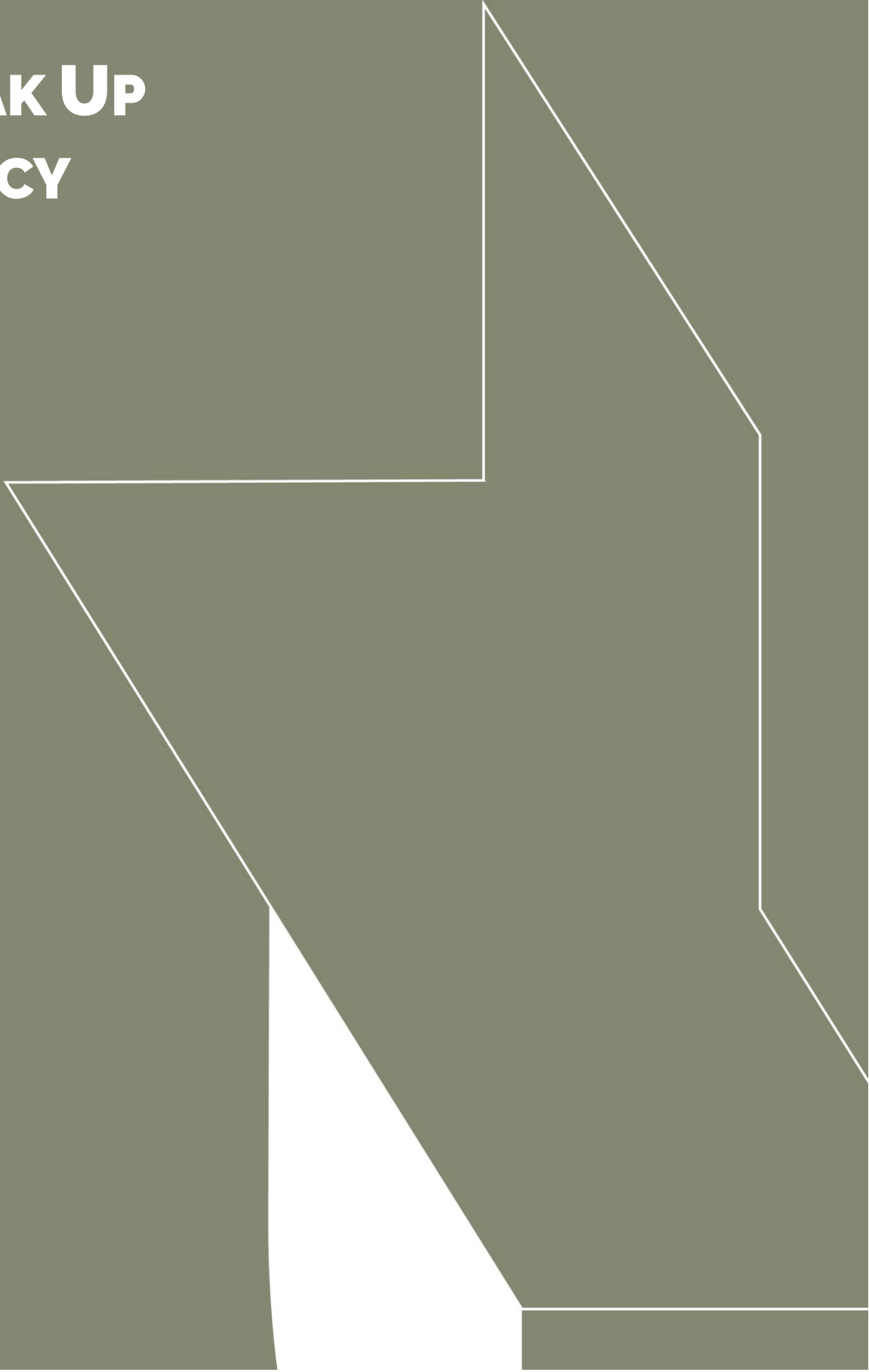




# **SPEAK UP POLICY**





### Document Summary

---

<b>Document Name</b>	<b>Speak Up Policy</b>
<b>Document Owner</b>	Governance Function
<b>Prepared by</b>	Legal and Sustainability departments
<b>Approved by</b>	Board of ER Group Limited
<b>Date of Approval</b>	18 July 2025
<b>Effective Date</b>	18 July 2025

### Version Control

---

<b>Date</b>	<b>Author</b>	<b>Version</b>	<b>Description of changes</b>
18 /07/2025	Chief Legal and Governance Executive	1.0	Creation
07/04/2026	Chief Legal and Governance Executive	1.1	Name of ER Group Limited updated



**Contents**

**1 Introduction .....4**

**2 Purpose.....4**

**3 Applicability .....5**

**4 Definitions and Interpretation .....5**

**5 Applicable principles.....5**

    Accessibility .....5

    Good faith .....6

    Whistleblower protection.....6

    Anonymity .....6

    Confidentiality.....6

    Transparency, objectivity and impartiality.....7

**6 Responsibilities .....7**

    Board of Directors.....7

    Speak Up Committee.....8

    Case Managers.....8

    External expert.....9

    Employees .....9

    Management .....10

    Persons responsible for ethics and/or compliance.....10

**7 Eligible users ..... 10**

    The Internal Reporting System may be used by any natural person who is:.....10

**8 Possible wrongdoings or malpractices ..... 10**

    Illegal, immoral or illegitimate behaviours that may give rise to an Alert: .....10

**9 Internal Reporting System ..... 11**

    The Reporting Channel.....11

    Admissibility analysis.....11

    Recording and classification of communications.....12

    Investigation.....13

    Resolution of the case.....13

    Non retaliation measures .....14

    Deadlines for the resolution of a case .....14

**10 Protection of the whistleblower and the person under investigation ..... 14**

    Whistleblowers:.....15



Persons under investigation: .....15

**11 Prohibition of retaliation .....15**

**12 Data protection.....15**

**13 Data retention ..... 16**

**14 Approval and Revision of this Policy ..... 16**



## 1 Introduction

ER Group Limited and its Group Companies (hereinafter the "Group" or "ER Group") is committed to high standards of openness and strongly believes that all reasonable and valid concerns of Employees and third parties, questionable practices, or potential wrongdoing must be considered within a defined process. The Group has thus established an Internal Reporting System with a Reporting Channel to identify, uncover, investigate and address any irregular, unlawful, criminal, or discriminatory behaviour, in alignment with the Group's commitment to employees and principles of good governance.

## 2 Purpose

The purpose of the Speak Up Policy is to provide a channel of effective communication of Employees' or Third Parties' concerns so as to facilitate the disclosure of any wrongdoing or malpractice of which they become aware and to provide protection for whistleblowers who report allegations. It further outlines the process on how reported concerns will be handled and investigated

The aim of the Speak Up Policy is to promote transparency to underpin the risk management systems, to ensure fair and ethical practices are maintained ensuring the effectiveness of the Codes of Ethics, codes of conduct, and the Group's values, and to help protect the reputation of the Group.

The Group encourages those with knowledge of illegal or irregular situations to report them through the established channel.

All Employees (at any hierarchical level) and directors are expected to report any suspected irregularities or violations of laws or internal rules which they became aware of or suspect. This will allow verification and appropriate actions to remedy issues and prevent recurrence, thereby enhancing the professional, social, and ethical environment and ensuring compliance with laws, regulations, and policies.

The Group has decided to centralise the management of whistleblowing alerts and malpractice reporting into a single, accessible Reporting Channel, for Employees and third parties.

This Policy embodies all the principles and processes applicable to the Group as to its subject matter and supersedes and cancels in all respects any existing policy or procedure within the Group in relation to its subject matter.

Any channels (email address, hotline or go-to-person) preexisting this Policy will henceforth redirect the whistleblower to the Reporting Channel.

Employees may still contact their hierarchical superior for any matter falling within the ambit of this Policy. The matter will be referred to the person in charge at the Compliance or People departments of the Group so that the alert can be processed in accordance with this Policy.



### 3 Applicability

This Policy applies to ER Group Limited and its Group Companies that have adopted ER Group's compliance framework.

### 4 Definitions and Interpretation

In this document:

"Alert"	means is the act by an individual of revealing or reporting, without any direct financial consideration and in good faith, facts or information relating to questionable practices by or within a Group Company
"Case Manager"	means the person appointed to process the Alerts
"Employee(s)"	means a person in employment with the Group and includes all categories of Employees and workers employed on an indeterminate or determinate duration, including full-time, part-time, casual workers and trainees under an apprenticeship, traineeship/training scheme
"Group"	means ER Group Limited and the Group Companies
"Group Company"	means ER Group Limited or any company related to, or associate of, ER Group Limited to which this Policy applies and "related" shall be construed in accordance with the Companies Act 2001 while "associate" shall mean those companies disclosed as associates in the audited financial statements of ER Group Limited
"Policy"	means this Speak Up Policy as amended from time to time
"Reporting Channel"	means the online platform maintained by the Group for the purpose of allowing the disclosure of any wrongdoing or malpractice of which Employees or third parties become aware and the processing of such Alerts
"Reporting Person" or "whistleblower"	means an individual revealing or reporting, without any direct financial consideration and in good faith, facts or information relating to questionable practices by or within a Group Company
"Third Party/ies"	refer(s) to any person(s) in interaction with a Group Company and who may use the Reporting Channel

### 5 Applicable principles

#### Accessibility

The Reporting Channel is public and easily accessible to employees and third parties to submit an Alert according to this Policy.



## Good faith

A Reporting Person must act in good faith and without financial compensation. Any allegation in the Alert must be presented objectively and factually.

A Reporting Person is deemed to act in good faith when his/her Alert:

- follows this Policy and is based on facts or signs that suggest behaviour violating the Group's principles, ethics codes, or applicable laws;
- is made having reasonable grounds for believing that the facts reported are true in the light of the information available to him/her and
- is done without intent to harm (which includes but is not limited to allegations that are frivolous, or vexatious in nature and seeking to or cause emotional or material harm to a person or seek to deceive the recipient).

If the allegations are proven to have been made in bad faith or solely for personal interests, the whistleblower protection will not apply and disciplinary measures may be taken.

## Whistleblower protection

The Group shall guarantee bona fide whistleblowers protection against retaliation or victimisation of any kind for having made an Alert through the Reporting Channel.

Any person who participates or assists in an investigation will also be protected.

## Anonymity

The Reporting Channel allows anonymous Alerts which will be processed as far as practicable. However, whistleblowers are encouraged to identify themselves when making an Alert as admissibility of the Alert may be impacted or an investigation may be limited without the source of information.

## Confidentiality

Confidentiality is the cornerstone of the Group's Internal Reporting System:

- Case Managers and Administrators commit to confidentiality in writing;
- those interviewed and consulted undertake to maintain the strictest confidentiality regarding the alert and the content of exchanges;
- the Group undertakes to respect the confidentiality of the personal data of the parties concerned (i.e. the whistleblower and the persons mentioned or implicated in the alert) in accordance with applicable data protection laws and internal policies;



- every effort will be made to protect the anonymity of the person using the Reporting Channel. The whistleblower's identity and identifying details may only be disclosed with their consent, except as required by administrative or judicial authorities, and may only be accessed by those involved in the management of the case.

Any person participating in the processing of an Alert should not discuss reported concerns with colleagues or third parties or the media, during and after the Alert is being processed. Any unauthorized disclosure may result in disciplinary action.

Such communications, if any, shall be handled by the Communication department of the corporate office of the Group.

### **Transparency, objectivity and impartiality**

The Internal Reporting System ensures that alerts are processed in a transparent and fair manner.

Persons mentioned in an Alert or investigation have the right to know the reasons for it. Depending on the needs of the investigation, they may be informed of its progress.

The Case Managers, who in charge of managing and processing the alerts received through the Internal Reporting System, must do so in an objective and impartial manner.

## **6 Responsibilities**

### **Board of Directors**

The Board of Directors of ER Group Limited takes responsibility for the Group's overall compliance with the applicable laws and internal policies and is committed to promoting compliance and diligence in the management of the Internal Reporting System.

Therefore, the Board of Directors is responsible for approving this Policy, establishing the systems, providing the adequate human and financial resources and designing mechanisms for effective a whistleblowing management. This does not affect the independent decisions of each Group Company, which follow their country's legislation and business specifics.

The Board of Directors delegates to the Corporate Governance Committee the responsibility of supervising and monitoring the effectiveness of the Internal Reporting System.

The Corporate Governance Committee may appoint one or more of its members as Administrator(s) of the Internal Reporting System and shall appoint the Case Managers who shall be senior managers primarily responsible for human resources, legal, compliance, internal audit and/or sustainability matters.



The Corporate Governance Committee shall receive regular reports from the Speak Up Committee and report in turn to the Board of Directors. The Corporate Governance Committee will report annually on the Internal Report System in the Integrated Report.

### **Speak Up Committee**

The Administrator (as the case may be) and the Case Managers constitute the Speak Up Committee.

The Speak Up Committee has overall responsibility for the Reporting Channel and as such:

- oversees the processing of the Alerts by the Case Managers;
- assists the Case Managers in their duties;
- receives the reports and recommendations of the Case Managers and collectively decides the most appropriate action or sanction proportionate to the seriousness of the report and rules on the recommendations proposed by the investigator;
- decides on the referral of cases to the authorities where applicable;
- closes the cases.

### **Case Managers**

Case Managers are bound by an enhanced duty of confidentiality when processing the Alerts and are responsible inter alia for:

- receiving and handling of Alerts;
- acknowledging the receipt of any Alert as soon as possible (maximum 3 working days);
- collecting and recording alerts in the dedicated system and ensuring communication with the persons concerned by the Alert
- assessing the admissibility of any Alert and informing the whistleblower accordingly as soon as possible (maximum 10 days);
- investigating the facts reported (through fact-finding, data analysis and interviewing) in the Alerts and as far as possible endeavouring to process any Alert within a maximum of three (3) months from the date of acknowledgement of receipt.
- presenting their findings and conclusions in a substantiated report as well as recommendations as to the most appropriate action or sanction to be taken;
- documenting the entire follow-up process on the Reporting Channel;
- assisting the relevant departments or functions with the implementation of the recommended measures or follow up plan.

The Alerts are assigned to Case Managers depending on their nature:

- Compliance: acts of corruption, influence peddling, fraud, money laundering and terrorism financing, Non-compliance with laws, regulations and internal policies and procedures;



- Human Resources: acts of discrimination and moral or sexual harassment, damage to the health and safety of persons Non-compliance with laws, regulations and internal policies and procedures;
- Legal: anti-competitive practices, Data protection infringement, Intellectual property violation, Breach of confidentiality or cybersecurity, Non-compliance with laws, regulations and internal policies and procedures
- Alerts that do not fall within any of the categories listed above ("other") will be assigned to the Compliance Case Manager.

As part of their mission, the Case Managers are required to uphold the highest standards of conduct. By accepting their appointment, each undertakes to comply with the following additional obligations:

- ensure that measures are taken to protect people and the Group;
- observe the utmost good faith and keep his/her independence of mind at all times;
- respect the principles of confidentiality, discernment, impartiality and objectivity, proportionality and minimization of the data collected, as well as transparency and fairness towards the people whose data is processed;
- keep the whistleblower's identity strictly confidential;
- only disclose information about the persons concerned (who are presumed not to be at fault until the conclusion of the investigation) and the content of the Alert to those who need to know;
- process the Alerts with diligence;
- not be in a situation of conflict of interest or be at risk of being in such a situation; if this is not the case, he/she must immediately withdraw from the handling of the Alert and inform the Speak Up Committee and Compliance Department.

The Case Managers are responsible for ensuring compliance with these principles by any person (internal or external to the Group) to whom they delegate all or part of their Case Managers' duties, or whose assistance they request; they ensure that this person is not, or is not likely to be, in a situation of conflict of interest. This person must also adhere to the present policy and the present section in writing.

Any breach may give rise to disciplinary or legal proceedings.

### External expert

If, at the beginning or during the investigation of a case, the situation so requires, the Group may contact an external expert. In this case, compliance with the principles set out in this Policy and applicable law shall be ensured.

### Employees

All Employees involved in an investigation must cooperate (e.g. provide requested documents, not destroy documents or collude with a witness) and answer questions honestly.



## Management

Managers are responsible for ensuring that their teams' employees are aware of this Speak Up Policy.

## Persons responsible for ethics and/or compliance

The role of the persons responsible for ethics and/or compliance in each cluster, activity or country is to:

- where necessary, adapt the Speak Up Policy to take account of local specificities, without however undermining the protection of whistleblowers and the persons mentioned in the alert, and translate it into the chosen languages.
- ensure that this Speak Up Policy is disseminated to all entities within its scope.
- ensure that a "Communication Kit" is made available to Human Resources and Managers.
- advise anyone with questions about the Speak Up Policy.

## 7 Eligible users

The Internal Reporting System may be used by any natural person who is:

- a Group employee (any person employed on an indeterminate or determinate duration, including full-time, part-time, casual workers and trainees under an apprenticeship, traineeship/training scheme)
- a shareholder of a Group Company
- a director or committee member of a Group Company
- a client or customer of a Group Company
- an external worker, contractor, subcontractor and supplier of a Group Company
- a business partner of a Group Company
- a person otherwise involved with a Group Company (from trade unions, NGOs, local authorities, the State, etc.)

## 8 Possible wrongdoings or malpractices

Illegal, immoral or illegitimate behaviours that may give rise to an Alert:

- Theft, fraud, corruption, influence peddling, money laundering and terrorist financing
- Conflict of interest
- Anti-competitive practices
- Sexist behaviour, Harassment (moral, sexual), Discrimination, or Violence
- Safety and Health issues
- Data protection infringement
- Intellectual property violation
- Breach of confidentiality or cybersecurity
- Non-compliance with laws, regulations and internal policies and procedures
- Environmental issues



- Other

## 9 Internal Reporting System

### The Reporting Channel

The Group has set up an online platform, Speak Up, as a Reporting Channel. Alternatively, any alert can be raised or violation reported on [ethics@ergroup.mu](mailto:ethics@ergroup.mu).

Speak Up is made available to whistleblowers through:

- a link on the Group Companies' websites, as well as on MyExperience
- QR codes displayed in emails, on websites and in various locations within Group Companies.

<https://er.whispli.com/speakup>



The Alert may be submitted anonymously if the whistleblower chooses to do so, despite the guarantee of confidentiality. However, in the case of an anonymous Alert, the investigation may face limitations due to the inability to verify information. Therefore, it is recommended that the whistleblower provides the reason for anonymity, so it can be considered during the processing and investigation of the Alert.

The Reporting Channel allows for ongoing communication with the whistleblower including, if deemed necessary, the request for additional information from the Whistleblower.

When accessing the Reporting Channel, the whistleblower is invited to create an account (in his name or as a guest for anonymous Alert) and to provide details of his Alert.

Depending on the category of issue being reported, a Case Manager will be assigned to the Alert.

### Admissibility analysis

On receipt of an Alert, an acknowledgement of receipt is sent to the Reporting Person within 3 days and the Case Manager carries out a preliminary analysis to determine whether the report constitutes an admissible alert. If the Case Manager is unable to make a decision, he may request further information from the author of the Alert and call on the services of competent professionals to make this assessment.

If the Reporting Person has identified himself/herself, he/she will receive an email notification inviting him/her to connect to the 'follow up' section; if he/she has opted for anonymity, the author must log in regularly with his/her guest access to check for follow ups.



Admissibility of the Alert will be determined taking the following into consideration:

- the allegations fall within one of the breaches listed in this Policy, and
- the person making the report is acting in good faith and without direct financial consideration.

When the facts occur outside professional activities, the whistleblower must have personal knowledge of them to benefit from whistleblower protection.

Only admissible alerts may be investigated internally, or forwarded to the relevant department for processing when no internal investigation is required.

Alerts filed anonymously are subject to special precautions regarding their processing: an alert will only be admissible if the supporting evidence is sufficiently detailed to establish the seriousness of the facts.

At the end of this analysis, the Case Manager concludes whether the Alert is admissible or inadmissible:

- if inadmissible:
  - o the author of the Alert is informed in writing within 10 business days and, if necessary, referred to the appropriate person within the Group who can assist
  - o The Case Manager closes the Alert and the data is immediately archived
- If admissible:
  - o the Reporting Person is informed in writing within 10 business days
  - o the Case Manager starts the investigation process and as far as practicable endeavours to process the Alert within a maximum of three (3) months from the date of acknowledgement of receipt
  - o the whistleblower is able to follow the status of the Alert on the Reporting Channel

### **Recording and classification of communications**

All communications received are analysed by the appointed Case Manager independently.

The identity of the person making the Alert and the person(s) concerned are kept confidential.

Each Alert is assigned an identification code and is incorporated into a database under this code.

The whistleblower and the Case Manager can interact, in confidentiality and anonymously (as applicable) through the Report Channel, to progress on the investigation.



## Investigation

The Case Manager then initiates or coordinates the investigation aimed at establishing the materiality of the violations and characterising the liability of the alleged perpetrators.

This investigation may be carried out by the Case Manager(s) or a third party (lawyers, experts, auditors) with appropriate guarantees for the protection of personal data.

As part of their investigation, authorised Case Managers or third parties are entitled to:

- Collect and process any data (accounting, banking, computer) that they deem relevant (excluding data prohibited from collection) concerning the company or the persons involved;
- Conduct interviews allowing the accused to respond to the accusations to which they are the subject;
- Interview any person to collect any information to verify the accuracy of the alleged facts.

The Case Manager will communicate to the whistleblower, in writing, and within a reasonable time not exceeding 3 months from the acknowledgment of receipt, or in the absence of acknowledgment of receipt, within three months from the expiration of a period of seven working days following the alert, information on the measures envisaged or taken to assess the accuracy of the allegations and, if necessary, the measures taken to remedy the subject of the Alert and the reasons for it.

Throughout the investigation process, the presumption of innocence is guaranteed to all persons concerned. Where appropriate, the right of the person concerned to be informed of the acts or omissions attributed to him or her and to be heard at any time shall be guaranteed. Such communication shall take place at such time and in such manner as is deemed appropriate to ensure the proper conduct of the investigation.

## Resolution of the case

At the end of the investigation, the Case Manager(s) present their findings and conclusions to the Speak Up Committee:

- If the wrongdoing or the malpractice is deemed not to have been established: Case closure:

If it is determined that no irregularity, act contrary to the law or to internal rules has been demonstrated, the Speak Up Committee shall close the case without the need to adopt any measure, and the decision shall be documented.

The whistleblower and the accused persons will be notified in writing of the closure of the procedure where applicable.

- If the wrongdoing or the malpractice is deemed to have been established:



If it is established that there has been an act or omission involving irregular, unlawful, criminal or discriminatory conduct that contravenes the applicable laws or the Group internal policies, the Speak Up Committee shall approve a follow up action plan which may include:

- o an action plan (for example, launching an audit, modifying a process, reorganizing a department, setting up training courses);
- o disciplinary sanctions;
- o civil proceedings;
- o the referral of the matter to competent authorities;
- o or the lodging of a complaint; and
- o non retaliation measures.

If the offender is a third party, the Speak Up Committee shall report such non-compliance to the competent authorities.

### **Non retaliation measures**

During the investigation and after its closure, a whistleblower, facilitator or any other person involved in the investigation who feels or fears reprisals may report the situation via the alert system or directly by informing the Case Manager.

Where the risk of reprisals is confirmed, specific protective measures may be proposed by the Case Manager or the Speak Up Committee, in conjunction with the relevant human resources department, for example:

- temporary or permanent reassignment (e.g. working from home);
- a change in line management;
- engagement with HR to monitor the workplace situation.

### **Deadlines for the resolution of a case**

Subject to applicable laws, the time for processing an Alert and completing of the investigation shall exceed 3 months from the receipt of the communication, except in cases of particular complexity requiring an extension of the time limit, in which case the time limit may be extended by up to a maximum of a further three months.

## **10 Protection of the whistleblower and the person under investigation**

The rights and guarantees of whistleblowers, persons under investigation and witnesses must be respected in all proceedings.

In this regard, they shall be protected against any kind of retaliation, discrimination and penalisation on the grounds of the Alert made through the Reporting Channel.

**Whistleblowers:**

Provided that:

- (i) they have reasonable grounds to believe that the information referred to is true at the time of the Alert or disclosure and,
- (ii) the Alert is made in good faith,

whistleblowers who disclose irregular, unlawful, criminal or discriminatory conduct shall be entitled to protection by the Group as follows:

- Right to information through the Reporting Channel
- Right to choose anonymous or nominal status
- Right to confidentiality
- Acknowledgement of receipt of the Alert and right to reasonable information
- Right to a transparent investigation and to an impartial interlocutor
- Rights derived from Data Protection
- Right to non-retaliation

**Persons under investigation:**

Any person under investigation shall benefit from:

- the right to be informed of actions or omissions attributed to them.
- maximum respect for the presumption of innocence during the investigation of the case, the right to be heard, the right of defence, and the right of access to the case file.
- the right to the preservation of the identity of the person under investigation by guaranteeing the confidentiality of the facts and data of the proceedings.

**11 Prohibition of retaliation**

The Group expressly prohibits acts constituting retaliation against whistleblowers as a result of their use of the Reporting Channel.

Retaliation means any acts or omissions which are prohibited by law, or which, directly or indirectly, result in unfavourable treatment that places the persons suffering them at a particular disadvantage compared to another in the employment or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure, and provided that such acts or omissions occur during the duration of the investigation procedure or within one year of the completion of the investigation procedure or of the date on which the public disclosure took place. An exception is made where such action or omission can be objectively justified by a legitimate aim and the means of achieving that aim are necessary and appropriate.

**12 Data protection**

The party responsible for the processing of personal data is each Group company.



The information provided by the whistleblower shall be processed for the purpose of managing the Alert made through the Reporting Channel.

The personal data provided shall be kept for the following retention period, unless it is necessary to keep them for a longer period due to the opening of an administrative and/or judicial procedure.

The processing is necessary for compliance with the legal obligation applicable to the controller.

Personal data shall not be communicated to third parties unless, where appropriate, it is necessary for the processing of an internal investigation, the opening of disciplinary proceedings, the adoption of disciplinary measures, or in compliance with a legal obligation, it is communicated to law enforcement agencies, courts or other competent authorities.

Whistleblowers may exercise their rights of access, rectification, deletion, limitation of processing, portability and objection at the registered office of the Group or by sending an e-mail to [dataprotectionofficer@ergroup.mu](mailto:dataprotectionofficer@ergroup.mu).

### 13 Data retention

Alert	Data Retention
Inadmissible alert	Anonymization in the semester following analysis of admissibility.
Admissible alert - being processed	Kept in active base until final decision on further action.
Admissible alert processed and closed with no further action taken	Anonymization in the semester following final decision on follow-up.
Admissible alert processed and closed, leading to further action	Retention of data until the end of the procedure or the time limit for appeals against the decision.

### 14 Approval and Revision of this Policy

The Speak Up Policy is approved by the Board of Directors of ER Group Limited.

The Policy shall be reviewed and updated in accordance with amendments to mandatory legal provisions and on a periodic basis to ensure it remains relevant to the Group. The revised version of the document will be submitted to the Board of ER Group Limited for approval and once approved will automatically apply to the Group Companies.

Requests for revision or amendments to this document must be submitted to the Group Governance Function for review and subsequent updates. A list of authorised changes to the Policy will be summarised in the revision history as shown on the cover page.