇒ *Adoption of disciplinary measures or any other sanctions, including a fine.*
- ⇒ *Coercion, intimidation, harassment or ostracism.*
- ⇒ *Discrimination or other unfavourable treatment.*
- ⇒ *Failure to convert a fixed-term employment contract into a permanent contract, where the employee legitimately expected such conversion.*
- ⇒ *Non-renewal or early termination of a fixed-term employment contract.*
- ⇒ *Damage, including to a person's reputation, particularly on social media, or economic/financial loss, including loss of financial opportunities and loss of income.*
- ⇒ *Inclusion on 'blacklists' (created on the basis of formal or informal sector/industry agreements) which may result in the person being unable to find employment in the sector or industry in the future.*
- ⇒ *Early contract termination or cancellation for the supply of goods or services.*
- ⇒ *Cancellation of a licence or permit.*
- ⇒ *Request to undergo psychiatric or medical examinations.*

The Company considers the psychological and physical well-being of its employees and business partners fundamental, and is committed to protecting any person who makes a report in good faith.

7.3.3 Conditions for protection

- ⇒ *Whistleblowers must reasonably believe that any information they have on reported breaches is true, and not supposition, hearsay, conjecture, or news in the public domain.*
- ⇒ *A whistleblower's good faith is safeguarded even in the event of an inaccurate report due to a genuine mistake (lack of knowledge of the law).*
- ⇒ *The reporter must clearly indicate in the subject line of the report that it is a whistleblowing report.*
- ⇒ *In order to constitute retaliation, there must be a close connection, or clear consequentiality, between filing the report and the alleged act of retaliation directly or indirectly suffered by the whistleblower.*

Without prejudice to any other right or remedy, protection of the whistleblower is not guaranteed if:

- ⇒ *criminal liability for the offences of slander and defamation, or civil liability for the same offence in cases of wilful misconduct or gross negligence, has been established against the whistleblower by a first instance judgment.*

If such liability is ascertained, a disciplinary sanction may be imposed on the whistleblower or person reporting the alleged offence.

8. DISCIPLINARY SANCTIONS

Should any investigation carried out according to the above procedure demonstrate violation or offence against Company personnel or third parties (consultants, external staff, business partners, etc.), the Company shall act promptly to apply disciplinary sanctions.

Any such sanctions aim to promote a safe environment for persons deciding to report violations or unlawful conduct, and also ensure that persons reporting such conduct are guaranteed protection at all times.

9. TRAINING AND INFORMATION

The Company undertakes to raise awareness of these procedures to all interested parties, both internal and external, by making information available at all times, and through periodic training.

This procedure is available on:

- the Company's website
- the Company noticeboard

OPERATING INSTRUCTIONS FOR THE “SESTANTE” WEB-BASED WHISTLEBLOWING PORTAL

- 1. What the scope of the portal is**
- 2. Who the portal is for**
- 3. What the purpose of the portal is**
- 4. When to file a report on the portal**
- 5. Who will receive your report**
- 6. What cannot be reported**
- 7. What internal company channels can be used to file a report**

What the scope of the portal is

TecniKabel S.p.A.

Who the portal is for

- All Company employees
- Persons whose role involves administration, management, business control, oversight or powers of representation
- Self-employed workers and contractors working onsite
- Volunteers, interns and trainees, both paid and unpaid working onsite
- Freelance professionals and consultants supplying services to the Company onsite

What the purpose of the portal is

To ensure persons filing reports are safeguarded in terms of maintaining confidentiality, and protected from any potential retaliatory action. As a result, the portal also seeks to prevent any risks or situations developing that might be detrimental to the Company and consequently to the collective public interest.

To provide guidelines and operating instructions to the reporter on the subject, contents, recipients and methods of handling reports, and inform them of the type of protection they will receive (in line with European and national legislation).

When to file a report on the portal

A file may be reported when the reporter has well-founded and reliable knowledge of alleged or ascertained illicit conduct in a work-related context. The subject of the report may be a specific breach of national or EU rules and/or wrongdoing of a different nature that harms the public interest or the integrity of the Company.

Facts that are clearly unfounded, information that is already public domain, as well as unreliable indiscretion, conjecture and/or hearsay are not considered the basis for admissible reports.

Before proceeding to make a formal report, you should consider discussing the issue with your direct manager, wherever possible.

Who will receive your report

The Company has entrusted whistleblowing report management to the Whistleblowing Committee. The Committee is qualified to ensure compliance with the provisions of Legislative Decree no. 24/2023.

What cannot be reported

Allegations, conjecture, retaliation or requests that may be considered personal grievance of the reporter are not admissible. Neither are reports of breaches of national defence or matters of national security.










What internal company channels can be used to file a report

Having consulted union representatives, the Company decided to adopt an **internal web-based channel**; the **Sestante Whistleblowing platform/portal**.

The platform allows reports to be transmitted to authorised persons (recipients of the report).

The whistleblower is also entitled to request a face-to-face meeting. This meeting should be set within a reasonable period of time from the request.

How to make a whistleblowing report on the Sestante platform

	<p>To file a whistleblowing report, go to https://tecnikabel.software231.eu or the website and access the webpage. Follow the instructions and read the privacy policy (acknowledge your consent).</p>
	<p>Click on 'new report' and fill in the mandatory fields marked with (*), i.e. title and subject of the report. The reporter may also choose to fill in the other, non-compulsory fields, which provide information about the identity of the reporter. Facts in the report should be substantiated with evidence as much as possible and supported with:</p> <ul style="list-style-type: none">- The time and place in which the breach (the subject of the report) occurred.- A description of the breach (including evidence, or attachments where possible).- Any facts that allow the person to whom the reported facts are attributed, to be identified. <p>The reporter may also provide additional information by attaching files and audio files to the report.</p>
	<p>The platform will ask you - as an optional - for your consent to disclose your identity (if provided) to persons other than those in charge of receiving and managing reports.</p>
	<p>When you are certain of the written or audio content to be submitted, click on “complete report and send”.</p>
	<p>The platform will then issue you with a unique alphanumeric code (ticket code). This should be noted down, kept safe, and not disclosed to third parties. The code is the only way to access this report and check its status. To monitor progress and the operator's response, click on 'reopen ticket' on the home screen (regardless of whether you filed an anonymous report, or if you have revealed your identity).</p>
	<p>Once the report has been filed, you will receive either acknowledgement of receipt, or notification, directly visible in the platform. This acknowledgement represents the final notification that the report has been received.</p>
	<p>You will receive the outcome of your report within three months of acknowledgement of receipt or notification (except in special cases).</p>
	<p>You can submit reports anonymously via the platform. How reports are dealt with differs from country to country in accordance with local regulations.</p>
	<p>All data and information on the platform is stored on the platform for a period of 5 years.</p>

Whistleblowing report flowchart

NOTIFICATION



Response within 90 days of notification of receipt.

Concluding remarks

- The Company promotes the principles of ethical conduct, respect for integrity, and protection of the whistleblower throughout the whistleblowing process.
- The Company is committed to protecting the privacy of all persons involved.
- Reports are stored securely on the platform.
- All reports are subject to a preliminary investigation; you may be contacted for further information by the Committee in charge of managing your report.
- Reports are confidential.