# WHISTLEBLOWING POLICY

# and

# COMPLAINT REPORTING MECHANISM

**Approved on the 24th October 2023**

**Valid from the 17th December 2023**

## Whistleblowing Policy and Complaint Reporting Mechanism

## Table of Contents

| | Revision | | | | | |
|---|---|---|---|---|---|---|
| **Version: 1** | **0** | **1** | **2** | **3** | **4** | **5** |
| **Date** | 30.06.2020 | 24.10.2023 | | | | |
| **Elaborated by** | FOD and Administration | Compliance Manager | | | | |
| **Verified by** | Grants | A. Bertani<br><br>Trade Unions | | | | |
| **Approved by** | Executive Committee | Executive Committee | | | | |

# 1 PURPOSE

EMERGENCY ONG ONLUS (hereinafter "**EMERGENCY**" or '"**the Organization**") intends to promote an organizational culture characterized by responsible, conscious and respectful behaviours, by means of factoring its practices into *human rights based approach* and in the active prevention and correction of internal wrongful acts, malpractices, misconducts and crimes, as our wrongdoing directly and negatively affects our chances for fulfilling our mandate and vision and, ultimately, leans on affected populations.

In these terms, EMERGENCY **recognizes the crucial role** played by all its stakeholders, internal and external, in supporting EMERGENCY pursuing such ambitions for **integrity, legality, transparency** and, in general, for adherence to **the ethical, legal and procedural standards overarching its action**.

Abiding by Art. 4, c. 1, of the Italian D.Lgs. 24/2023, this policy "*WHISTLEBLOWING POLICY and Complaint Reporting Mechanism*" (hereinafter, "**Whistleblowing Policy**") and the reporting channels provided hereinafter, were adopted in consultation with the trade unions representatives indicated at Art.51 of the Italian D.Lgs. n. 81/2015, which expressed positive feedback in the dedicated session.

EMERGENCY is firmly committed to **guaranteeing that any person** can **safely report concerns on any illegal and/or unethical and/or incorrect behaviour conducted by personnel of EMERGENCY**, **its partners or of (sub)contractors**, **without any fears of repercussion**, by meeting what the CHS Alliance Commitment 5's quality criterion expresses as "Complaints are welcomed and addressed."

This policy is in place to reassure prospective Whistleblower(s) that **it is welcome, safe and acceptable to speak up through the dedicated channels and to flag a suspicion**, in order for EMERGENCY to ensure safe, dignifying and conducive environment for served communities, staff and members and to pursue **integrity as well as continuity** in the action, **through loyalty to human rights, its mandate, constituency and stakeholders**.

The Whistleblowing Policy means to **encourage** staff and served populations members especially, to **raise existing substantial concerns**, **at an early stage and in an appropriate way**.

The aim of the **Complaint Reporting Mechanism procedure** (here below at section 4) is to **ensure that an appropriate process exists, and it is visible,** which promotes accountability in Emergency NGO "*so that communities and employees are better able to report abuses and*

*access additional protection through deterrence*"[1], by deploying a **fair, expedite and discreet** mechanism for the emersion, investigation and response to relevant concerns**.**

This policy is amended here, to meet the specific requirements of Italian Legislative Decree No. 24/2023 on Whistleblowing and to align, to the feasible extent, to the ANAC Guidelines approved with Decision n°311 of July 12, 2023.
This Policy is clearly referred to and coordinated with the *Organization, Management and Control Model* upon Italian Legislative Decree n. 231/2001, which provides the sanctions in case of violation.

This policy is to review periodically every two years or promptly when:
- change in structures and operations that might affect the following procedures, roles and responsibilities;
- change in the context of operations that might affect the following procedures, roles and responsibilities;
- change in pertaining laws.

## 2 SCOPE AND INTERACTIONS WITH OTHER INTERNAL REGULATIONS

This Policy is actionable by:

- EMERGENCY NGO **Personnel** (regardless if remunerated or not, temporary, permanent or semi-permanent, daily worker, if employee or consultant, if actual, former or prospective) ***governance*** **bodies' members** and association's **members**;
- EMERGENCY' **served communities'** members,
- EMERGENCY's **partners, contractors and sub-contractors and their staff** members,
- **third parties**, whom it happens to see, hear and learn of wrongdoing relevant to EMERGENCY, regardless of having a working relationship with EMERGENCY.

This Policy covers **the knowledge or genuine suspicion**:
**of behaviours, acts and/or omissions carried out in the perimeter of EMERGENCY's operations, either or both, by EMERGENCY's Personnel, contractors, subcontractors and partners**, that result in **violations, or threats or attempts of violations**, with the potential of:
- **causing harm to individuals rights and to the public interest**
  and/or
- **undermining the integrity** of EMERGENCY.

These behaviours, acts or omissions might include, but are not limited to, the followings:

[1] HAP (Humanitarian Accountability Partnership) Standard in Humanitarian Accountability and Quality Management, 2007.

- ✓ **Breach of national and EU laws (either criminal, administrative or private)** (civil, administrative or criminal) such as, *for instance*, fraud or mismanagement, bribery; tax evasion; unauthorized disclosure of confidential (either personal and non-personal) or personal information; danger posed to health, safety and security at the workplace; sexual abuse and harassment; stalking; mobbing; hate speech; each and all unlawful conducts triggering EMERGENCY's responsibility upon Italian Legislative Decree No. 231/2001; conducts undermining the European Union's financial interests (Art. 325 TFEU) and the scope of European legislations in these fields or the European internal market (Art. 26, para. 2 TFEU) and the scope of European legislations in these fields or Union competition and State aid rules, or the rules of corporate tax or to arrangements as a means to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
- ✓ **Breach of International Law, in particular those related to Humanitarian Aid, as expressed by the Humanitarian Principles, the Core Humanitarian Standards, the Code of Conduct, and similar unethical conducts,** as well as of the values and principles of EMERGENCY, articulated in the EMERGENCY's Code of Ethics contained in the *Organization Model* (MOG);
- ✓ **Breach of EMERGENCY's policies** (PSEAH, Child Protection, Anti-Corruption, Anti-Fraud, Data Protection, Privacy, etc.)
- ✓ **Breach of the *Organization Model* "MOG"** (*Modello di Organizzazione, Gestione e Controllo*) adopted by EMERGENCY NGO upon Italian Legislative Decree No. 231/2001, and the **descending internal regulations (manuals) and/or procedures** such as, for instance, fraudulent procurement; undeclared conflict of interest; severe offence in violation of safety and security standards, money-laundering, etc.;
- ✓ **Any acts or omissions that could cause relevant, significant and severe harm** (e.g., economic, environmental, to the health and safety, reputational, etc.) to the Organization, the served communities and populations, personnel, representatives or third parties in general;
- ✓ other **violations of Italian and in-country administrative, civil, tax or criminal law** provisions;
- ✓ Any conduct **aiming at covering up** the breaches listed above and similar ones.

This Whistleblowing Policy **DOES NOT apply** to reports and complaints or claims:

- X Falling under labour law claims (i.e. salaries, working time; leaves, conflicts and grievances among staff members, work performance, etc.) which are to enter and treat upon HR Management channels and procedures;
- X Personal data treatment within the perimeter of the individual work relationship with EMERGENCY, having no harm to public interest or the entity's integrity which are to enter and treat through *privacy* channels and procedures;
- X Dissatisfaction on services (extension, duration, whereabouts, modalities, content, etc.) delivered by EMERGENCY, where not relevant as alleged violation of human rights, do no harm and/or core humanitarian standards, which are to enter and treat upon *F.O.D. Program and Logistic Management procedures at Field Level*.

- X on issues already in the public-domain which will be treated accordingly;
- X on issues beyond EMERGENCY's direct connection or command. Generally, EMERGENCY can only respond to complaints that are about issues that EMERGENCY is or was responsible for at the time of eventual display of the concerned misconduct or within its perimeter of command;
- X that are offensive and slanderous and/or mainly based on mere rumors, missing reference to facts, or to the description of a specific misconduct/event with details on *what, who, when, where and how*. When anonymous, this type of report is dropped automatically;
- X submitted with the main purpose of intimidation and retaliation, which is dropped out automatically;
- X Incoherent with renowned facts or unreadable, which is dropped out automatically;
- X apparently malicious or frivolous i.e. made with gross negligence, which is dropped out automatically and eventually, when minimum factors occur, they are pursued against;
- X carried out by an abusive access to data system which are dropped out automatically and eventually pursued against;
- X part of bulk emailing which are dropped out automatically and eventually pursued against.

**!** Please note that, while the Italian Legislative Decree No. 24/2023 limits:
(i) **the objective scope** of the provided guarantees and obligations to the list of illicit conducts contained therein (mainly point I. above) and
(ii) **the subjective scope** – and the label of "Whistleblower" – to those reporters who came to know of a breach relevant to the decree, in the course or because of their work with the entity,
**EMERGENCY has decided to extend the objective and the subjective scopes over the perimeter set by the Italian Legislative Decree 24/2023,** as provided here in this paragraph**.**
This is due to the **particular nature of the action conducted by EMERGENCY**, as a humanitarian, not-for profit, third sector organization operating abroad, bond by relevant international laws and standards for humanitarian actors, (e.g. *Accountability to Affected Population* (AAP), as well as, based on its mandate, **a private entity delivering exclusively on the public interest**.

This Policy applies at EMERGENCY **globally** (i.e.: at Main Office, at Field Offices and at any activity sites, even if temporary or shared with partners).

This Policy does not replace the other policies and procedures at EMERGENCY, **but it complements them, by establishing a unique internal reporting and management mechanism on violations** (either suspected, apparent, threatened or at the stage of an attempt) with pertaining rules, principles and procedures.

In particular, this policy complements:
- → *The Humanitarian Principles;*
- → *The Core Humanitarian Standards;*

- → *EMERGENCY Code of Conduct and Code of Ethics;*
- → *Anti-Fraud & Anti-Corruption Policy;*
- → *PSEAH policy;*
- → *Child Protection Policy;*
- → *Data Protection Policies and Manual;*
- → *EMERGENCY Organisation, Management and Control Model ex Italian Legislative Decree No. 231/2001;*
- → *EMERGENCY Administrative and Financial Manual;*
- → *Safety&Security Policies and Procedures;*
- → *EMERGENCY Standard Operating Procedures (field level);*
- → *Any further policy, which EMERGENCY may develop ahead, in pursuing the elevation of operational and integrity standards.*

## 3. PRINCIPLES AND DEFINITIONS

Technically, "whistleblowing" defines as *a confidential disclosure of any concern encountered in the work-related context in relation to a perceived wrongdoing or malpractice* (by means of any conduct exemplified in the previous paragraph 2 or similar behaviours).

Pursuant to EMERGENCY's expansion of the objective and subjective scope of the relevant Italian Legislative Decree 24/2023, "whistleblowing" is intended at EMERGENCY as: *a confidential disclosure of any concern encountered in **EMERGENCY's action-related** context, in relation to a perceived wrongdoing or malpractice* (by means of any conduct exemplified in the previous paragraph 2 or similar behaviours)

- **"Whistleblower"** or "Complainant", or "Reporter" is any person(s) disclosing a concern encountered in any EMERGENCY's action-related context, here including those not having any working relationship with EMERGENCY (i.e. beneficiaries, patients, communities' leaders, authorities, etc.).
- **"Reported person(s)"** or "Alleged person(s)" or "Subject of Complaint" is the person(s) allegedly carrying or having carried out the concerned wrongdoing**.**
- **"Witness(es)",** "testimony(ies)", "informed person(s)" is anyone who was present at the time of the carrying out of the wrongdoing or had indirect knowledge of it (heard, seen, read, etc.).
- **"Report",** "Concern", "Complaint", "Disclosure" is the specific act of disclosing an actual or suspected wrongdoing.
- **"Incident",** "Object of", "Content of", "Issue" report/complaint/concern is the fact, behaviour, act or omission contained and described in the disclosure.
- **"Channel"** is the entry manner of the report/complaint/concern. It might be through a dedicated platform, email account(s), hotline, the referent person for verbal reporting, box for papery submission etc.

- **"Compliance"** is acting accordingly to laws, regulations, standards, contractual obligations, mandates and values. Focus is on "*how we deliver*".
- **"Feedback"** is the information, the statement of opinion, the reaction (return back) to a process/activity (or the information obtained from such reaction).
- **"Complaint Reporting Mechanism (CRM)"** is the set of tools, rules, principles, responsibilities and procedures that is meant to allow safe, discreet, expedite and accountable report of complaint/concerns and response to, at the Organization level.
- **"Whistleblowing Law"** is, in particular, the Italian Legislative Decree No.24/2023 regulating the subject for all private and public entities incorporated and registered in Italy.

**All EMERGENCY Personnel** (in its broader meaning) **is required to report promptly and at an early stage, any breach (or suspicion of) of** the standards aforementioned, **through the internal** reporting channels made available.

**Any disclosure is to happen first through the provided internal channels** indicated at par. 4.1 hereinafter.

Pursuing the provisions ofl D.Lgs. 24/2023, a report can be filed to the **external channel** of the **Italian National Authority for Anti-Corruption (ANAC)**, **if, and only if**:

- the reporter has priory filed the report to the internal channels of the Organization following the provisions of this Policy, but the Organization remained silent for over 3 months;
- the reporter has grounded expectation that the report will be dropped or voided if put forward at the internal channels or, otherwise, it may trigger retaliation against the reporter;
- the reporter has grounded concern of immediate and actual harm to public interest if having to pass through the internal channels.

ANAC, besides being a secondary channel, is the **unique channel** indicated by Italian Legislative Decree No. 24/2023 **for reporting on suffered retaliatory acts**.

In case of reverting on ANAC as secondary channel, please refer to the whistleblowing section of the ANAC platform (https://whistleblowing.anticorruzione.it/#/), so that your report will be treated technically as "whistleblowing". Be informed that ANAC considers eligible as "whistleblowing" only the reports on acts, omissions and behaviours that look to breach the laws listed in Italian Legislative Decree No. 24/2023.

**Under specific conditions**, Whistleblower can **also** report **publicly,** if:

- the Whistleblower has priory tried to report via the internal and the secondary channels abiding by the provided prescriptions for each one of the channels, without any feedback within the provided deadline;

- the Whistleblower has grounded concern of immediate and actual harm to public interest if having to pass through the internal channels;
- the Whistleblower has grounded expectation that the report to secondary channels can trigger retaliatory fallouts or that it can be ineffective due to the specific circumstances of the reported misconduct, such as the risk of covering up and destruction of evidences or that the function managing the reporting channels might be involved in the misconduct or with the alleged person.

**!** In making wider disclosure to channels other than the internal ones (second or public), prospective Whistleblowers are **strongly advised** to first seek further specialist guidance from professionals, since serious legal aspects such as Data Protection and criminal law may be involved in the disclosure of concerns. Indeed, if the report to external channel(s) falls short of one or more of the established technical and legal requirements, the reporter may face legal consequences, which are actionable by EMR, the alleged person(s) or the authorities.

**!** If proceeding via external channels (secondary or public), prospective Whistleblowers are here advised that the guarantees and exculpatory conditions (for instance, on the use made of personal data, or against slandering, etc.) provided by Italian Legislative Decree No. 24/2023 are inapplicable:

- when reports are on breaches others than those considered relevant by Legislative Decree No. 24/2023; and/or
- when the Whistleblower(s) cannot fall under the category of those having working relationship with EMERGENCY.

All the aforementioned, **without prejudice of further mechanisms in favour of the reporter that the reporter might turn to** with the aim of claiming for the case or rights, such as, *for instance*:

- typically in the field of EMERGENCY NGO, the channel made available by the donor eventually funding the EMERGENCY action in whose perimeter falls the misconduct or the international organization(s) or the public body(ies) to which EMERGENCY is accredited;
- syndicate(s);
- judicial authority.

In general, Whistleblowers should bear in mind that **wider disclosure over internal channels done unjustifiably and frivolously** could result in disciplinary or legal action and could undermine public confidence in the humanitarian sector.

**EMERGENCY has the duty to protect against any form of retaliation, even if only threatened or attempted, the Whistleblower(s) and the associates, i.e**.:

- those facilitating the disclosure/report and working in the same context;
- Whistleblower's partner or relative within the 4th degree, who is involved in the same work context;
- Whistleblower's direct colleagues;
- Whistleblower's entities doing business in the same sector;
- Anonymous Whistleblower who might be later identified and be subject to retaliation.

**! Any form of retaliation against individuals who reported in good faith** information on crimes, wrongful acts, malpractices or misconducts**, is forbidden.**

This means that any disciplinary action or repercussion - including but not limited to (Art. 17 Italian Lgs. Decree No. 24/2023) *dismissal, suspension, demotion in grade, non-promotion, change of duties, change of place of work, reduction of salary, change of work hours, negative merit notes, negative references; taking disciplinary measures or other sanctions, discrimination, non-renewal of contract (etc.)*) - imposed to the Whistleblower(s) and the associates, who put forward a genuine concern in good faith, is null and void and EMERGENCY could be sanctioned, accordingly.

Furthermore, Whistleblower reporting appropriately and in good faith is protected against claims for violation of personal data or secret (here excluding the medical and the forensic secrecy) concerned in the reported issue.

**It is strictly forbidden to lean any negative consequences on Whistleblower(s) reporting in good faith, regardless of the found substance of the concern.**

In order for the Whistleblower(s) to deserve protection and for the report to be considered genuine, it does NOT matter if the concern is later found ungrounded/unsubstantiated through the relevance evaluation or the investigation segments of the response procedure.
**A genuine concern, submitted appropriately and timely, with full respect of confidentiality, is a precious and valid contribution** to EMERGENCY's pursuit of its values and preservation of its integrity. Thus, even if concern is later found unsubstantiated, no reprisal will hit the Whistleblower(s) or the testimonies nor the reported person**.**

Whistleblowers and their associates, who suffered retaliatory measures as defined by the Italian Legislative Decree No. 24/2023 (i.e. directly connected to having reported a breach relevant to the decree - by a person who falls under the category defined therein - with the established modalities and through the provided channels) shall **report it to ANAC as primary channel** for it to investigate and evaluate the grounds of the alleged retaliation, impose the removal of all retaliatory acts and their consequences and sanction EMERGENCY. This is not, however, an access to remedy for the reported person who is willing to challenge the decisions of the disciplinary proceeding.

Compliance function and all personnel at EMERGENCY receiving such report on retaliatory acts shall promptly revert the reporter to the ANAC channel when relevant, maintain high confidentiality on the report and definitively delete any trace of the report from the entry or internal channel.

! **Malicious** (fabricated, speculative, consciously false, grossly negligent etc.) **concern(s), entered into the reporting channels** for **personal or third party's gain**, with **purpose of defamation, slandering or causing harm** to any personnel or to EMERGENCY itself, constitutes **gross misconduct and it is ground for disciplinary and legal action** (Art, 16, paragraphs 2, and Art. 21 Italian Legislative Decree No. 24/2023) against the malicious reporter(s), pursuing disciplinary sanction system of the Organization, as provided in the MOG ex Italian Legislative Decree No. 231/2001 and the Internal Regulations adopted on January 22, 2019.

**EMERGENCY will pursue on malicious reports** as they affect the security of the working environment, the reputation of the Organization and of the fellow humanitarian workers, and they represent a severe betrayal of ethics and of the mandated values.

**Whistleblowing' safeguards** (included the waivers related to data protection and privacy and security measures, etc.) **do not apply to malicious reporter(s)** and **specific sanctions** for malicious reporting are provided into the sanctioning system of EMERGENCY MOG.

→ The **identity of the Whistleblower(s)**, as well as of the one of **the reported person(s) and of any other person(s) involved** in the reported matter, is to **consider at all times highly confidential**.

The identity of the people involved (**including any information from which the identity may be directly or indirectly inferred**), shall not be disclosed to persons other than those responsible for receiving, investigating the concerned report (and appointed with formal authorization ex Article 12, paragraph 2 of Italian Legislative Decree No. 24/2023) and sanctioning (here limited to the identity of the reported person(s)); **unless the persons** involved give their **different, specific and explicit consent**, and provided that such disclosure is limited to their own identities.

Beyond the bold and explicit rules on data protection (i.e. GDPR) and on Whistleblowing itself for this part, protecting the identity of each and all individuals involved in the report is **straight application of human rights, of respect of human dignity, of principle of innocence and abidance by do no harm.**
In fact, repercussions of data leaks and breaches can be extensive and severe, either for EMERGENCY, the people involved, the served community, in terms of security (up to triggering of honour crimes and attacks to EMERGENCY's facilities) and of dignity and reputation. Usually such accusations are persistent and indelible, regardless of the genesis of the specific incident and the conclusions reached through the investigation.

Due to the severity, violation of confidentiality in this field is to address, pursuing the Organization internal sanctioning system, with**:**

- **proper disciplinary sanctions, up to the dismissal for cause, for employees, if the case may be;**

- **proper contractual actions and/or remedies, for consultants, service providers, suppliers, etc.**

The articulation of this safeguard along the progressive segments of the complaint reporting mechanism (entry, case profiling, referral to investigation, disciplinary proceeding) will be detailed ahead in this document.

The following **principles** govern this Policy, the provided channels for entering reports and the procedures in response (CRM) of the entered concern:
**Transparency:** Whistleblowing Policy and Complaint Reporting Mechanism are known by EMERGENCY personnel, partners, contractors and sub-contractors and by served communities, in particular the purpose, access, procedures and dedicated functions. Relevant involved individuals are notified on progressions in the established procedure;
**Integrity:** Whistleblowing and CRM are consistent with ethical values and standards;
**Accountability:** a mechanism for implementation of the Policy is available, visible, accessible, operational, responsive, informative and responsible functions are assigned;
**Rule of law:** Whistleblowing Policy and CRM are well defined, duties and responsibilities are pre-assigned and known, criteria and rules governing the procedures are detailed and explicit, investigation and decisions come timely, tracked, motivated and notified;
**Impartiality and independence:** objective evaluation of facts based on evidence; the report is treated on its merits, without prejudice, and decisions made is impartial;
**Non-discrimination:** all Whistleblowers, testimonies and alleged persons are treated equally regardless of a person's age, disability, culture, ethnicity, gender, gender identity, religion or sexual preference;
**Responsiveness and Timeliness:** reports are taken seriously and handled swiftly. Notification of receipt to Whistleblower(s) is within 7 days from the knowledge of receipt (24 hours for PSEAH related allegations). Decisions on the incident are made within 3 months (14 days for PSEAH related allegations) from the acknowledgement of receipt unless exceptional circumstances impose a different timing;
**Accessibility:** the mechanism is accessible and it is designed to tackle barriers such as language, illiteracy, poor education, disabilities, poverty, distance, fear of reprisal;
**Cultural appropriateness:** the mechanism is set up to take into account specific cultural attributes of the local communities;
**Limited purpose:** reports are used to the only purpose of investigating suspected violations;
**Consent:** disclosure of personal data of the Whistleblower(s) and the testimonies only by explicit, free, specific consent;
**Confidentiality:** information are minimized to those relevant to the investigation on potential violation and they are shared only among formally authorized people;
**Safety:** potential dangers to each party involved is duly considered through risk analysis and ways deployed to prevent prospective injuries and harm;

**Efficiency and proportionality:** the mechanism uses appropriate methods to handle complaints, according to their level of complexity and sensitivity.

## 4. REPORTING A CONCERN – COMPLAINT REPORTING MECHANISM (CRM)

The aim of the **Complaint Reporting Mechanism** is to **ensure that an appropriate and accessible process visibly exists** which promotes accountability in Emergency NGO "*so that communities and employees are better able to report abuses and access additional protection through deterrence*" , by deploying **a fair, expedite and discreet** mechanism for the emersion, investigation and response to relevant concerns.

**Report shall be made appropriately** through the available channels only – in these regards, please see what already explained in the previous paragraph 3 and, for details on internal channels in paragraph 4.1 hereinafter.

**Reporting appropriately,** entails:

- acting **timely** (*better earlier than later*) through the available channels and instruments;
- submitting/sharing/discussing **information only with the authorized functions** at Main Office or Field Level;
- as far as possible, providing **all** the already available information on **who, what, how, where, when**;
- expressing the personal degree of certainty/uncertainty on the reported facts/acts/omissions/conducts (i.e. I heard/ I saw/ I was there/ I'm sure/I believe that/ I guess/ I sense/ etc.)
- if possible, mention **whom else,** other than the alleged person(s) and the Whistleblower(s), was eventually present or could know about the reported fact/act/omission/conduct;
- attaching **any relevant material evidences**, which are already in Whistleblower's possess at the time of report, that support the allegation(s);
- referencing **any further source of information**, that could support the verification of facts;
- expressing **personal concerns on risks**, that might come along for the reporter(s) and the associate (if any).

**!** **Facts that consist in a violation** in the work-context of EMR can be reported **even without knowing who the alleged person** might be!

**!** **Report can be anonymous.**

In case of anonymous report, EMERGENCY will extend its greatest efforts to find out about the reported issue. However, prospective anonymous Whistleblower(s) shall be informed that anonymity may deeply affect the abilities of EMERGENCY to establish a clear direction for investigation. Moreover, in case of danger for the Whistleblower and associates, anonymity will prevent EMERGENCY from deploying adequate safeguards. Prospective Whistleblower(s) wishing to submit an anonymous report are advised that, in this case, it is even more critical to provide adequate details

on the concerned allegations and the whereabouts in EMERGENCY, as well as to indicate any reliable further source of evidence that EMERGENCY can revert onto for verifying the reported information.

**The Whistleblower can be assisted, if wished so, by a trusted person as facilitator**.

In this case, the trusted person is required to sign off a *Non Disclosure Agreement* and, as a facilitator is entitled to the same protection measures provided for the Whistleblower(s), except for the inversion of the onus of proof in case of retaliation, which is recognized only to the Whistleblower(s).

**! Whistleblower is highly discouraged from starting any investigation alone on the reported (or yet to report) issue,** even if willing to provide material evidence to the report that is about to be submitted.

Investigation is a complex procedure with several safeguards to uphold, thus it is reverted on specifically trained people and dedicated functions.
Moreover, investigating on own initiative the initial concern can expose the Whistleblowers to significant additional risk.
EMERGENCY has provided this mechanism factoring also in Duty of Care, in order to ensure a response without any over-exposure of reporting stakeholder(s).

## 4.1 Channels

EMERGENCY has deployed the following **internal channels for entry of reports**:

- **Dedicated email accounts:**
  - **complaintreporting@emergency.it –** it reverts on Compliance Manager at Main Office in Milan.
    At country mission level, EMERGENCY has deployed country-dedicated functional accounts **complaintreporting.[*country*]@emergency.it** that, for each country, is composed by the following parts "complaintreporting."+ the specific name of the country in English (es. afghanistan/sudan/uganda etc) and it reverts on appointed Complaint Reporting Officers at country level.
  - **complaintcommittee@emergency.it –** it reverts directly to President and Vice-President and shall be **used only when** the other two email addresses are both managed by persons potentially involved in the wrongdoing.

  All languages are allowed, however English is preferable.
  Plain anonymity is impossible to assure when acting through this channel. However, Whistleblowers willing to use pseudonyms are reassured that EMR will not seek at any time, into their IPs or real identity;
- **Complaint box** is a physical box available and marked where present, at EMR facility, office or work site even if these sites are temporary. Complaint box is to locate in non-exclusive-use areas, while ensuring discretion, in order to avoid detection of Whistleblowers (see *Annex 2* for locating

Complaint Box in your duty station). Forms are available at the box premises; nonetheless, free-form papery complaint can be dropped-in, anytime. Complaint box allows fully anonymous complaints. Compliant box is locked and opened at least fortnightly by the Complaint Reporting Officers on the Field (HR Manager and/or Country Admin and/or Country Dir) or by the Compliance Manager at Main Office or by formally authorized and trained people at temporary sites or in other Italy Offices. Collected complaints are then entered into the *Complaint Management Platform* of EMERGENCY (Microsoft ltd) that Complaint Reporting Officers share with Compliance Manager at Main Office.

- Via **postmail in well-closed envelope** to the attention of *Compliance Manager* at EMERGENCY NGO ONLUS, Via S.Croce 19, 20122 Milan, Italy. This channel can ensure full anonymity to the Whistleblower, if wished so.

- **Hotline** (see *Annex 1* for numbers at Country Missions, where relevant) can be available at Country Missions and at Main Office. It consists of a voicemail service where complaints can be submitted 24-7. The voicemail is downloaded by the Complaint Reporting Officers and reports are later entered into the *Complaint Management Platform* at EMERGENCY. Anonymity here is possible for personal identity details, biometrics (voice) and the calling number are collected, though. Any language is allowed.

- **Verbal complaint to dedicated functions:** complaints can be submitted orally to the dedicated functional roles: i.e. Compliant Reporting Officer at Country Mission or Compliance Manager at Main Office. Any language is allowed. When translation is necessary please try to coordinate for such translation or mediation, before the meeting takes place. Anonymity of the Whistleblower here is excluded; however bold safeguards are provided to avoid spreading of identity data.

**!** In case one of the Complaint Reporting Officers in-country is involved by the report, the Whistleblower may revert directly to the other Complaint Reporting Officer at Field level or to the Compliance Manager at Main Office.
In case the Compliance Manager at Main Office should be involved, reports may be reverted to **complaintcommittee@emergency.it**

Personnel at EMERGENCY, other than those entitled and authorized to manage the CRM channels, receiving a report that falls under the scope of this Policy, is **required** to:

- transmit it swiftly within 3 days from the receipt (immediately for PSEAH related reports) directly to the channels indicated above (and/or the roles entitled to manage them);
- notify the reporter accordingly; and
- delete any trace of the report in own instruments, devices, files and records once the entitled role confirms the receipt of the transmission. The transmitting personnel may keep on own files only the acknowledgement of the receipt, as guarantee of having complied with the instructions above.

Any violation of the requirements above is considered misconduct and sanctioned accordingly.

## 4.2 Key roles and Responsibilities

Key roles in managing **the entry and the immediate aftermath** of a report are:

- **Complaint Reporting Officer** (CRO) – is in figure of minimum two people in each country-mission/program, usually those are the HR Field Manager (or the Country Admin where HR Field Manager is not present) and the Country Director, who are specifically and formally appointed for this function and the pertaining data treatment. In circumstances like language barrier, spread service delivery and facilities across fragmented, hardly accessible and/or remote territory, or when one or both the appointed CROs are unavailable, delegates of CROs may be assigned temporarily with defined tasks and with the official clearance of the Compliance Manager, following a dedicated training session;
- **Compliance Manager** (CM), is the qualified person at Main Office, specifically and formally appointed;
- **Complaint Committee** (CC) is composed by President and Vice-president.

These roles are **entrusted with formal assignment** and **formal act of authorization to data treatment,** which is **graduated upon the type of assigned role** (*for instance*, Complaint Reporting Officers have access only to reports that fall under the assigned geographical scope and within the pertaining rank(s) of sensitivity of the complaint) for treating relevant and personal data. They are included in the Data Protection Register with the assigned responsibilities.

For the entry-phase of the report, the following are the main responsibilities for each assigned role:

- **the Complaint Reporting Officer** (CRO):
  - Makes this policy visible at country level and provide advice and training on how to use entry channels;
  - Ensures complaint boxes are duly distributed, appropriately placed and maintained as well as timely opened and papery *Complaint form* and *Disclosure Notice on Data Protection* (*Annex 5*) are available at the premises of the Complaint box;
  - Ensures hotlines are available and functioning;
  - Ensures support to the Whistleblower(s) in case of reporting;
  - Is available for verbal reports;
  - monitors the entry of reports into the dedicated email account at country level, complaintreporting,[*country*]@emergency.it;
  - Ensures personal data (direct and indirect) are protected and shared only among dedicated functions or authorized people;
  - Ensures confidentiality on the entry of the report and its content;
  - Ensures timely collection of reports from Complaint Box and Hotline;

- Ensure notification of receipt to Whistleblower(s) within 7 days (24 hours for PSEAH related reports) from collection together with the *Disclosure Notice on Data Protection*;
- Timely enters received complaints into the Complaint Management Platform.

- **the Compliance Manager (CM)**:
  - Makes this Policy visible at overall level and in Main Office and provide advice and training to all staff and stakeholders on how to use it;
  - Trains, advices, coordinates and supports the Complaint Reporting Officers;
  - Monitors on the entries into complaintreporting@emergency.it
  - Provides notification of receipt of the report to the Whistleblower(s) who entered the report via complaintreporting@emergency.it within 7 days (24 hours for PSEAH related reports) together with *the Disclosure Notice for Data Protection*;
  - Ensures timely review of complaints entered into the Complaint Management Platform by CROs and makes decisions in complaint profiling phase;
  - Enters complaints received through complaintreporting@emergency.it into the Complaint Management Platform;
  - Reports on complaint-drop to the Complaint Committee with due *data minimization*, in order to keep this procedure accountable;
  - Ensures minimization of personal data in the report and confidentiality of the report and the contents;
  - Monitors channels in order to learn on potential weaknesses and recommendable improvements.

- the **Complaint Committee** (CC):
  - Ensures notification of receipt to the Whistleblower reporting directly through complaintcommittee@emergency.it within 7 days from the receipt of (24 hours for PSEAH related report) together with the *Disclosure Notice for Data Protection*;
  - Ensures confidentiality on the entry of the report, its content and the pertaining personal data.

## 4.3 Visibility

**Channels listed above shall be visible and accessible**.

To ensure adequate visibility and accessibility, the following measures apply:
- Publication on EMERGENCY's website (also pursuing prescriptions of Italian D.Lgs. 24/2023);
- Footnote message in emails from the compliance function attained roles;
- Inclusion of reference to this Policy and the CRM to all contracts with personnel, partners and contractors;
- Dedicated induction session for newly recruited staff;
- Refresher trainings for all personnel;

- Consistent messages and signs on EMERGENCY's Accountability System in the country-missions and related activity sites, which are adequate to the context.

## 4.4 Confidentiality

**! Identities of the Whistleblower(s), of the alleged person(s) and of third parties included in the report,** as either direct witnesses or informed people, **are highly confidential.**

These identities, where known or inferable in any way, are **to keep secret** and are to **disclose**, yet abiding by *data minimization* principle, **only among the people formally authorized** to receive and treat the complaint.

The Complaint Reporting Officer(s) at Field Offices and/or the Compliance Manager at Main Office will act, also in the notification of the Complaint Committee, **abiding by rigorous protection standards** regarding these identities, which could not be disclosed in any case, unless prescribed conditions occur ( *i.e.*, at the same time, consent+ necessity/absence of other material evidence).

Identity of the Whistleblower(s), the victim/survivor(s) might be disclosed to the Investigation Team, (*see below* paragraph 5 and subsequent) **if and to the extent** to which they are **essential to the investigation**.

Identity of the alleged person is disclosed limited to the Investigation Team and, if the case may be, to those in charge of the disciplinary proceeding.

Identity of the witness/testimony and informed people are to disclose only to the Investigation Team.

In case the Whistleblower(s) or the victim(s) require(s) the identity to be secret, then the Complaint Reporting Officer(s) and/or the Compliance Manager shall protect the identity even in the referral for investigation.

Hence, when identities are essential to the investigation (even preliminarily), the Complaint Reporting Officer(s) and/or the Compliance Manager will inform the Whistleblower(s) or the victim(s) that the investigation may suffer of the secrecy to the point of not allowing further investigation and wait for the Whistleblower(s)' or victim(s)' final decision on consent.

Whistleblower(s) and testimony(ies) are here informed that this request may come to them only by the Compliance Manager or the Complaint Reporting Officer(s) with sole purpose of guaranteeing the investigation of the reported behaviour.

When the report allows the collection of evidences and clues beyond the statements contained in the report, then the Whistleblower(s) or victim(s)' identity shall be kept highly confidential and cannot be disclosed.

**The entry of a report itself is to keep highly confidential.**

Notifications beyond the first receiver of the complaint/report content will involve only the authorized people at the Compliance function (Complaint Reporting Officer(s), Compliance Manager, Complaint Committee, Investigation Team and DPO or Supervisory Board, where relevant).

Other notifications, *for instance* those due for early warning purposes, are to release only by the Compliance Manager or by the Complaint Committee, and they will only contain the essential information necessary for mitigating risks, without any further details on the complainant, the complaint and other people involved.

All entry channels listed above are designed and deployed in ways that intend to guarantee protection of data, especially for identities and any further element from which identities are inferable directly or indirectly.

Any violation of the duty of confidentiality, including the fact that a report enters and/or its contents, is to sanction as a violation of EMERGENCY's integrity standards and of contractual obligations (work secrecy).

Confidentiality on identity of the Whistleblower(s), victim, alleged person(s) and witnesses and persons however mentioned in the report, **is prescribed by the law**.

Any violation of the safeguards listed above can be heavily fined by the related authorities and by EMERGENCY itself.

## 4.5 Communication/Feedback

Notification of receipt is due to the known or reachable Whistleblower(s) within 7 days (24 hours for PSEAH related report) from the acknowledgement of the report by the dedicated function.

The notification may include the *Disclosure Notice on Data Protection*, a brief description of the CRM at EMERGENCY with the aim of informing the Whistleblower on pertaining rights and access to protective measures.

Verification on Whistleblower(s) and associates' (if any) exposure to danger because of the report, shall be made swiftly at the time of this notification, if not expressed yet in the report itself.

When:

- the Whistleblower(s) is a staff member and it is deemed appropriate to apply protective measures; and/or
- the alleged person(s) is a staff member and it is deemed necessary to swiftly apply precautionary measures in order to separate the alleged person(s) from the working environment and/or the victim(s);

*then,*

the entry of the report will be notified to the relevant most senior line manager(s) of either/both of the alleged person(s) or of the Whistleblower(s), yet strictly abiding by minimization of data principle, in order to ensure coordination in the application of supporting or protective measures and the safety of the person(s) involved and of the operational environment, as well as the integrity of the verification process.

## 4.6 Profiling the report (relevance)

→ **Upon receipt, the report is registered into the Complaint Management Platform.**

The Complaint Management Platform is a digital instrument at EMERGENCY's IT infrastructure, dedicated to proper data transfer between duly authorized officers at Field and Main Office levels, and utilized to track, verify and store the progressions on the report. The Platform allows unlimited access only to the Compliance Manager (Main Office) and to the IT administrator (who, however, is not allowed to visualize contents). Complaint Reporting Officers, instead have visibility restricted to those country-specific complaints that they have directly uploaded into the Platform or that the Compliance Manager has shared with them.

→ **Strictly within 20 days (24 hours for PSEAH-related report) from the receipt,** the Compliance Manager, either alone or in coordination with Complaint Reporting Officer(s) for the mission, will conduct verification on the relevance of the report under Compliance and the case profiling review of relevant reports.

This phase is intended to:

→ **verify the relevance of the report** – with descending immediate exclusion of slanderous, unreadable, out of scope complaints or feedbacks and requests in nature, *see* paragraph 2 here above;

→ **verify the completeness of the report**; whenever feasible, the CM or the CROs will put forward request for integrations (preliminary investigation);

→ **verify the exact nature of the allegation(s)** for those reports that resulted relevant, despite and beyond what is expressed in the original report;

→ **assign the sensitivity rate to the relevant report** and reverting it under the provided procedure;

→ **elaborate the *Case Profiling Template*** (*see* Annex 3) for the relevant report, in order to launch and organize the investigation.

→ Compliance function role can **conclude on the irrelevance** of a report when:

- the content is slanderous or generic without the chance to obtain clarifications;
- the report is unreadable, deteriorated, expressed in a second language in such a poor way that is impossible to understand it;
- is evidently an individual labour claim;
- it is about a conflict/grievance at work without traits of threat, corruption, fraud, harassment, sexual harassment, bossing, mobbing or the violation of other pertaining laws;
- it is already in the public domain;
- it is about dissatisfaction with the type, extension, modalities, location of service delivery;
- it is out of control and command of EMERGENCY, **unless** it is **SEAH- related** in other international or national NGOs **in missions where EMERGENCY sits in PSEAH clusters or Network**.

**! PSEAH related reports are to investigate mandatorily in any case and circumstance**, regardless of the completeness of the original report and of the consent by the survivor to disclose identity or to participate into the investigation. In case of denial of consent by the survivor, the related testimony cannot be used in the accusations.

→ **A report resulted irrelevant under Compliance**, can be re-directed (within the confidentiality limits) **to other competent functions in** EMERGENCY, when:

- it is about an individual labour claim or a grievance in the work team or a work performance related matter;
- it is about dissatisfaction on the type, modalities, whereabouts, distribution or extension of ancillary services (canteen, laundry and similar);
- it is, in its own nature, a feedback or a comment;
- it is, in its own nature, a request related to subjects other than ethical, legal and integrity standards.

In the cases listed above, the report can be re-directed by the CM, with the appraisal of the reporter, under the relevant department and dealt with through the provided procedures for the related matter.

→ In **case profiling phase**, the Compliance Manager might try to collect further information to reach better understanding on the relevance and/or seriousness of the reported conduct/incident, in order to decide whether to drop the case, to re-direct it under a different procedure or to apply the pertinent sensitivity rate a (*see the table below in par. 4.8*) and proceed accordingly.

All personnel and associates shall guarantee the highest degree of timely collaboration with the Compliance function at EMERGENCY, in order for such function to qualify the entered report(s) correctly. Hence, reluctance, unjustified delay, obstruction, opposition are to consider serious misconduct and sanctioned accordingly, when relevant.
Pursuant the confidentiality principle, the Compliance function cannot specify what reasons led to the request for information, while the contacted person may not disclose to any other party on having received a request of information by the Compliance function nor the subject thereof.
Compliance Manager or Complaint Reporting Officer(s) may also contact the known Whistleblower(s) to integrate information or exclude that the case is double-treated. They may also request an interview or declaration to ascertain such facts.

From this moment, the CM or the CRO informs the Whistleblower(s) on the chance to receive assistance from a trusted person upon Whistleblower's preference. Should the Whistleblower(s) request the support of a trusted person, such person, with the exclusion of lawyers, will have to sign off the *Nondiclosure Agreement* before being allowed to access the procedure.

During this phase, translation could reveal critical to understand the report, the eventual evidences attached and/or to gain insight that allows to rate the sensitivity of the case.

**Translation could be in-house or out-sourced.**

In-house translation may revert on native speaker colleagues, preferably national HR Officer(s) with the ability of speaking a good level of English. When it is not recommendable to involve national HR Officer(s) – i.e. lack of due neutrality, biases, conflict of interest, other risks, etc. - or HR Officer(s) is/are not present in country mission, another staff member can be appointed for the task. The appointed translator shall sign the *Nondisclosure Agreement*, including a specific *Non-conflict of interest clause* tailored to the case.

Out-sourced translation is necessary in case no staff member can be appointed. The out-sourced translator shall sign off a *Nondisclosure Agreement* with a *no-conflict-of-interest clause* and be able to guarantee data protection standards, beside the professional ones. This option is to consider residual as it could slow down the procedure and pose higher risks for confidentiality, since the Compliance Manager and/or the Complaint Reporting Officer(s) cannot ascertain, beforehand which data are to minimize.

## 4.7 Protective Measures and Precautionary Measures

Protection measures, listed in paragraph 3 above, include protection from negative consequences following the filing of a report and supporting measures during the investigation process.

→ Additionally, EMERGENCY will provide precautionary measures in order to mitigate risks for the Whistleblower(s), the victim(s) (if different from the Whistleblower(s)), the associates, the public interest and the integrity of EMERGENCY itself, along the submission of the report and the reach of conclusion on the case (either in the preliminary phase, in the full investigation phase or in the disciplinary proceeding phase).

→ At the reception of a report, and once initial information are sufficient, EMERGENCY, through the risk assessment exerted by the CM in this phase, will evaluate risks for:

- the public interest (such as threat to public health, security, etc.);
- the Whistleblower(s) in person and associates (when the Whistleblower is known);
- the testimonies and informed people;
- the alleged person(s);
- the second (as donors, for instance) and the third parties.

After completion of the risk assessment, the Complaint Committee, together with Compliance Manager, may decide to take precautionary measures. Such measures are several and they may apply either to the alleged person(s), to the work environment, to the running action, to the victim(s) and may include distancing the persons involved, publishing specific alerts and suspending from work the persons involved, etc. Such a timely response to risks is a matter of responsibility falling under Duty of Care.

**!** **In PSEAH-related allegations**, the *victim-centered approach* imposes to apply precautionary measures as soon as possible, in order to avoid repetition of alleged violation and to prevent the causing of further damage to the survivor(s), the associates and the community of beneficiaries as a whole.

## 4.8 Case Profiling Conclusions – Notification and Report

→ The conclusions of **case profiling** can span through:

- ***Irrelevant*** (readability, relevance, type of wrongdoing, degree of control by EMR, etc.)
- ***Case to investigate/deal with*** *at Field Level;*
- ***Case to upscale to Complaint Committee at Main Office*** *for eventual investigation* (always the case for PSEAH and Child Safeguarding related reports).

→ **Case sensitivity rate** is pre-established (see the table below as a non-exhaustive list). At each rate it corresponds the main owner(s) of the investigation:

| RATE | CATEGORY | OWNER/ CO-OWNER |
|---|---|---|
| 0 | One-on-one grievances in work environment related to work organization, performance, fitting the assigned role, respecting work shift and working hours;<br>Minor, non-systematic irregularities and inaccuracies in procedures and operational protocols;<br>Disappointment/dissatisfaction on ancillary services (canteen, laundry, etc.) not showing signs of potential fraud/corruption, threat to public health, etc.;<br>Disappointment on cultural/religious inappropriateness below hate speech level;<br>Use of EMERGENCY logo and role for personal profit;<br>Gambling;<br>Occasional eccentric behaviours in the work environment and/or context;<br>Low and medium-low failures in work secrecy. | Field |
| 1 | Collective grievances in work environment, irregularities, failures and delays affecting correctness in decent work (social security included) and safety and security standards;<br>Misappropriation;<br>Embezzlement;<br>Incorrect use of equipment;<br>Recurrent use of narcotics and alcohol;<br>Harassment;<br>Inappropriate language and rudeness;<br>Hate speech;<br>High failures in work secrecy;<br>Gross negligence in personal data protection;<br>Violation of Whistleblowing Policy;<br>Mobbing e bossing;<br>Fabrication of information/documentation due to structural delays and internal negligence;<br>Potential risks for patients' safety and security; | Field/CM |

| | | |
|---|---|---|
| | Improper disposal of waste at EMERGENCY premises; etc. | |
| 2 | Failures in *core humanitarian standards*;<br>Failures in *Do no harm*;<br>Failures in services with the potential of triggering violent reactions (security);<br>Near-miss in security and safety regulations;<br>Reluctance and unjustifiable failures in investigation at Field Level;<br>Off-records with the potential for setting up slush (illicit) funds;<br>Failures in launching procurement and in the related selection process;<br>Absence of contractual documentation where required;<br>Dangerous handling/disposal of health waste;<br>etc. | CM/CC |
| 3 | Failures in Humanitarian Principles, PSEAH, Child Safeguarding, Corruption, Fraud, Data Protection and Privacy,<br>Major safety and security violations;<br>Money-laundering,<br>Terrorism financing,<br>Aiding and Abetting irregular immigration;<br>Human Trafficking,<br>Modern slavery,<br>Infibulation,<br>Environmental pollution,<br>Threat to public health,<br>Macro-crimes,<br>Notification of international, national, local authorities' indictment against EMERGENCY,<br>Notification of private's indictment against EMERGENCY. | CM/CC+DPO (if relevant) +OdV |

→ Case sensitivity rate is assigned upon information available at prima facie level. During the investigation, **case sensitivity rate can increase or decrease** upon the progressive gathering of additional information and/or evidences. Where sensitivity rate decreases in such a way to return into Field Level from Main Office, then the investigation or decision is reverted to the Field level. On the opposite, when sensitivity rate increases in such a way to trigger Main Office competence, then the investigation and/or decision thereof is reverted to the Main Office bodies and procedures at that level.

In each and every case, **the Whistleblower(s) shall be informed** on the conclusions of this phase and the following steps, either investigation or decision.

**! When set forth as contractual obligations** with institutional donors, for the relevant sensitivity rate assigned to the report, the Compliance Manager shall notify the donor through the channels provided in the contract that EMERGENCY has received a grounded report, specifying the type of allegation and to which facility/duty station it relates; the notice shall also indicate the procedure and timeline that will be followed. The notice shall not disclose details on the facts described in the

report; specifically, no mention to the identities, where known, of Whistleblower(s), alleged person(s), informed people/testimonies shall be disclosed to the donor.

### 4.9 Tracking and Retention

→ When report is relevant, the CM or the CROs shall **elaborate *the Case Profiling Template*** (see Annex 3) and upload it to the Case Management Platform, yet abiding by the *data minimization* principle.

This document shall frame the subsequent actions of the Investigation Team, defining and tailoring the scope of the investigation, planning the investigative tasks and keeping track of the relevant evolvements along the carryout of the procedure.

The *Case Profiling Template* is to share exclusively through a link generated by the Complaint Management Platform, while **downloading the file into the pc or transferring and copying into own individual account is prohibited.** The link is accessible only through personal work email account of the members of the CC and the Investigation Team (when not assigned to external services).

When investigation and/or decision is/are at Field level only, the Complaint Reporting Officer(s) shall upload the relevant progressions, findings and conclusions into the Complaint Management Platform. Only the CROs and the CM shall access such documents and information.

**! The Complaint Management Platform tracks and registers, for any future verification, every access and all the pertaining actions in this environment.**

→ **Complaints profiled as relevant** (and eventually investigated) shall be **kept on the register for 5 years from closure of the relevant proceeding, regardless of the type decision taken.**

→ **Reports considered irrelevant or re-directed under other procedure**, are subject of a monthly anonymized report elaborated by the CM that is sent out to the Complaint Committee for accountability of the actions and decisions made around these reports. The CM keeps the related reports, segregating them from the related personal data, for 3 months after the consolidation of the monthly report, and later, if no issue occurs, delete them definitively.

→ **A separate section of the register dedicated to no case-complaint drops shall be kept for 3 years** in the **anonymized version**, in order to allow learning and connecting eventually re-emerging issues, while Compliance Manager, with the support of IT services and DPO, ensures non-recoverability of the cancelled personal data.

# 5. INTERNAL INVESTIGATION PROCEDURE

## 5.1 Investigation bodies

→ When a relevant complaint is profiled at **sensitivity rate 1 through 3**, it can (1)/shall (2-3) upscale **to Complaint Committee** in the composition of the President and Vice-President, together with the Compliance Manager.

→ When assigned a **sensitivity rate 0 through 1**, the relevant complaint is to manage **at Field Level**, where the most of the procedure stays in the competence of the CROs, instead.

The **Complaint Committee** at Main Office (**sensitivity 1-3**), or the C**ROs at Field together with the CM** (**sensitivity 0-1**), may conclude that:

- all the necessary information are already collected and verified and decision can be made on the reported facts – case is directly referred for final decision and disciplinary proceeding (par. 6 below) where relevant;

or

- further investigation on the reported facts is necessary.

→ **When further investigation is deemed necessary**, then the CROs when the report stays at Field Level (0-1) or the Complaint Committee at Main Office when the report scales up to this body (1-3), either case with the support of the CM, activate the **Investigation Team**.

| INVESTIGATION TEAM COMPOSITION | |
|---|---|
| LEVEL | MEMBERS |
| FIELD | HR FIELD MANAGER AND COUNTRY DIRECTOR, *IN CONSULTATION WITH* THE COMPLIANCE MANAGER. |
| MAIN OFFICE | HR DEPARTMENT RESPONSIBLE PERSON, REFERENT OF THE LEGAL OFFICE AND COMPLIANCE MANAGER. |

**! Whistleblowers, alleged persons and testimonies are informed that report and its content can be dealt with by external consultants.** In this case, the external consultants are required to uphold the confidentiality standards provided by Italian Legislative Decree No. 24/2023 with its references to GDPR and EMERGENCY will ask to sign specific Data Protection Agreement.

→ **Commission for Investigation** at Main Office at minimum is composed by:

- President;
- FOD Director, as directly responsible for the implementation of field activities;

- Chairman of the Supervisory Board, for the analysis of topics linking to the Legislative Decree No. 231/2001.

**The Commission for Investigation** at Main Office can decide to add other members on the following basis:
- Absence of conflict of interest or renowned biases;
- Relevant subject matter investigated (programming/administration&finance/logistics/ medical/communication/security/etc.)
- Technical aspects involved in the reported matter.

**The additional members** might include, without limitations, the following functions at EMERGENCY:
- Scientific Director, for the analysis of health issues relating to patients management;
- DPO, when a reported issue deals with Data Protection and Confidentiality breaches;
- Person in Charge of Safety & Security at the Work Place at EMERGENCY when a reported issues deals with Safety&Security at the work place;
- PSS Specialists, for PSEAH-related reports;
- Financial Director, when a reported issue deals with financial and economic issues;
- IT Director/Cyber security Specialist.

Internal functions and/or third parties in charge as members of **Commission for Investigation** at Main Office shall be required to sign off the *Nondisclosure Agreement* together with the *Non-Conflict of Interest Clause*.

→ The Compliance Manager shall inform the Commission for Investigation at Main Office on the case, at the end of the Investigation procedure, through the *Final Report on Investigation* (Annex 6), provided that all personal data are removed unless they are essential for decision-making, and in any case secreting the identities of the victim(s) and/or the whistleblower(s) – as well as the information that could indirectly allow the identification – if consent on disclosure was denied.

→ Where the case is to immediately refer for decision to the Commission for Investigation at Main Office without any investigation procedure, then the Commission is informed on the case by the Compliance Manager through the *Case Profiling Template*, provided that all personal data are removed unless they are essential for decision-making, and in any case secreting the identities of the victim(s) and/or the whistleblower(s) – as well as the information that could indirectly allow the identification – if consent on disclosure was denied.

→ **! Downloading shared files into personal device, removing password from these files and sharing/transmitting the files outside the Commission members and those entitled along this procedure is strictly prohibited.**

The **Investigation Team at Field Level** will decide on the findings of the Investigation and validate the made decision with the Compliance Manager, who might inform, where conditions allow that, the concerned senior manager at Main Office.

## 5.2 Key Roles and Responsibilities

**Investigation Team** shall:

- establish an investigation plan, track all progressive steps into the case profiling template (see Annex 4);
- **!** refrain from investigating political opinions, cultural preferences and religious beliefs of the alleged person(s) and/or the Whistleblower(s) as well as any personal aspects irrelevant to the subject matter of the incident that might emerge along/by the investigative operations from work devices, emails, texts, posts, communication etc.;
- **!** protect confidentiality throughout;
- refrain from notifying/informing other functions/people unless necessary for taking swift precautionary measures and within the limits agreed with the Compliance Manager who is in charge of the eventual notifications;
- proceed swiftly by upholding the timeline of max 2 months from the reception of the report (in case of PSEAH related incidents, recommended timing is within 2 weeks since the report);
- **!** track all progressive steps, findings and outcomes;
- come to conclusion in a timely, complete, motivated and written manner in the Final Report on Investigation.

**Commission for Investigation** at Main Office shall:

- **!** be composed quickly as summoned by the Compliance Manager;
- Review and evaluate swiftly the Investigation findings and conclusions;
- Decide on descending measures (if any);
- **!** Keep a Minutes of Meeting in writing.

## 5.3Protective Measures and Precautionary Measures

*See paragraph 4.7 above.*

## 5.4 Notifiche

Once the Commission for Investigation at Main Office - or the Investigation Team at Field Level - reaches the decision on the case, the Compliance Manager, or the Complaint Reporting Officer(s) at Field level, promptly notifies conclusions on the case to:

| COMMUNICATION OF CONCLUSIONS | |
|---|---|
| → ANY CONCLUSIONS | |
| TO | CONTENT AND MODALITIES |

| | |
|---|---|
| Known Whistleblower(s) | main trait of the conclusions (*case closed for no case to answer or lack of evidence, or innocence of the originally alleged person; carry-over to disciplinary proceeding, or a combination of the preceding ones*); ultimate (set of) allegation(s), steps to follow ahead, timing, ensuring data minimization at the most extent. |
| Known alleged person | if heard during the investigation |
| Donors which were informed of the emersion of a relevant case | upon outstanding contractual obligations with the pertaining provided instrument (if any) |
| Senior manager previously informed on the need for precautionary or protective measures | limited to the descending removal or continuation of precautionary (alleged person(s)) or protective (Whistleblower(s) and testimony(ies)) measures. |
| → IF CARRY-OVER TO THE DISCIPLINARY PROCEEDING – MAIN OFFICE LEVEL | |
| ✚ To the HR Department, which is in charge of instructing the disciplinary proceeding | the abstract of the *Minutes of Meeting* of the *Commission for Investigation* at Main Office will be shared through the link to the Complaint Management Platform |
| ✚ To the known Whistleblower(s) and testimony(ies) | with the aim of establishing whether they accept their identities to be disclosed during the disciplinary proceeding when allegation(s) of misconduct against the reported person(s) mainly rests on their declarations. |
| → IF CARRY-OVER TO DISCIPLIANRY PROCEEDING – FIELD LEVEL | |
| ✚ To the Compliance Manager | to validate the made decision before any application; |
| ✚ To the known Whistleblower(s) and testimony(ies) | with the aim of establishing whether they accept their identities to be disclosed during the disciplinary proceeding when allegation(s) of |

| | |
|---|---|
| | misconduct against the reported person(s) mainly rests on their declarations. |

Any further notification deemed necessary for the specific traits of the case and its circumstances is to discuss previously with the Complaint Committee, consulting the DPO, and to be approved formally before release.

### 5.5 Retention

Retention varies upon the type of conclusion.

- → Cases closed with the formula **no case to answer** shall be anonymized (eventual material evidences apprehended are definitively cancelled) and **only essential information for learning purposes can be kept**. The essential information are stored in a separate section of the register in Complaint Management Platform **for 1 year** and form part of Compliance Manager's annual report to the Board of Directors.

- → Cases closed with the formula of **innocence of the originally alleged person(s) are anonymized** and kept **for 1 year in their essential information for learning purposes only** in a separate section of the register on the Complaint Management Platform.

- → Cases closed with the formula of **lack of evidence** are kept in separate section of the register in Complaints Management Platform **for 3 years**, **especially when PSEAH related**, since new information may be found or repetition of the alleged conduct could disclose elements that are also informative to the one investigated previously.

- → Cases **to carry-over to disciplinary proceeding** shall comply with the rule established in Italian Legislative Decree No. 24/2023; hence, documents shall be kept **for 5 years from the notification of the conclusion** of the disciplinary proceeding.

- → **Combinations of the above formulas for one case** shall be treated in a differentiated manner and **information essential to each part are to keep in the different relevant sections** of the register in the Complaint Management Platform, **for a timing that complies** with the rules established for each type of conclusion.

# 6. DISCIPLINARY PROCEEDING (SANCTIONING)

**Disciplinary proceeding highly factor into human rights and national labour laws**.

For EMERGENCY system described above, disciplinary proceeding **shall begin following a decision** of the **Commission for Investigation at Main Office** or **the Investigation Team at Field Level** such as ***to carry-over to disciplinary proceeding***.

Clearly, no reported or detected allegation(s) of breach can be sanctioned bypassing the phase of the disciplinary proceeding.

**!** **Applicable sanctions** in disciplinary proceeding shall only be those:

- allowed by human rights law (and decent work standards in particular);
- allowed by applicable national labour laws and strictly within limits established therein,
- included in the Organization sanctioning system and made known to personnel, partners and (sub)contractors before the occurrence of the relevant facts and conduct.

## 6.1 Descending Measures

Disciplinary proceeding starts from the *Minutes of Meeting of the Commission for Investigation* at Main Office or the *Final Report on Investigation* of *the Investigation Team at Field Level*, since it results from the conclusions therein and the descending measures provided therein.

Disciplinary proceeding **shall display and finalize swiftly, within 14 days from the communication of the decision** made by the Commission for Internal Investigation at Main Office or by the Investigation Team at Field Level, for the latter case as validated by the CM.

Applicable disciplinary measures are, specifically, those indicated **in the MOG** ex Italian Legislative Decree 231/2001 of EMERGENCY and **the internal regulations adopted on January 22, 2019**.

Sanctions are applied **in a motivated manner** and **strictly upon the following criteria**::

- pre-established automatic sanction for type of substantiated allegation, where relevant (for instance, PSEAH);
- objective severity of breach in a given range (nature, qualification by law/CoC), also considering dimension and impact of caused or potential harm;
- subjective severity of breach (negligence, gross negligence, will);
- either attempted or committed breach, where relevant (excluded for PSEAH);
- existence of exculpatory circumstance for the alleged person(s) (blameless condition at the time of the act/omission/conduct, state of need/necessity, deception, repentance, etc.);
- existence of aggravating circumstance for the alleged person (role, specialization, reiteration, etc.).

**Previously applied precautionary measures** to the alleged person(s) may be continued, removed or even considered sufficient to absorb the descending disciplinary measures established at this phase.

**Previously provided protective measures** to the Whistleblowers and associates might be continued, removed, increased or decreased upon the outcomes of this procedure and the eventual changes in the context (risk analysis and updating).
The delegate for the disciplinary proceeding:

- → elaborates **the formal communication** containing the disciplinary measure(s) applied **with clear and motivated reference to the proven** conduct/act/omission **and the criteria** that has headed to the type of sanction(s) **to the alleged person(s)**;
- → **obtains the signing off of the communication by the authorized role** for sanctioning at the Organization;
- → **notifies the alleged person(s) accordingly**.

## 6.2 Notification

- → Compliance Manager is to notify on the completion of the disciplinary proceeding and of the resulting applied measures.
- → When allegation(s) fall under MOG and OdV members were not involved neither in the Commission for Investigation at Main Office nor in the disciplinary proceeding, then the disciplinary proceeding delegate shall notify the outcomes to the OdV.

- → CM or CRO (if at Field Level), **notifies the Whistleblower** on the completion of the procedure, with the main traits (sanctioned/not sanctioned), the timing for application and the responsible function at EMR for further action.
- → **! Unless the Whistleblower(s) is direct victim** of abusing, harassing and exploiting conducts by the alleged person(s) no detail on the type of sanction applied to the alleged person(s) is to share to the Whistleblower(s) in the final feedback.

## 6.3 Retention

Retention terms are established directly by the law.

| RETENTION CATEGORIES | | |
|---|---|---|
| CATEGORY | TIMING | RESPONSIBLE FOR RETENTION |
| NO LAW SUIT | 5 YEARS FROM THE NOTIFICATION TO THE WHISTLEBLOWER OF THE CONCLUSIONS | COMPLIANCE MANAGER<br>RELEVANT HR OFFICE |
| LAW SUIT | VARIES DEPENDING ON THE DURATION OF THE RELEVANT | RELEVANT HR OFFICE |

| | | |
|---|---|---|
| | LITIGATION AND SUBSEQUENT APPLICABLE RETENTION TERMS | |
| DISCIPLINARY MEASURES APPLIED TO EMERGENCY NGO PERSONNEL | 5 YEARS IN THE EMPLOYEE'S PERSONAL FILE AT THE HR DEPARTMENT, ALSO IN CASE THE EMPLOYEE IS DISMISSED | RELEVANT HR OFFICE |
| MEASURES APPLIED TO (SUB) CONTRACTORS AND CONSULTANTS | 3 TO 5 YEARS FROM THE COMMUNICATION OF THE SANCTION AND UPON ITS SEVERITY | RELEVANT DEPARTMENT |

## 7. TRAINING AND DISSEMINATION

All EMERGENCY Personnel shall become acquainted and be duly trained on the contents of this Whistleblowing Policy, in order for such Policy to effectively impact on the prevention of the relevant facts.

- → This Policy **shall be attached to the employment agreements of all staff members**. Employees and prospective employees shall commit to read carefully the Policy, declare that they have read and understood such Policy and undertake to comply with the terms and conditions contained herein.
- → **Clear reference to this Whistleblowing Policy shall be shared with actual and prospective contractual counterparts before entering into the relevant agreements.** They shall be required to declare in the agreements with EMERGENCY that they have read and will comply with the Policy.
- → **Implementing Partners** (i.e. participating in a consortium for the carry-out of an intervention), at least those in actions funded by institutional donors, are required to follow a training session on this Policy, unless they can prove they have their own and it was properly disseminated.

Training plan on this Policy and pertaining procedures inside EMERGENCY are **based on proper identification of differing training needs** of staff **based on their respective functions**, tasks and responsibilities and based on their different potential exposure to/direct contact with beneficiaries.

The table below indicates, for each staff category, the type and number of hours of training and the periodicity for refresher training sessions:

| Staff Category | Type of training | Period |
|---|---|---|

| | | |
|---|---|---|
| Complaint Reporting Officer(s) | ToT<br>12 hours | At the entry and every 18 months or earlier at any change in structure and Policy |
| Managers who might be called to sit in the Commission for Investigation or as delegate in disciplinary proceeding | Advanced Training<br>6 hours | At the entry and every 18 months or earlier at any change in structure and Policy |
| Personnel "at the last mile" (in the facilities, where services are delivered) | Intermediate Training<br>4 hours | At the entry and every 12 months or earlier at any change in structure and Policy |
| Line Managers | Intermediate Training<br>3 hours | At the entry and every 12 months |
| Other staff/personnel | Basic Training<br>2 hours | At the entry and every 18 months or earlier where Policy is revised |

| External | Type of Training | Period |
|---|---|---|
| Implementing Partner' and sub-grantee' senior managers and appointed CRO(s) | Intermediate Training<br>3 hours | Upon the timing expressed in the pertaining MoU |
| Contractors, Sub-contractors, suppliers, vendors | Informative session<br>1 hours | At the entry and upon the timing established in the contract |

Training sessions may also be exerted by means of e-learning tools and procedures, provided that appropriate tools are implemented to check that trainees take effective training, and they can interact real time with the trainer.

Training sessions shall be held by trainers specialized in the relevant subject matters and/or by the Compliance Manager. At the Field level, also the Complaint Reporting Officer(s) may act as trainer(s), once CROs have already received the relevant ToT (see table above in this paragraph).

**At least once along the working relationship with EMERGENCY, every staff member would have received a training in presence.**

**!**Trainings shall be tracked through an agenda of topics, date/time and signed off by the trainer and the trainee(s). These tracking instruments are kept by the HR function either at Main Office or Field Level.

**!** All **persons eligible for training** shall **be informed that that their names may be shared with EMERGENCY's donor(s) and second party auditor(s)** when required, based on specific contractual obligations.

The Compliance Manager, with the support of Complaint Reporting Officer(s) for the Field Level, shall keep a parallel register. Such register shall record, for each training session, the type of training, type and # of trainees, agenda, duration, date and time of delivery, place/method and trainer(s), owner of the supporting documentation and type of supporting documentation. The retention term of this information is 3 years from the day on which training for each session is completed

## 8. MONITORING AND LEARNING

**Accountability principle** requires the Compliance function **to regularly monitor** the application of this Policy.

- → As indicated above, the **Compliance function will keep an up to date register of complaints**, recording all cases, which were dropped, taken ahead to investigation and eventually up to disciplinary proceedings. Such register will be **a tool for monitoring the performance** of EMERGENCY in handling these procedures.
- → At least **once a year, the Compliance Manager shall report to EMERGENCY's Board of Directors** the outcomes of compliance activity, based on data recorded in the register and on periodic surveys, in order to give information for **implementing and improving EMERGENCY's compliance system**, implementing plans of internal audit and setting goals in terms of integrity and compliance.
- → A copy of such report shall also be delivered to the Supervisory Board.

# ANNEX 1

# Hotlines numbers sheet

RECIPIENTS:

ALL

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

| COUNTRY | HOTLINE N° | ACTIVATION |
|---|---|---|
| AFGHANISTAN | (0093) 07990001233 | 06/2022 |
| KRI | *SETTING IN 2024* | --/2024 |
| ITALIA | *(0039) 02-8631 6893* | 11/2022 |
| SIERRA LEONE | *SETTING IN 2024* | --/2024 |
| SUDAN | CURRENTLY INACTIVE DUE TO THE CRISIS' IMPACT ON LANDLINE | 06/2022 |
| UGANDA | *SETTING IN 2024* | --/2024 |

# Annex 2

# Locations of Complaint Box

RECIPIENTS:

ALL

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

| COUNTRY | SITE | LOCATION |
|---|---|---|
| AFGHANISTAN | KABUL HOSPITAL | Box outside Head Nurse office, outside SUB ICU, outside Main Office |
| | ANABAH HOSPITAL | Box outside Maternity, outside Driver Room, outside OPD |
| | LASHKAR GHA HOSPITAL | Box outside Main Office, outside Main Gate, outside OPD |
| KRI | SULEYMANYA REHABILITATION CENTRE | to deploy |

| | | |
|---|---|---|
| ITALIA | UFFICIO DI MILANO | *ANTI BAGNO 1° PIANO DX*<br>*ANTI BAGNO 3° PIANO SX* |
| | UFFICIO DI ROMA | *ANTI-BAGNO* |
| | LIFE SUPPORT | A BORDO |

| | | |
|---|---|---|
| SIERRA LEONE | *in compilazione* | *in compilazione* |
| | *in compilazione* | *in compilazione* |

| | | |
|---|---|---|
| SUDAN | SALAM CENTER – KHARTOUM | *in compilazione* |
| | PORT SUDAN | *in compilazione* |
| | NYALA | *in compilazione* |
| UGANDA | ENTEBBE HOSPITAL | *in compilazione* |
| | OFFICE | *in compilazione* |

# Annex 3

# Case Profiling Template

RECIPIENTS:

INVESTIGATION TEAM' MEMBERS

COMPLIANCE MANAGER

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

# CASE PROFILING TEMPLATE - 2023

***TO SUPPORT INVESTIGATION AND RELATED COMMUNICATION***

- THIS FILE IS TO UTILIZE ONLY AMONG INVESTIGATION TEAM MEMBERS AND COMPLIANCE MANAGER OR AUTHORIZED ROLES AND TO SHARE ONLY VIA FOLDER AND LINK GENERATED IN THE COMPLAINT MANAGEMENT PLATFORM.
- IN INDETIFYING ALLEGATIONS PLEASE REFER TO THE MOST RECENT VERSION OF THE CONCERNED POLICY, LAWS OR CODE OF ETHICS/CONDUCT.

| | |
|---|---|
| **Case ID n°** | |
| **Date of receipt of the report:** | |
| **First receiver of the report:** | |
| **Involved personnel** | *Name:*<br>*Role:* |
| **Duty station of the reported person:** | |
| **Location of the reported facts (if known):** | |
| **Date of activation of Investigation Team:** | |
| **Allegations upon the original report:** | 1. [Allegation #1]<br>2. [Allegation #2]<br>3. [Allegation #3]<br>4. [Allegation #4] |
| **Deadline for investigation:** | |
| **Date of elaboration of Investigation Plan:** | |
| **Names and roles of the Investigation team members:** | |
| **Investigation Plan:** | |

| | |
|---|---|
| | <table><tr><th>Action</th><th>Explanation</th><th>Date for completion</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table> |
| **Brief description of the original content of the report together with background information** | |
| **Draft of questions to verify the relevant facts** | |
| **People to interview and reasons for interview** | <table><tr><th>Name</th><th>Type and aim of the interview</th><th>Date</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table> |
| **Update of information upon investigation progression** | |
| **Date of conclusive analysis by Investigation Team** | |

| | |
|---|---|
| **Date of elaboration of Investigation Final Report:** | |
| **People shared the Investigation Final Report and modalities of the sharing:** | |
| **Precautionary/Protective Measures to apply or to keep:** | |
| **Date of application of relevant measures:** | |

# Annex 4

# Informative Note on the use of work instruments

RECIPIENTS:

PERSONNEL

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

## 10 – COMPUTERS – EMAILS - INTERNET

The use of Internet and e-mails è is limited to work related tasks.
Please see the procedures contained in the protocol "**Security and internal regulation on privacy"**.

Personnel shall **use discreetly and strictly for work purposes** all the instruments that Emergency NGO makes available in order for personnel to carry out their work tasks, such as, for instance, computer (PC or laptop), phone, mobile phone, email accounts, etc.

The email accounts assigned to personnel are also grouped in several mailing lists (for example, Milano staff mailing list, etc.).

Creation of mailing lists was made with the aim of regulating and rationalizing the use of general mailing lists or group lists in order to discipline the volume of this internal communication on the Organization's IT infrastructure and the effective need to use this type of communication.

Sending out messages to these mailing lists is allowed only with the explicit authorization of the concerned manager.

# Annex 5

# Disclosure Notice on Data Protection

RECIPIENTS:

WHISTLEBLOWER, REPORTED PERSON, VICTIM, FACILITATOR

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

*UNDER ELABORATION*

# ANNEX 6

# Investigation Final Report

RECIPIENTS:

INVESTIGATION TEAM MEMBERS, COMPLIANCE MANAGER

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

# Investigation Final Report

| | |
|---|---|
| **General Information** | **Investigation Team Members:** |
| | **Date of investigation initializing:** |
| | **Instructions:** |
| | **Reasons for investigation:** |

| | |
|---|---|
| **Investigation procedure** | **The investigation procedure:** |
| | **People interviewed:** |

| | |
|---|---|
| | **Other source(s) of evidence:** |

| | |
|---|---|
| **Conclusions** | **Substantiated Facts** |
| | **Unsubstantiated Facts:** |
| | **Mitigation factors:** |
| | **Aggravating factors:** |
| | **Other relevant information:** |
| | **Precautionary/Protective Measures:** |
| | **Organizational weakness/shortfalls identified in the investigation on the incident and the related causes:** |

| | |
|---|---|
| **Descending measures** | **Suggested measures against the reported person(s):** |
| | **Recommendations to tackle the identified organizational shortfalls:** |
| | **Date:** |

| | |
|---|---|
| **Supporting documentation in the investigation procedure** | |

# Annex 7

# Sanctions System (MOG)

RECIPIENTS:

PERSONNEL, CONTRACTORS AND PARTNERS (AND THEIR PERSONNEL)

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

*MOG UPDATING ONGOING*

# ANNEX 8

# Internal Investigation Procedure

RECIPIENTS:

INVESTIGATION TEAM MEMBERS, WHISTLEBLOWER, VICTIM, REPORTED PERSON, COMMISSION FOR INVESTIGATION MEMBERS

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

## 1. Full Investigation Procedure

→ Investigation is the work of deepening into the conduct, act or omission **with the aim of:**

- ✓ verifying news/alerts on potential violations of laws, policies, procedures and internal regulations, in order to determine, and to prevent as far as possible, facts that could harm the public interest, personnel, individuals' rights or integrity of EMERGENCY and that could trigger legal consequences or reputational damage against the Organization;
- ✓ **deploying timely remedial** measures.

→ Usually, investigation display **through**:

- ✓ **What;**
- ✓ **Where;**
- ✓ **When;**
- ✓ **Who;**
- ✓ **How;**
- ✓ **Why.**

→ Investigation activities might **span throughout**:

- ✓ **Corporate intelligence**: e.g. available databases research and other open-access and public sources (for instance, social media);
- ✓ **Documentation analysis**: on relevant internal documents;
- ✓ **Forensic analysis**: work devices (such as pc, phone, tablet, laptop, servers etc.) assigned to the alleged person(s) to detect evidences of the allegations (hence, emails, documents, texts, etc.);
- ✓ **Key people interview:** Interviews to the Whistleblower(s), Testimonies, Informed people and Alleged Person(s), etc.

→ The ***investigation action plan***, contained in the **Case Profiling Template** (see Annex 3), will establish what measures are to undertake in order to investigate facts/acts/omissions, whom to involve and when. The action plan is updated as the investigation proceeds ahead, both for the actions and the timeline.

**!** **Preferably, hearings are video-recorded**, subsisting the explicit consent of the person to hear.

| HEARING/INTERVIEW – RULES | | |
|---|---|---|
| WHO/WHAT | RULE | RESPONSIBLE FUNCTION |
| → Whistleblower, victim, testimony, informed person and reported person | ✓ **summoning in writing** any time it is feasible, notwithstanding minimization of data, | CM or CRO |

| | | |
|---|---|---|
| | ✓ concurrent **request for consent on the video-recording.** The eventual consent shall be explicit and in writing.<br><br>***or***<br><br>***(when summoning is verbal):***<br><br>✓ pre-verify attitude of the summoned person to video-recording at the time of the verbal summoning.<br>✓ When starting the hearing ask for explicit consent and record it if released.<br><br>X when consent to video-recording is denied hearing cannot be video-recorded.<br><br>→ In case consent is limited to audio-recording – (**!** sole video-recording without audio is useless for the purpose of this procedure) – and **it combines with consent to disclose identity**, at the start of the hearing the concerned person will be asked to declare identity data while the Investigation Team members would specify date, time and place of the hearing.<br><br>✓ hearings shall happen in the order specified in the list here beside, on the left hand column | |
| reported person | X This person shall not be approached at all or come to know of any aspects of the allegation or investigation before the summoning by the Investigation Team to arrange the interview.<br><br>X During interview(s) with the alleged perpetrator, information related to the specific case and the reporter and or the survivor, the witness and informed people shall be limited to a delicate balance between allowing right to defense of the alleged perpetrator and avoiding any | CM, CRO and Investigation Team members |

unnecessary exposure/identification of the reporter/survivor.

→ Initial Notification to the alleged perpetrator shall contain the following information:

- ✓ the investigators are following up on a misconduct issue;
- ✓ the process is at the information-gathering stage;
- ✓ the investigators would like to talk to the alleged perpetrator as part of this information gathering process;
- ✓ the request on consent for audio-recording the hearing;
- ✓ the person is entitled to be accompanied by a colleague or a relevant (interpreter, lawyer, Union Representative, Staff Representative, etc.) third party who, in case, will need to sign off a Nondisclosure Agreement.

→ During the hearing (only after having gathered concurrent information on facts and eventually material evidences, in order to (a) give the alleged perpetrator as much information as possible to know the alleged facts and/or (b) collect evidence/indications/circumstantial evidence to corroborate/disprove the alleged facts during the interview):

- ✓ the alleged perpetrator should be informed on the type of allegation, but it shall not be disclosed the identity of the reporter or the victim nor details that would allow the identification of the witness(es)
- X none of the evidence, documentation or testimony gathered in the investigation should be showed to the alleged

| | | |
|---|---|---|
| | perpetrator or any other interviewees as the investigators are simply trying to establish the facts.<br>✓ The alleged perpetrator has to right to remain silent in this hearing. | |
| Whistleblower and/or victim | → IF allegations are mainly based on declarations of the Whistleblower(s) and/victim, then<br>✓ the CM or the CRO should request in a motivated manner the release of explicit, free and specific consent by these people, to use the contents of their declarations.<br>X if consent is denied, and investigation is only based on these declarations, then the procedure is to close with the formula of *lack of evidence*, as the only available information cannot be used in the proceeding.<br><br>→ IF investigation process allowed the collection of evidences additional to the initial declarations of the Whistleblower(s) and/or of the victim, then:<br>X disclosing the very specific contents of the Whistleblower(s) and/or of the victim is not necessary to carry out the hearing of the alleged person;<br>✓ pursuant to the confidentiality principle and the protection due to Whistleblower(s) and associates, specific contents of the Whistleblower(s) or the one of the victim shall be kept secret, in this case. | CM or CRO |

→ ***Case profiling template*** also requires defining the **questions at the core of the allegation(s)** for the specific case under management, in order to address the efforts in investigation and the findings.

**!** Any collected evidence, **either in charge or discharge** of the allegation(s), shall be tracked and stored in the investigation dossier.

→ The **investigation dossier** is set up, populated and stored by the Compliance Manager on the Complaint Management Platform and in a dedicated folder with access limited to the Compliance Manager. This is to guarantee integrity of the information collected and received throughout.

**! PSEAH-related allegations** are investigated on the basis of this general procedure together with **the additional protocol on "Guidelines on Handling SEA-related Allegations"** (Annex 9).

## 2. Source of evidence

Source of evidence might be:

- **material** (things, documents, records, audio/video footage, etc.);
- **people** (testimonies).

Source of evidence can allow inference of circumstances, facts, behaviours, conducts.

**!** This part of the investigation phase poses a **number of rusty interactions with other laws**, especially labor law, criminal proceeding law and data protection.

Data protection law, specifically, in combination with labour law, restrains the abilities of the Employer to look into the devices and instruments assigned to the staff member(s), pursuing the prohibition to investigate and question the staff' opinions (political, social, religious, etc.) and the one of constant surveillance on performing job duties.

→ **Detection of evidences** on work devices can deploy **only if:**
  ✓ the staff member(s) ordinarily uses those work devices/apps and accounts to carry out job duties (which qualifies them as instruments for ordinary carry-out of job performance), and

the personnel is informed preemptively on related Data Protection traits implied in the use of work devices, apps, documentation, etc. (see Annex 4).

**!** In each and every case, investigation conducted onto work devices **shall avoid look into personal** software and hardware, apps, accounts, information, documentation etc., that might co-exist with the work apps and instruments into the work device, especially when internal regulations on the use of work devices are absent or do not explicitly prohibit this combination or promiscuous use between personal and work related.

Deploying internal regulations on the use of work devices in these terms, especially ruling Data Protection and access of the Employer to those devices, is crucial to allow adequate and legitimate extraction and use source of evidences out of work device (see Annex 4).

! In fact, under Data Protection law, **consent of the alleged person to access work devices and instruments cannot afford the legitimate use**.

→ **Legitimate interest** of the Employer, in order to protect the integrity of the Organization, or public interest where it is the case, **may justify access** to work devices, apps and documents **after the upraising of the suspicion** having been the staff priory informed on the use of those work devices, apps and documentation and the circumstances that would allow the Employer to access them (see Annex 4).

**Personnel within the organization, who is allowed to access** and apprehend those information/sources of evidence, is (under ART 29 GDPR) a) **formally authorized**; b) **received clear instructions** to operate together with confidentiality clause; c) is **properly trained**.

* External consultants, eventually engaged to run the investigation, shall (under Art. 28 GDPR) a) be **evaluated for their ability** to uphold GDPR's requirements; b) **formally nominated** as Data Controller/Data Processor; c) **receive clear instructions** on operational procedure to follow and how to abide by confidentiality throughout.

## 3. Conclusions on investigation

→ Investigation shall be **duly documented throughout** by **the Investigation Team** and, without prejudice of the possibility to report the case to the local authority, it can lead to:

| CONCLUSIONS | |
|---|---|
| FORMULA | RULE |
| **closure of the case for *no case to answer*** | in-depth investigation has achieved review for that the alleged conduct(s), act(s), omission(s) does not breach any law, policy, procedure relevant to Whistleblowing policy. |
| **closure of the case for lack of evidence** | investigation did not achieve sufficient evidences to sustain a disciplinary proceeding; |
| **closure of the case for alleged person(s)'innocence** | the investigation found evidence of the innocence of the alleged person(s); |
| ***to carry over to disciplinary proceeding*** | investigation has found evidences that can support sanctioning; |

| |
|---|
| **a combination of the ones above.** |

**Conclusions:**

- → shall be in writing and duly motivated (see Annex 6);
- → shall elaborate a technical ultimate (set of) allegation(s) based on the collected information;

✓ can identify alleged person(s) different or additional to the original one(s);

✓ can identify further incidents happened along the reported case and set up allegation(s) for this additional part against the originally alleged person(s) and/or to further one(s) without the need to open a new case;

✓ can determine if and what improvement is required to the Organization in order to prevent, detect and tackle similar conducts in the future, and any further recommendations, accordingly;

- → if carry-over to disciplinary proceeding is established, shall indicate the applicable (range of) sanctions for the type of allegation(s) upon the sanctioning system established within the Organization, and the criteria to use in order to graduate the sanction to the specific circumstances pertaining the case.

# ANNEX 9

# Guidelines on Handling Allegations of Sexual Exploitation, Abuse and Harassment

EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

# *Protocol*

# *Guidelines on Handling Allegations of Sexual Exploitation, Abuse and Harassment*

# *(2023)*

## INTRODUCTION

These guidelines are issued to support investigators when having to deal with allegations of Sexual Exploitation, Abuse and/or Harassment (SEAH).

These guidelines are meant to ensure that a comprehensive and objective investigation of a SEAH-related incident (or number of incidents) is carried out, and that the members of the *Investigation Team*(s) dealing with SEAH-related incidents or concerns will be able to display the most appropriate professional conduct.

An internal investigation is not a legal proceeding, and **it does not have "to prove beyond all reasonable doubt" that an allegation is true or false.**

Instead, an internal investigation in SEAH, must gather as many evidences as possible surrounding an allegation for the entitled *Commission for Investigation at Main Office* to come to a 'reasonable conclusion' (for withdrawal of the case or for disciplinary proceeding, whether with the additional reporting to relevant authorities for criminal offence or not).

**The collection of evidences is not the reporter's responsibility.**

**Evidence might be either in charge or discharge of the alleged person** ("alleged perpetrator", hereinafter).

**! In principle, the victim of the sexual misconduct** ("survivor" hereinafter) **is considered and treated as SEAH survivor since the knowledge of the incident, regardless of the evolvements of the investigation and its findings, except for the case of grounded malicious reporting.**

When the report deals with SEAH acts and conducts, these guidelines shall complement the intake of incident and the rolling out of the full investigation as per the related procedures in the *Complaint Reporting Mechanism* Policy.

## SCOPE

This Protocol is applicable to all allegations/concerns of sexual exploitation, abuse and/or harassment (SEAH) which is brought against EMERGENCY's or its partners' and (sub)grantees' Personnel, regardless of the country of operations.

These guidelines should be provided to the line, senior, top manager(s) and members of the governance, that are likely to be informed on the incident or managing an investigation on receipt of an allegation of SEAH.

## PRINCIPLES

The following are the principles informing the entry of the report, the *relevance* review and the investigation procedures on SEAH-related report:

→ **HIGH CONFIDENTIALITY:**

EMERGENCY believes in upholding the safety and dignity of all those who come into contact with the Organisation.

**!** If allegations of sexual misconduct (and/or similar) are made known to one of more individual(s) working at EMERGENCY, **the receiver(s) shall promptly report the allegation/concern to the Compliance Manager at Main Office and/or, when relevant** (i.e. national staff, place of misconduct, whereabouts of the survivor/reporter) **to the concerned Complaint Reporting Officer(s) at Field Level** , and treat the information in a highly confidential manner.

"Highly confidential" means that the information will only be passed on to another person, if the latter ***needs to know it*, being the authorized person (i.e. *formally assigned a role in compliance and integrity*) or, further to the latter,** for the sole purposes of:

- protecting someone's human rights from immediate and actual danger;
- urgent tackling of the exposure of the survivor or the prospective survivor(s) to the alleged perpetrator or urgent mitigation of the repercussions of the incident.

Information will be passed further than what provided above, when explicit and informed permission of the complainant/reporter is present, together with the prior clearance by the Compliance Manager.

**Failure in respecting the confidentiality of others is a serious breach** of Whistleblowing and Privacy requirements and it will result in immediate disciplinary response.

→ **ACCOUNTABILITY:**

Experience showed us that in many contexts in which we work it is unlikely that we will hear important complaints unless we actively promote the fact that we welcome them.

**! Assigned managers in different parts of the Organisation are responsible for ensuring that an adequate implementation of the Whistleblowing and Complaint Reporting Mechanism is in place** as per the relevant Policies at EMERGENCY.

In fact, an adequate CRM system ensures that complaints are solicited, heard, recorded, analysed, acted upon and an adequate response is given to the reporter(s). And ideally, sourcing out the learning for the entire organisation and for the sake of beneficiaries.

**! Personnel must always take complaints or allegations on sexual exploitation, abuse or sexual harassment very seriously.**

"Very seriously" means that report is immediately in-taken, without any comment on its nature and content by the staff receiving it and duly referred to the authorized function (compliance) in the Organization.

Managers are responsible for explaining the expectations of the Organisation in these terms and align with the indications above and below. Staff and managers are equally responsible for upholding them. Not doing so represents a breach of the PSEAH Policy and therefore it constitutes a disciplinary offence.

→ **PROPORTIONALITY:**

! **Breach of SEAH is always to consider as a gross misconduct**, regardless of it is attempted, threatened or committed, thus it shall be treated and sanctioned accordingly.

In fact, **SEAH** is a misconduct **harming human and personal dignity as well as security,** with predictably **permanent effects on the survivor and the associated people,** with the potential of **disrupting the trust in the humanitarian actors** and consequently putting **at risk humanitarians in the context,** thus **eventually preventing those in need from being provided an essential response. The cascade of effects from a SEAH incident is extensive and often, unpredictable.**

→ **HUMANITY (HUMANITARIAN PRINCIPLE) and SAFETY:**

! **SEAH act immediately offends human dignity,** in each and every case.

Therefore, the modalities for investigating SEAH-related reports shall strictly factor into ***the victim-centred approach.*** Investigating a sexual misconduct can trigger or increase risks to the security of the survivor, the reporter, the investigators, the fellow humanitarians.

! **A risk assessment exercise shall always precede and inform the investigation plan.**

! **Interview to the survivor is potentially trauma reliving. Survivor must be respected in these terms and investigators shall be well-prepared for this interview in order to avoid recurrent solicitation of the survivor.**

→ **RESPONSIVENESS AND TIMELINESS**:

reports are taken seriously and handled swiftly. Notification of **receipt to reporter** is within **24 hours** from the knowledge of the incident/report. **Investigation** on the incident is to run quickly and, as far as possible, **within 14 days**, from the knowledge of the incident/report unless circumstances impose a different timing, which is to motivate duly in the *Case Profiling Template* and to the reporter.

## PROCEDURES

### Entry points of signals, warnings and "incidents"

Complaints and concerns might come frequently to any staff member in many ways. Beside the provided channels in *Complaint Reporting Mechanism*, reports/complaints might come from any internal and external sources.

**!** Internal complaints **are to enter via the set channels of the *Complaint Reporting Mechanism*, even when initially filed to non-dedicated function/role**.

→ **Staff, out of the dedicated function,** who receives SEAH-related complaints/reports or who happens to see (witness) or hear (informed person) of SEAH-related incident, is required **to report promptly to the dedicated function** (Compliance Manager and/or Complaint Reporting Officers).

In this transfer, if the survivor or the reporter does not consent to be known to the dedicated function or to participate further into the investigation that is to launch, the witness or the informed personnel shall still:
1 refer promptly the incident to the dedicated function omitting the identity of (or details from which the identity can be inferred) the survivor/reporter, and
2. specify that survivor/reporter does not consent for the identity to be known nor to be involved in the investigation.

External complaints could come from any source at any time in all modalities. Either way, it is important that there is a swift, written, trackable version of the complaint/report in the intake process.

The complainant/reporter can submit the complaint in writing with the support of anyone else of trust.

Should the complainant need it, EMERGENCY will provide support for putting in writing the complaint/report in Complaint Reporting Form or in an email text to the relevant function (complaintreporting.*country*@emergency.it or complaintreporting@emergency.it) .

### Evaluating Report

Once an allegation/report/concern of sexual exploitation, abuse and/or harassment is known to the Compliance dedicated personnel at Main Office and/or Field Level, as per the indications contained in *Complaint Reporting Mechanism*, the involved function level must decide what to do within 24 hours.

→ There are three likely options:

i. Urgent need to investigate;
ii. Need for further information before launching an investigation on SEAH-related matter;

iii. Collate into ongoing investigation on the same incident or on what it seems a pattern of behaviour by the same alleged person(s) - number of incidents.

**!** Investigation is **the immediate procedure to follow,** without any further delay, when the following criteria are met:

- ✓ The allegation is clearly a breach of the PSEAH Policy;
- ✓ The report is readable and understandable;
- ✓ There are already enough information in the report on whose basis is possible to launch and conduct a full investigation phase (or collate to an open one).

It is unlikely that all the above is met the first time an allegation of SEAH is heard or reported, though. It is likely that the Compliance function will need to carry out initial review on the incident and send out a request for integration(s) or make an initial research in order to clarify whether the incident falls under PSEAH or another Policy.

**! The initial review and collection of integrations must not breach anybody's privacy and those who knows about the report must not confront the subject of the complaint at this stage**.

→ In addition, all Personnel at EMERGENCY and/or those in Compliance function handling SEAH-related allegations shall be aware of the followings:

a) Complaints or allegations may come unofficially to EMERGENCY. It could be that there is a **persistent rumour or concurrent hints coming to our attention**. Persistent rumours or signs/hints **shall be pursued directly by EMERGENCY in case of SEAH,** without waiting for an explicit report/complaint on that(those) incident(s).

b) **Once a complaint has come to our notice then it becomes 'ours'** as it **does the responsibility** to **look into it,** regardless of the intention of the survivor or of the reporter – so **please, disclose this to the victim/survivor or reporter at the very outset!** The investigation, conclusions and disciplinary proceeding (if any) shall respect survivor/reporter denial of consent, though.

c) There **does not necessarily need to be** a 'victim'/'survivor', a 'complainant' or 'witnesses'.

d) **We investigate 'incidents', not people,** so those concerned by an allegation do not necessarily <u>have to still or already be</u> at EMERGENCY at the time of the investigation, for EMERGENCY to run the investigation on SEAH-related misconduct.

e) **An investigation is used to gather evidence on facts** about an incident (or a series of incidents) and **not about a person, <u>even when it deals with a pattern of behaviour</u>.**

→ **Once ready to investigate** the incident as SEAH-related, the Compliance Manager informs the *Complaint Committee* within the limits of data minimization principle.

**X Unless decisive** for establishing the composition of the *Investigation Team* (e.g. neutrality, conflict of interest, special needs etc.) **details on identities** (when known) of the reporter(s) and the survivor(s) **or any detail from which the identities may be inferred** directly or indirectly) **shall not be shared** nor such information will go in the alleged perpetrator(s)'s file(s) until the investigation is completed.

→ *The Complaint Committee*, evaluates with the Compliance Manager **the imminent risks** (if likely), eventually sets protective measures and summons *the Investigation Team*, which is subsequently shared the *Case Profiling Template* by the Compliance Manager. The Case Profiling Template for the Investigation Team may contain also identity data of the reporter(s) and the survivor(s), **when relevant and consented to** (alleged perpetrator identity, where known, is inevitably shared), in order to inform the investigation pattern.

! **When contractual obligations with funding donor(s) establish it,** the Compliance Manager will notify the concerned donor(s) on the receipt of a SEAH-related incident report and the procedure that EMERGENCY will follow to investigate it and the eventual precautionary or protective measures applied upon the risk assessment exercise. No details on the specific whereabouts, the survivor, the reporter, the alleged perpetrator or the mentioned people are due in this notification.

! A Reminder: local legislation must be taken into account but **standard advice** to the investigators is that the **alleged perpetrator should not be approached or informed of any aspect of the allegation or investigation, until all the other evidences are collected and the alleged perpetrator(s) is asked for a formal interview at the end of the investigation phase**.

## Commissioning the Internal Investigation

Team for investigation is then quickly set as per *Internal Investigation Procedure*.

*Investigation Team*'s composition for SEAH-related allegations shall uphold the following standards:

1. per the standard at EMERGENCY, the Investigation Team is in odd numbers and pre-established in composition. For SEAH-related case, one of the three permanent members will take the role of lead investigator and the others are co-investigators.
2. **Investigation Team shall be formed considering high confidentiality (best composition is maximum 3 people) on the "need to know" basis and possibly ensuring the support of a PSS Specialist or a member competent in PSS.**
3. For SEAH-related case to investigate, the members are **necessarily from outside the program/project/department of pertinence where the allegation emerged** and with **no direct line management role on the alleged perpetrator and/or the survivor**. Thus, in case one or more of the fixed members of the Investigation Team would be incompatible with this requirement (3), the concerned member(s) shall be excluded since the beginning by the Compliance Manager with formal notification to the *Complaint Committee* and the excluded member(s) will be substituted with a competent one among those listed in the procedure as eventual/additional members for the *Commission for Investigation at Main Office*.

The *Investigation Team* can be assisted by experts and focal points on specific matters involved in the incident. In this case, the summoned expert/focal point will need to sign off the *Nondisclosure Agreement with No-conflict of interest clause*.

## Protecting Those Involved in investigations

EMERGENCY PSEAH Policy states that survivor(s) will be **offered immediate support as necessary, that is in line with the wishes and needs of the survivor(s)** and to levels that are appropriate locally (and in any case to a level deemed acceptable by professional staff).

Thus, risk assessment exercise is required to happen swiftly after the receipt of the report and identify risks for the survivor(s), for the reporter(s), for the facilitators, for the alleged perpetrator(s), for the investigators and for the fellow colleague(s) and organization as a whole.

**Identified risks, from victim shaming through honour crime, documented in *the Case Profiling Template*, shall also inform** the modalities of the investigation.

EMERGENCY must and will move survivors, reporters, witnesses or alleged perpetrators to safer locations, if resulting necessary by the risk assessment exercise and if viable upon the context and concerned person's will.

EMERGENCY will always offer PSS support (and/or legal) to the survivor(s), who might consent or not to it. Managers with assigned role in Complaint Reporting on the Field are strongly recommended to map existing GBV and PSS services locally available in order to make a swift referral of the survivor(s) or associates at the aftermath of the entry of a SEAH-related report.

Maintaining high confidentiality is the best way to protect people involved and EMERGENCY requires that this is respected by all those involved.

Reporter/Survivor are always offered the chance to be assisted during the investigation procedure by an entrusted person of their own. When involved, this person will need to sign off the *Nondisclosure Agreement*.

The alleged perpetrator(s) can be suspended from work, temporarily re-assigned or imposed compulsory leave if there is a risk to anyone by their continuing to be at work (pursuant the applicable labour laws). Such precautionary measures will be decided by *the Complaint Committee* and communicated to the relevant manager(s) of the alleged perpetrator by the Compliance Manager, simply motivated by "precaution". Managers eventually reached for such measures to apply are required to fully cooperate and not to investigate further onto the reasons.

In case the alleged perpetrator(s) is later found innocent, eventual compulsory leave days imposed will be compensated back to the person, if applicable.

**EMERGENCY reassures that any complainant/reporter in good faith is protected against retaliation** as it is provided in Whistleblowing Policy.

Where professional advice is sought, confidentiality on identities of persons involved or mentioned in the allegation and in the investigation, must be always respected, which means that direct and indirect information on personal data are to omit.

## Distribution of tasks and responsibilities

**Lead Investigator**: generally, the most senior member of the *Investigation Team* either in working experience or specific knowledge on SEAH; is responsible for decision-making, follow-up and confidential reporting.

**Investigation Team**:
The team will comprise:
(1) Lead Investigator who focuses on asking questions,
(1) 2 Co-Investigators.

Within 2 days from the appointment, the lead investigator must provide the *Investigation Team* with a proposal of **investigation plan**, contained in the *Case Profile Template*.

The *investigation plan* needs to include*:*

- Details of the report, including background information;
- All steps of the investigation procedure, including mission trips, notifications, summoning, production of MoMs and approval of, etc. with brief explanation of comments;
- Suggested names of people to be interviewed and reasons for interviewing them;
- Draft of questions on core constituting aspects/facts to clarify;
- Timeline for completing the investigation;

The *Investigation Team* will collectively review the investigation plan, make amendments as necessary and approve it (date on the *Case Profile Template* will be the one of the approval).

If any of the members of the *Investigation Team* has any previous direct knowledge of the incident or having direct relationship other than professional with the people to interview, the other investigators shall be informed from the beginning, in order to evaluate potential conflict of interest at the right time.

## Principles for Investigations on SEAH allegation(s)

There are six (6) principles guiding the carry-out of the investigation:

i. Confidentiality of all parties;
ii. Investigate the allegation/incident and **strive for collecting material evidences or concurring clues** on the facts (conduct included), not on the individual attitude and thoughts;
iii. Burden of proof is not on the survivor nor on the reporter;
iv. Presumption of innocence for the alleged perpetrator;
v. The investigator is not the decision-maker on the final weight of the findings;
vi. The investigator does not make moral judgements relating to any of the parties to the allegation.

**Timing:** Timescale for this kind of allegations is tight (max 10 days from the launch of the investigation) for all concerned parties and this must be accommodated. Nevertheless, the need for speed does not take precedence over the need for a thorough and careful investigation. If the investigators find that they need more time, this should be discussed with the reporter/survivor where known, duly motivated, included in *the investigation plan* and notified to the reporter/survivor (where known).
In terms of availability, investigators are expected to free themselves from other responsibilities as much as possible, in order to take on this duty.

The reporter/survivor shall be promptly informed of any unforeseen delays that occur during the investigation.

If a complainant or a victim/survivor withdraws a SEAH-related allegation, EMERGENCY will continue to investigate the allegation, leaving the complainant/survivor aside.
In fact, EMERGENCY holds an obligation to investigate the allegations against its personnel beyond the will of the reporter/survivor to participate in this procedure.

## Conducting Interviews

Investigation Team and the *Case Profile Template* must stipulate that interviews should be conducted in the following order:

1. Survivor/(2.)Reporter (if one/each consents to be part of the investigation);
2. Witness(es) with direct knowledge about the alleged misconduct;
3. Informed people with potential direct knowledge on a pattern or (parts of) the facts;
4. Alleged perpetrator;
5. People with indirect knowledge of alleged misconduct can be summoned and interviewed if, and only if a thorough investigation requires it and in case, duly motivated in the dedicated slot of the interviews grid in *Case Profiling Template*.

**Pursuant *the victim-centred approach* and the HUMANITY and SAFETY principles, interview to the survivor(s) is considered trauma re-living. Survivor(s) must be respected in these terms and investigators shall be well-prepared for this interview in order to avoid repetitive solicitation of the survivor(s).**

**Preferably, interviews are audio-recorded if the interviewee explicitly consents to it. Guidelines contained in *Internal Investigation Procedure* (Whistleblowing and CRM Policy) shall be followed for this option.**

The alleged perpetrator(s) shall not be approached or come to know of the investigation before the investigators reach out to this concerned party in order to arrange the related interview.

Alleged perpetrator(s) shall only be contacted when the investigators have completed all other interviews in the list above and the evidence gathering.

Whenever possible, contact the alleged perpetrator(s) in writing and keep copy of the notice of the meeting in the incident case file.

During interview(s) with the alleged perpetrator, information related to the specific case and the reporter(s)/survivor(s) shall be limited to a delicate balance between allowing right to defence of the alleged perpetrator(s) and avoiding any exposure/identification of the reporter(s)/survivor(s).

The **notification** to the alleged perpetrator shall outline that:

- the investigators are following up on a misconduct issue involving the alleged perpetrator's responsibility;
- the process is at the information-gathering stage;
- the investigators would like to talk to the alleged perpetrator as part of this information gathering process;
- the interview is preferably audio-recorded and explicit consent or denial is requested in writing;
- the subject is entitled to be accompanied by a colleague or a relevant (interpreter, lawyer, Union Representative, Staff Representative, etc.) third party who, in case, will need to sign off a *Nondisclosure Agreement* before the interview.

During the interview, the alleged perpetrator(s) should be informed on the type of allegation, but it shall not be disclosed the identity of the reporter(s) nor details that would allow the identification of the survivor(s). Here it is where it comes that having gathered concurrent information on facts and eventually material evidences is decisive to conduct this interview properly.

At this stage and for these cases, none of the evidences, documentation or testimonies gathered in the investigation should be showed to the alleged perpetrator(s) and/or to any of the other interviewees as the investigators are not carrying out a disciplinary hearing and assigning liabilities – they are simply trying to establish the occurred facts.

## Recording Statements and other evidence

If consent to audiovisual-record is denied, the Co-Investigators should take full notes of the interview, detailing dates, names, places, what is actually said about what was heard and seen etc – i.e. Minutes of Meeting. After this has been done, the Minutes shall be closed and saved with a password if in soft copy, and they should be shown/sent to the concerned interviewee(s). The concerned interviewee is asked to make any appropriate amendments and then, sign off, date the Minutes as *the interviewee's true version of events* and return it to the Lead Investigator, enclosed with password. If the interviewee is illiterate, the investigators should read the Minutes to them and get their approval of. It might not be appropriate to gain a signature in this case.

Either for Minutes of Meeting or for audio-visual records, the Compliance Manager shall store an electronic version saved with a password and named in such a way to avoid identification of persons involved and the topic of the incident. A case-code was already assigned by the Compliance Manager at the entry of the report/compliant and it must be maintained throughout when referring to the case.

Within the limits of domestic laws, the records are kept in the case file following the retention rules for the Final Report on Investigation below.

Access to records is limited to Investigation Team members.

Eventual material evidences (screenshots, vocal messages, audio-visual records of any kind, letters, documents, emails etc.) collected in the course of the investigation shall be kept only if relevant to the incident and, in the latter case, password protected.

## Final Report writing, retention and recommendations

The purpose of the Final Report on Investigation is to inform the decision-making of the *Commission for Investigation at Main Office* on the appropriate course of action.

Report shall be closed with a password and named in such a way so to avoid identification of involved parties and topic(s). Use the case code provided by the Compliance Manager at the intake of the case.

The report must contain:

- An executive summary outlining:
- The original complaint topic and date
- The specification whether the alleged perpetrator is known or unknown;
- The profile of the complaint made – without personal identifying details of the reporter and/or of the survivor;
- The members of the *Investigation Team* and any modification that has modified the composition thereof, providing details on the reasons are omitted, as details could allow inference of identities;
- The date of inception of the *Investigation Team* and any event that has influenced on the timing thereof;
- Body of the report:
- Methodology used for the investigation and interviews (no personal data details – use labels such as "interviewee 1, interviewee 2, survivor, alleged perpetrator..)
- Investigation findings – grounded facts/behaviour
- Analysis of the findings against CoC, relevant Policy and Internal Regulations
- Conclusions and recommendations:

for instance (and without limitation):

- The allegation(s) appears to have substance and a disciplinary proceeding against alleged perpetrator is to hold swiftly;
- The allegation appears to have some substance but is not completely covered. Some elements of the allegations may be taken ahead to disciplinary proceeding, while other elements are not (and the related specifics);
- The investigation team was unable to find enough evidences and/or decide as to whether the allegation is substantiated. Commission members to act accordingly and consistently with the context;
- The allegation appears to lack substance, it is not substantiated as SEAH and no further disciplinary action should be taken in these terms;

- The allegation is fabricated and reporter/survivor shall be heard in disciplinary proceeding for malicious reporting.

Regardless of the outcome of the investigation there is always need for four essential actions:
- Managerial Action to deal with any negative fallouts from the investigation (eg damage to a staff member's reputation due to a false allegation);
- Identification of internal learning on the weaknesses and failures which might have caused, eased or allowed the incident or the cover thereof;
- Notification to the reporter/survivor (if not found malicious/frivolous) and to the alleged person (if interviewed);
- Notification to donor on the outcomes of the procedure, where relevant.

## Report Sharing

Follow the procedures set in the general investigation procedure at paragraph 5 of the Whistleblowing Policy.

## Report retention.

| RETENTION RULES | | |
|---|---|---|
| CASE | RULE | RESPONSIBLE |
| allegation is partially or fully upheld | full report should be kept for 5 years in the subject of complaint's file, alongside all details of the undertaken disciplinary action | HR DEPT |
| allegation is found to lack evidence and decision on the substance of the incident was not possible | one copy is stored confidentially for 3 years (for reference in the future should there be doubt over the quality of the investigation or decision-making) and one copy kept on the subject of complaint's file. | COMPLIANCE MANAGER<br>AND<br>HR DEPT. |
| allegation is dropped as not substantiated | the report is definitively cancelled after 1 year from the intake of the incident | COMPLIANCE MANAGER |
| allegation is found fabricated | the Investigation Final Report, once cleaned from irrelevant information and related personal | COMPLIANCE MANAGER |

| | | |
|---|---|---|
| | data, forms part of the evidences against the malicious reporter/survivor and will follow the procedural timing provided for the new incident (i.e malicious reporting). | |