



WHISTLEBLOWING POLICY E MECCANISMO DI SEGNALAZIONE

Approvata il 24 ottobre 2023

Valida dal 17 dicembre 2023





Whistleblowing Policy e Meccanismo di Segnalazione

Sommario

1. FINALITA'	pg. 4
2. AMBITO DI APPLICAZIONE ED INTERAZIONE CON ALTRI REGOLAMENTI INTERNI	pg. 5
3. PRINCIPI E DEFINIZIONI	pg. 8
4. FARE UNA SEGNALEZIONE – MECCANISMO DI SEGNALEZIONE (CRM)	pg. 14
4.1 Canali	pg. 16
4.2 Ruoli chiave e Responsabilità connesse	pg. 18
4.3 Accessibilità	pg. 19
4.4 Riservatezza	pg. 21
4.5 Comunicazioni/Notifiche	pg. 22
4.6 Profilazione della segnalazione (rilevanza)	pg. 24
4.7 Misure Protettive e Misure Precauzionali	pg. 25
4.8 Conclusioni della fase di profilazione della segnalazione – Notifiche e Reportistica	pg. 27
4.9 Tracciamento e Conservazione	
5. INDAGINE INTERNA	pg. 28
5.1 Organi della procedura di indagine	pg. 28
5.2 Ruoli chiave e Responsabilità connesse	pg. 30
5.3 Misure Protettive e Misure Precauzionali	pg. 31
5.4 Notifiche	pg. 31
5.5 Conservazione	pg. 33
6. PROCEDIMENTO DISCIPLINARE (SANZIONI)	pg. 33
6.1 Misure conseguenti	pg. 34
6.2 Notifiche	pg. 35
6.3 Conservazione	pg. 35
7. FORMAZIONE E DISSEMINAZIONE	pg. 36
8. MONITORAGGIO E APPRENDIMENTO	pg. 38
Allegati:	pg. 39
Appendice 1 - Scheda numeri hotline	pg. 39
Appendice 2 - Collocazione Complaint Box	pg. 41
Appendice 3 - Modulo di Profilazione del caso	pg. 45
Appendice 4 - Nota informativa sull'uso della strumentazione di lavoro	pg. 49
Appendice 5 - Informativa sulla riservatezza	pg. 51
Appendice 6 – Modulo di Report Finale di Indagine	pg. 53
Appendice 7- Sistema di sanzioni (MOG)	pg. 57
Appendice 8 – Procedura di Indagine	pg. 59
Appendice 9 - Procedura di gestione delle indagini per segnalazioni di SEAH	pg. 67



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 3 di 80

Versione: 1	Revisione					
	0	1	2	3	4	5
Data	30.06.2020	24.10.2023				
Elaborata da	FOD e Amministrazione	Compliance Manager				
Verificata da	Grants	A. Bertani RR.SS.				
Approvata da	Comitato Esecutivo	Comitato Esecutivo				

1 FINALITA'

EMERGENCY ONG ONLUS (di seguito "**EMERGENCY**" o l'"**Associazione**") intende promuovere una cultura organizzativa basata su un comportamento responsabile, consapevole e rispettoso, costruendo le sue pratiche sull'approccio basato sui diritti umani (*human rights based approach*) e sull'attiva prevenzione e correzione di azioni, condotte ed omissioni interne scorrette e/o illecite, poiché le irregolarità di questo tipo influenzano direttamente ed in modo negativo la possibilità di realizzare il nostro mandato e, in ultima istanza, si riversano sulle popolazioni colpite.

A tal riguardo, EMERGENCY **riconosce** il **ruolo cruciale** che tutti i propri portatori d'interesse, interni od esterni, svolgono nel sostenere EMERGENCY nel perseguimento delle sue ambizioni di **integrità, legalità e trasparenza** e, in generale, **dell'adesione agli standard etici, legali e procedurali** che sovrintendono il proprio agire.

In conformità a quanto previsto dall'art. 4, c. 1, D.Lgs. 24/2023, la presente policy "**WHISTLEBLOWING POLICY e Meccanismo di Segnalazione**" (nel seguito, la "**Policy Whistleblowing**") e i canali di segnalazione dell'Associazione di seguito indicati, sono stati adottati anche con un attento confronto con le rappresentanze sindacali di cui all'articolo 51 del D.Lgs. n. 81 del 2015, che hanno espresso il loro parere favorevole al riguardo.

EMERGENCY è fermamente impegnata a **garantire la possibilità di segnalare, in sicurezza e senza temere alcuna ripercussione, qualsiasi condotta scorretta, illecita o in violazione dell'etica di settore, che venga messa in atto dal personale di EMERGENCY o dei suoi partner, fornitori e consulenti**, perseguendo così il criterio 5 espresso negli impegni (9) della *CHS Alliance*: "*le segnalazioni sono benvenute e prese in carico*".

Questa Policy ha dunque il fine di assicurare ad eventuali segnalanti che riportare sospetti di violazione attraverso i canali individuati dall'Associazione è **un'azione benvenuta, sicura e meritevole**.

Le segnalazioni infatti consentono ad EMERGENCY di predisporre un ambiente di lavoro e di servizio sicuro, dignitoso e positivo, sia per le comunità servite che per il personale e soci. Le segnalazioni dunque, consentono di perseguire **una piena integrità e la continuità** dell'azione, **restando coerenti con i diritti umani, il proprio mandato, la propria base costitutiva ed i propri portatori di interesse**.

La Policy Whistleblowing intende quindi **incoraggiare** il personale tutto e i membri delle popolazioni assistite in particolare, a segnalare, **in modo precoce ed appropriato**, qualsiasi preoccupazione in questi termini.

Lo scopo del **Meccanismo di Segnalazione** ("CRM") (di cui al paragrafo 4 nel seguito) è quello di assicurare che ad EMERGENCY **esista, e sia facilmente accessibile e conoscibile, un processo appropriato, un meccanismo equo, spedito e discreto** per l'emersione, l'indagine e la risposta a questo tipo di questioni, che promuova l'accountability *"in modo tale che le comunità e il personale siano in grado di riportare abusi e accedere a un maggior grado di protezione attraverso la deterrenza"*¹.

La presente Policy Whistleblowing è qui riformata in conformità alle specifiche prescrizioni introdotte dal Decreto Legislativo n. 24/2023 sul Whistleblowing (anche alla luce delle linee guida ANAC approvate con Decisione n. 311 del 12 luglio 2023) ed è chiaramente indicata nel, e coordinata con, il Modello di Gestione Organizzazione e Controllo di EMERGENCY adottato ai sensi del D.Lgs. n. 231/2001, che a sua volta stabilisce le sanzioni applicabili per la sua violazione.

Questa policy dovrà essere rivista periodicamente, almeno ogni due anni dalla sua emissione, ed in ogni caso prontamente quando:

- siano avvenute significative modifiche della struttura o delle operazioni che influenzino le procedure, i ruoli e le responsabilità inerenti a questa policy;
- siano avvenute significative modifiche dell'ambiente (contesto) di azione di EMERGENCY, tali da influenzare le procedure, i ruoli e le responsabilità inerenti a questa policy;
- siano intervenute pertinenti modifiche legislative.

2 AMBITO DI APPLICAZIONE ED INTERAZIONI CON ALTRI REGOLAMENTI INTERNI

Questa policy è azionabile da:

- Il **Personale** (indipendentemente se remunerato o meno, se temporaneo, giornaliero o permanente, se dipendente o meno, se attuale, precedente o futuro) i membri della *governance* ed i soci (da qui in poi definito anche come "**Personale**"),
- i **membri delle comunità** che beneficiano degli interventi e dei servizi di EMERGENCY,
- i **partner, i fornitori e consulenti** di EMERGENCY ed il **loro personale**,
- **qualsiasi terza parte** cui accada di venire a conoscere della condotta scorretta/illecita del personale di EMERGENCY dei suoi partner, fornitori o consulenti.

La presente Policy Whistleblowing riguarda **la conoscenza, o il genuino sospetto** su **condotte, azioni od omissioni**, messe in atto **dal Personale di EMERGENCY, dei suoi partner, fornitori o consulenti**, che possano costituire **una o più violazioni, o nella minaccia o nel tentativo di violazione**, con il potenziale di:

- **causare danno a diritti fondamentali e al pubblico interesse**, e/o
- **minare l'integrità di EMERGENCY**.

Queste condotte, azioni e/o omissioni possono riguardare, senza limitazioni:

- ✓ **violazione di norme nazionali e/o dell'Unione Europea** (civili, amministrative o penali) come, per esempio, la frode e la mala gestione, corruzione; evasione fiscale; condivisione non autorizzata di informazioni confidenziali (sia personali che non) o di informazioni personali; pericolo alla salute e sicurezza sul luogo di lavoro; abuso sessuale e molestia sessuale; *stalking*; *mobbing*; discorsi d'odio; tutti gli illeciti che possano attivare la responsabilità amministrativa di EMERGENCY secondo il Decreto Lgs. N. 231/2001; condotte che mettano a rischio gli interessi finanziari dell'Unione Europea (Art.35 TFEU) e le relative prerogative legislative dell'UE, il mercato interno dell'UE (Art.26, para. 2 TFEU) e le relative prerogative legislative dell'UE in questo ambito, le regole dell'UE sulla competizione e sugli Aiuti di Stato, le regole della tassazione delle imprese e quegli arrangiamenti che cercando di ottenere un vantaggio fiscale aggirando l'oggetto o le finalità previste nella normativa fiscale applicabile all'impresa;
- ✓ **violazione delle norme internazionali rilevanti per l'ambito umanitario come espresse dai Principi Umanitari ed i Core Humanitarian Standards, il Codice di Condotta di Emergency, e condotte in violazione dell'etica e deontologia di settore** e dei valori e principi di EMERGENCY, anche espressi nel Codice Etico contenuto nel MOG;
- ✓ **violazione delle policy di EMERGENCY** (PSEAH, Protezione Minori, Anti Corruzione e Anti-frode, Protezione dei Dati, Privacy, etc.)
- ✓ violazione del "**MOG**" (Modello di Organizzazione, Gestione e Controllo) adottato dall'Associazione ai sensi del D.Lgs. 231/2001, e **dei regolamenti di settore interni (e manuali) e/o delle procedure stabilite** come, per esempio, frode nelle procedure di acquisto; conflitto di interessi non dichiarato; grave violazione delle norme di salute e sicurezza sul lavoro, riciclaggio, etc.;
- ✓ qualsiasi azione od omissione che possa cagionare un danno a diritti fondamentali, all'interesse pubblico, nonché qualsiasi danno grave, significativo e rilevante (per es. ambientale, economico, alla salute, alla sicurezza, alla reputazione, etc.) ad EMERGENCY, alle comunità e popolazioni servite, al Personale, ai rappresentanti dell'Organizzazione o a terze parti in generale;
- ✓ altre **violazioni delle leggi italiane o nazionali dei Paesi di intervento di natura civile, amministrativa o penale**;
- ✓ qualsiasi **condotta, azione e/o omissione tesa ad occultare** le violazioni che precedono e le altre sussumibili sotto questa lista non esaustiva.

La presente Policy Whistleblowing **NON SI APPLICA** a:

- X segnalazioni su questioni riguardanti vertenze di lavoro di proprio interesse (per es. Il livello salariale, l'organizzazione ed estensione dell'orario di lavoro, le ferie ed i permessi, i conflitti e gli attriti tra membri dello staff aventi ad oggetto la collaborazione tra loro o la gerarchia, la performance di lavoro, etc.) che saranno trattati secondo i canali e le procedure previste dal dipartimento Risorse Umane;
- X il trattamento dei dati personali nell'ambito del rapporto contrattuale di lavoro con EMERGENCY, ove questa modalità di trattamento non abbia ripercussioni sull'interesse pubblico o l'integrità dell'ente;

- X reclami sui servizi (loro estensione, durata, collocazione, modalità, contenuto, etc.) prestati da EMERGENCY che non abbiano a che fare con la violazione di diritti fondamentali, il *do no harm* e/o la violazione dei *core humanitarian standards*.

Si ritengono inoltre ragionevolmente da escludere, ai presenti fini, le seguenti segnalazioni:

- X segnalazioni su questioni che siano già di pubblico dominio;
- X segnalazioni su questioni che non siano connesse all'attività e/o non siano sotto il controllo diretto di EMERGENCY. Generalmente, EMERGENCY risponde soltanto a segnalazioni/reclami su aspetti di cui EMERGENCY abbia/avesse la responsabilità e il controllo nel momento in cui la presunta violazione sarebbe avvenuta;
- X segnalazioni e reclami che siano offensivi, diffamatori o basati semplicemente su voci, che non riportino fatti ed episodi o comunque la descrizione di una specifica condotta, azione e/o omissione e che non indichino almeno il "cosa", "chi", "quando", "dove" e "come". Qualora anonimi, i reclami e le segnalazioni che non riportino sufficienti elementi nei termini sopra indicati, saranno automaticamente esclusi;
- X segnalazioni presentate con scopi palesemente intimidatori e/o di rappresaglia, che saranno automaticamente escluse;
- X segnalazioni/reclami che siano palesemente incoerenti con fatti notori o illeggibili, che saranno escluse automaticamente;
- X segnalazioni evidentemente fabbricate, frivole e/o maliziose, che saranno automaticamente escluse ed eventualmente, ove ne ricorrano i minimi presupposti, perseguite a loro volta;
- X segnalazioni nascenti da un accesso abusivo a dati e sistemi che saranno escluse automaticamente ed eventualmente perseguite ove ne ricorrano i minimi presupposti;
- X segnalazioni realizzate con invio massivo di email, che saranno escluse automaticamente ed eventualmente perseguite ove ne ricorrano i minimi presupposti.

È opportuno qui rilevare, che mentre il Decreto Legislativo n. 24/2023 limita:

(i) **l'ambito oggettivo** di applicazione delle garanzie e prescrizioni in esso contenute alla lista degli illeciti ivi prevista e

(ii) **l'ambito soggettivo** – e quindi la qualifica di "Whistleblower" – a chi riporti sospetti o testimonianza su violazioni rilevanti per il decreto e conosciute in ragione del proprio lavoro/servizio per l'Ente,

EMERGENCY ha invece stabilito di estendere questi ambiti di applicazione oltre quanto perimetrato dal Decreto Legislativo n. 24/2023, come previsto qui di seguito, al paragrafo 2.

Questa decisione dipende **dalla particolare natura dell'attività svolta da EMERGENCY** quale organizzazione umanitaria, non-profit e del terzo settore che opera a livello internazionale ed è tenuta a rispettare le norme internazionali e quelle di settore (per es. *Accountability to Affected Population* (AAP)) per gli attori umanitari, nonché dalla natura del suo mandato, **quale ente privato la cui attività è, esclusivamente, di pubblico interesse**.

La presente Policy Whistleblowing **si applica ovunque EMERGENCY operi** (i.e. nella sede centrale, negli uffici Paese, nelle sedi di attività anche qualora temporanee e/o condivise).

La Policy Whistleblowing non intende sostituire le altre policy e procedure ad EMERGENCY, **ma le integra, predisponendo un unico meccanismo di segnalazione interna sulle violazioni e gli incidenti** (siano esse sospettate, evidenti, minacciate o allo stadio di tentativo) e di gestione delle stesse con le relative regole, principi e procedure.

In particolare, la Policy Whistleblowing integra:

- I Principi Umanitari;
- I Core humanitarian standard;
- Il Codice di Condotta ed il Codice Etico di EMERGENCY;
- La policy Anti-Frode & Anti-Corruzione;
- La policy su PSEAH;
- La policy sulla Protezione dei Minori;
- Le policy ed il manuale di Protezione dei Dati;
- Il MOG ex D.Lgs. n. 231/2001 di EMERGENCY;
- Il manuale amministrativo e finanziario di EMR;
- Tutti i regolamenti e procedure di salute e sicurezza sul lavoro;
- Le Procedure Operative Standard (field level);
- Qualsiasi ulteriore policy che EMERGENCY sviluppi nel quadro dell'avanzamento sugli standard operativi e sulla responsabilità sociale.

3. PRINCIPI E DEFINIZIONI

Tecnicamente, il termine "whistleblowing", è definito come *la rivelazione confidenziale di qualsiasi sospetto nell'ambito lavorativo che sia relativo alla percezione di scorrettezze o mala gestione* (attraverso condotte come quelle esemplificate nel paragrafo 1 o assimilabili).

Seguendo la volontà e la necessità di EMERGENCY di espandere gli ambiti oggettivo e soggettivo di applicazione del D.Lgs. n. 24/2023, "whistleblowing" può essere definito per EMERGENCY come *la rivelazione confidenziale (e protetta) di qualsiasi sospetto di violazione emerso **riguardo all'attività svolta da EMERGENCY** che sia relativo alla percezione di scorrettezze o mala gestione* (attraverso condotte come quelle esemplificate nel paragrafo 2).

- **"Whistleblower"** o "Segnalante" è qualsiasi persona fisica che riveli un sospetto (o la conoscenza) di fatti avvenuti nel contesto dell'attività svolta da EMERGENCY, **qui includendo anche coloro che non abbiano alcuna relazione di carattere lavorativo con EMERGENCY** (i.e. beneficiari e beneficiarie, pazienti, le loro comunità, leader e rappresentanti, autorità, ecc.).
- **"Persona segnalata"** o "Persona presunta" o "Persona oggetto di reclamo" è la persona che si presume abbia messo in atto la condotta scorretta e/o illecita.
- **"Testimone"** o "Persona informata" è qualsiasi persona che fosse presente al momento della condotta contestata o ne abbia avuta conoscenza diretta (avendo sentito, visto, letto, etc.).
- **"Segnalazione"** o "Report", "Sospetto", "Preoccupazione", "Rivelazione" è l'azione specifica di far conoscere/sapere della condotta scorretta/illecita, attuale o sospettata.

- **“Incidente”**, “Oggetto di”, “Contenuto di”, “Questione” è la condotta, l’azione e/o l’omissione considerata illecita/scorretta e descritta nella segnalazione.
- **“Canale”** è la modalità di comunicazione della segnalazione/reclamo/preoccupazione. Può trattarsi di una piattaforma digitale, di un indirizzo email dedicato, di una hotline, delle persone autorizzate a riceverla di persona, di una scatola per la raccolta di segnalazioni in cartaceo, etc.
- **“Compliance”** è la conformità del proprio agire alle norme cogenti, i regolamenti e gli standard di settore, gli obblighi contrattuali, il proprio mandato e valori. Il focus in questo ambito è su *“Come realizziamo l’attività/il servizio”*.
- **“Feedback”** è l’informazione, la dichiarazione, la reazione a un processo/attività (o l’informazione ottenuta attraverso quella reazione).
- **“Meccanismo di Segnalazione (CRM)”** è l’insieme degli strumenti, regole, principi, responsabilità e procedure che sono intese a consentire che le segnalazioni e la risposta alle stesse siano sicure, discrete, spedite, imputabili e verificabili a livello organizzativo.
- **“La normativa Whistleblowing”** è, in particolare, quanto previsto nel Decreto Legislativo n. 24/2023 che regola la materia per tutti gli enti pubblici e privati rilevanti, costituiti e/o registrati in Italia.

Tutto il Personale di EMERGENCY (nella sua accezione più larga) **è tenuto a segnalare prontamente** qualsiasi violazione (o sospetto di violazione, anche tentata) delle prescrizioni indicate nella presente Policy Whistleblowing, **attraverso i canali interni** predisposti.

Qualsiasi segnalazione deve essere comunicata, **come prima cosa, attraverso uno dei canali interni** appositamente predisposti e di seguito indicati al par. 4.1.

In conformità con quanto previsto dal D.Lgs. 24/2023, la segnalazione potrà essere consegnata ai **canali esterni predisposti dall’autorità ANAC**, nei seguenti casi:

- la persona segnalante ha già effettuato una segnalazione interna in conformità alla presente Policy Whistleblowing, ma l’Associazione non ha dato seguito alla stessa;
- la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione potrebbe determinare un rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Quello dell’ANAC (<https://www.anticorruzione.it/>), ossia l’Autorità Nazionale Anti-Corruzione. è il canale secondario/esterno indicato dalla normativa sopra richiamata. ANAC è invece indicato direttamente dal Decreto Lgs. n. 24/2023 come **l’esclusivo canale utilizzabile per segnalare le ritorsioni eventualmente subite da chi segnala**. In caso ci si rivolga ad ANAC, si dovrà fare riferimento alla sezione whistleblowing del suo sito (<https://whistleblowing.anticorruzione.it/#/>), in modo da garantirsi che la propria segnalazione sia trattata tecnicamente come “whistleblowing”. E’

da specificare che ANAC considera "whistleblowing" soltanto le segnalazioni aventi ad oggetto atti, omissioni e condotte che presumibilmente violino la normativa indicata nel D. Lgs. n. 24/2023.

A determinate condizioni, i segnalanti possono anche effettuare direttamente una **divulgazione pubblica**, quando:

- la persona segnalante ha previamente effettuato una segnalazione interna ed esterna, in conformità a quanto sopra indicato, ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

Nel predisporre una **divulgazione pubblica o nel rivolgersi al canale secondario, si raccomanda** a chi segnala di farsi consigliare da persone esperte in materia, prima di inviare la segnalazione tramite questi canali.

Poiché sulle segnalazioni di condotte scorrette/illecite incidono complessi aspetti della normativa sulla protezione dei dati personali e di diritto penale, qualora la segnalazione non fosse predisposta secondo tutti i requisiti tecnici e legali inerenti, la persona che segnala potrebbe subire conseguenze legali, azionabili sia da parte di EMERGENCY che da parte della persona segnalata, nonché direttamente da parte delle autorità.

Chi segnali tramite il canale secondario o la divulgazione pubblica non potrà godere delle garanzie e delle condizioni scriminanti e/o a discolora predisposte dal D.Lgs. n. 24/2023 (per esempio, sull'avvenuto utilizzo di dati personali, o contro l'accusa di diffamazione e calunnia, etc.) ogni qualvolta:

- si riportino violazioni non sussumibili sotto l'ambito oggettivo di applicazione del D.Lgs. 24/2023, e/o
- chi segnala non rientra nelle categorie previste dall'ambito soggettivo di applicazione di tale normativa, specialmente per le misure di protezione.

Tutto quanto sopra, **fermo restando ulteriori meccanismi posti a favore della persona segnalante**, ai quali quest'ultimo possa ricorrere, eventualmente al di fuori del contesto regolato dalla normativa Whistleblowing, per la tutela delle sue ragioni e/o diritti, quali ad esempio:

- tipicamente per il settore di attività di EMERGENCY, il canale/contatto predisposto dal donatore istituzionale che finanzia l'azione specifica di EMERGENCY entro il cui perimetro sarebbero avvenuti l'atto, l'omissione e/o la condotta presunti in violazione oppure le organizzazioni internazionali o gli organi pubblici cui EMERGENCY sia accreditata;
- i sindacati;
- l'autorità giudiziaria.

In termini generali, chi segnala deve essere consapevole che **le divulgazioni pubbliche e quelle comunque fatte all'esterno** dei canali predisposti internamente, **quando fatte in modo ingiustificato e/o frivolo**, possono minare la fiducia nel settore umanitario e potranno risultare in azioni disciplinari e/o legali.

EMERGENCY ha il dovere di proteggere chi segnala, e le persone fisiche e/o giuridiche associabili, contro ogni forma di ritorsione, sia essa anche "solo" minacciata o tentata.

Per "persone associabili" si intende:

- Chi facilita la segnalazione da parte del segnalante ed operi all'interno del medesimo contesto lavorativo;
- Parenti (compresi conviventi) entro il 4° grado, che operino nello stesso contesto lavorativo di chi segnala;
- Chi sia direttamente collega della persona segnalante, lavori nel medesimo contesto lavorativo della stessa e che abbia con detta persona un rapporto abituale e corrente;
- Enti di proprietà del/della segnalante o per il quale il/la segnalante lavori, o che operi nello stesso contesto lavorativo;
- Segnalante anonimo/a se successivamente identificato/a e soggetto/a a ritorsioni.

È proibita qualsiasi forma di ritorsione, contro chiunque segnali in buona fede eventuali o attuali violazioni.

Quindi, qualsiasi azione disciplinare o ripercussione – inclusi, a titolo esemplificativo (ex Art. 17 Decreto Legislativo n. 24/2023), il *licenziamento, la sospensione, il de-mansionamento, la mancata promozione, le modifiche del mansionario, la ricollocazione, la riduzione salariale, il cambio dell'orario di lavoro, le note negative, le referenze negative; le misure disciplinari o altre sanzioni, la discriminazione, il mancato rinnovo del contratto* (etc.) – imposte a chi abbia segnalato in buona fede, o alle persone fisiche/giuridiche associabili, è da considerarsi automaticamente nulla a qualsiasi fine. Inoltre, chi abbia segnalato correttamente ed in buona fede, non è punibile per contestazioni sull'utilizzo dei dati personali o su l'obbligo del segreto (escluso quello forense o medico) e quindi non dovrà subirne le conseguenze legali.

È severamente vietato riversare qualsivoglia conseguenza negativa su chi riporta sospetti in buona fede, indipendentemente dalla fondatezza degli stessi.

Perché chi segnala possa beneficiare delle protezioni previste dal decreto legislativo 24/2023 e la segnalazione sia considerata in buona fede, non è necessario che la questione riportata si confermi fondata attraverso il procedimento di indagine.

Una segnalazione genuina, presentata secondo i modi e i tempi prescritti in pieno rispetto della riservatezza, **resta un prezioso e valido contributo ad EMERGENCY** nel perseguire i suoi valori e preservare sua integrità. Quindi, anche qualora la questione oggetto di segnalazione si riveli



infondata, nessuna ritorsione deve colpire chi abbia segnalato, chi conosca dei fatti (testimoni) né la persona segnalata.

Il/La segnalante o le persone associabili che abbiano **sofferto ritorsioni** in ragione dell'aver promosso una segnalazione secondo i requisiti del Decreto Legislativo n. 24/2023 (ossia *direttamente connessa* alle violazioni delle norme indicate nel decreto - da parte di chi *appartenga alle categorie* indicate nell'ambito soggettivo di applicazione del decreto - *seguendo le modalità e canali* privilegiati dal decreto stesso) devono denunciare le suddette ritorsioni al ANAC quale canale primario, in modo che ANAC possa indagare e valutare le presunte ritorsioni ed eventualmente imporre la rimozione in toto degli atti ritorsivi e sanzionare l'Ente. Si tenga presente che ANAC invece, non costituisce un canale di ricorso per la persona segnalata contro le decisioni prese dall'Ente nei suoi confronti a seguito del procedimento disciplinare.

Qualora, la funzione di Compliance o chiunque altro ad EMERGENCY, riceva una segnalazione avente ad oggetto presunte ritorsioni da parte di EMERGENCY contro chi aveva segnalato, dovrà prontamente riorientare chi segnala le ritorsioni verso il canale ANAC, mantenendo il più alto grado di riservatezza sulla segnalazione di ritorsione e cancellando in modo irrecuperabile ogni traccia della segnalazione di ritorsione dai propri file, account e sistemi.

Al contrario, **segnalazioni fatte con malizia** (artificiose, speculative, intenzionalmente false, contraddistinte da colpa grave, etc.) **presentate per profitto personale o di terze parti**, con intenti calunniosi, diffamatori, **che causino danno** ad altri membri del personale o ad EMERGENCY stessa, **costituiscono un atto grave** e dunque **presupposto di applicazione di misure disciplinari** e/o **avvio di procedimenti legali** (Art. 16, comma 2, e Art. 21 Decreto Legislativo n. 24/2023) contro il/la segnalante malevolo/a, in conformità con il sistema disciplinare interno dell'Associazione, come previsto in particolare dal MOG ex D.Lgs 231/2001 e dal Regolamento Interno adottato in data 22 gennaio 2019.

EMERGENCY perseguirà le segnalazioni fraudolente in quanto queste ultime possono avere effetti sulla sicurezza nei contesti di operatività dell'Associazione, sulla sua reputazione e su quella degli operatori e delle operatrici, oltre a rappresentare un grave discostamento dall'etica di settore e dallo stesso mandato di EMERGENCY.

Le salvaguardie predisposte dalla normativa Whistleblowing (incluse le deroghe sulla violazione del trattamento dei dati, della privacy e delle misure di sicurezza, etc.) **non si applicano a chi abbia segnalato in modo fraudolento e specifiche sanzioni** sono previste per questa tipologia di violazione nel sistema sanzionatorio nel MOG di EMERGENCY.

L'identità **di chi segnala, così come quella della persona segnalata e di qualsiasi altra persona coinvolta nella segnalazione** è da mantenersi strettamente riservata.

Queste identità (inclusa **qualsiasi informazione da cui si possa derivarle**), non possono essere rivelate a persone altre da quelle investite formalmente della responsabilità di ricevere e/o di indagare le segnalazioni (e formalmente autorizzate ex Art. 12, comma 2 del Decreto Legislativo n.

24/2023) e/o di sanzionare il comportamento (qui limitatamente all'identità della persona segnalata), a meno che non intervenga **il consenso specifico ed esplicito** da parte del/della titolare dei dati, a valere sui suoi soli dati personali.

Aldilà della normativa specificamente relativa alla Protezione dei Dati (i.e. GDPR) e alle garanzie previste dal decreto Whistleblowing, proteggere l'identità di ciascun individuo coinvolto nella segnalazione è **applicazione immediata e diretta del diritto dei diritti umani, del rispetto della dignità umana, del principio di innocenza e del do no harm.**

Di fatto, le ripercussioni che possono discendere da una fuga di notizie e dalla violazione dei dati personali in questo ambito possono essere estese e gravi, sia per EMERGENCY, che per le persone coinvolte e per l'utenza tutta, in termini di sicurezza (fino al poter cagionare delitti d'onore o attacchi alle strutture di EMR) di dignità e di reputazione, poiché le accuse sono normalmente persistenti ed indelebili, indipendentemente dalla genesi dello specifico incidente e dalle conclusioni cui sia pervenuta l'indagine.

Data la gravità delle possibili conseguenze, **la violazione della riservatezza in questo ambito sarà trattata, in conformità con il sistema disciplinare interno dell'Associazione, con:**

- **sanzioni disciplinari appropriate, fino al licenziamento per giusta causa per i/le dipendenti;**
- **appropriate azioni e rimedi contrattuali, per partner, consulenti e fornitori, etc.**

L'articolazione delle misure di salvaguardia della riservatezza attraverso le varie fasi del meccanismo di segnalazione (ricezione, profilazione, indagine, procedimento disciplinare) saranno specificate di seguito in questo documento.

I seguenti **principi** governano questa Policy Whistleblowing, i canali predisposti per presentare segnalazioni e le procedure d'indagine e di risposta alle segnalazioni:

- **Trasparenza:** la Policy Whistleblowing e il Meccanismo di Segnalazione sono conosciuti dal personale di EMERGENCY, i suoi partner, consulenti e fornitori nonché, in particolare, dalle comunità servite, nei loro fini, modalità di azionamento, procedure e funzioni dedicate. Le persone coinvolte in un incidente sono regolarmente informate della progressione della procedura stabilita;
- **Integrità:** Whistleblowing e CRM rispettano i valori e gli standard etici;
- **Accountability:** il meccanismo per l'attuazione della Policy Whistleblowing è predisposto, visibile, accessibile, funzionante, responsivo ed informativo e le funzioni pertinenti sono assegnate;
- **Principio di legalità:** la Policy Whistleblowing e il Meccanismo di Segnalazione (CRM) sono ben definiti, le responsabilità sono preassegnate e conosciute, i criteri e le regole che sovrintendono alle procedure relative sono dettagliati ed espliciti, l'indagine e le decisioni avvengono tempestivamente, in modo tracciato, motivato e notificato;
- **Imparzialità e indipendenza:** la valutazione dei fatti è obiettiva e basata sulle prove e/o indizi chiari e concordanti; la segnalazione è trattata nel suo merito senza pregiudizi e le decisioni prese sono imparziali;

- **Non-discriminazione:** tutte le persone che segnalino, testimonino o che siano segnalate sono trattate equamente ed indipendentemente dalla loro età, abilità fisica, cultura, etnia, genere, identità di genere, religione, orientamento politico, appartenenza a organizzazioni sindacali, affiliazioni, convinzioni od orientamento sessuale;
- **Responsività e Tempestività:** le segnalazioni sono prese seriamente e gestite prontamente. La notifica di ricezione a chi segnala avviene entro 7 giorni dalla conoscenza della ricezione (24 ore per segnalazioni aventi ad oggetto PSEAH). Le decisioni in merito al caso, quando indagato, sono prese entro 3 mesi dalla conferma di ricezione della segnalazione (14 giorni per i casi rilevanti per PSEAH) a meno che non intervengano circostanze per cui si imponga una tempistica differente;
- **Accessibilità:** il meccanismo è accessibile ed è progettato per superare le barriere eventualmente imposte dalla lingua, dal grado di alfabetizzazione e di istruzione, dall'abilità fisica, dalla povertà, dalla distanza fisica o dalla paura di ritorsioni;
- **Appropriatezza culturale:** il meccanismo è predisposto in modo da considerare le specifiche culturali nelle comunità servite;
- **Finalità definite:** le segnalazioni ed il loro contenuto sono trattati al solo fine dell'indagine su possibili violazioni;
- **Consenso:** I dati personali di chi segnala e dei/delle testimoni possono essere rivelati solo dietro esplicito, libero, e specifico consenso;
- **Riservatezza:** le informazioni sui dati personali devono essere quelle essenziali e rilevanti per le indagini sulla presunta violazione e condivise soltanto tra una cerchia ristretta di persone formalmente autorizzate a trattarle;
- **Sicurezza:** i pericoli per le persone coinvolte dalla segnalazione devono essere debitamente considerati e soppesati attraverso l'analisi dei rischi e ove rilevanti devono essere predisposte le misure di prevenzione o mitigazione del pericolo;
- **Efficienza e Proporzionalità:** il meccanismo predispone strumenti sufficienti e adeguati al livello di complessità e gravità, per la gestione della segnalazione.

4. FARE UNA SEGNALAZIONE – MECCANISMO DI SEGNALAZIONE (CRM)

Il **Meccanismo di Segnalazione** (CRM) dell'Associazione, è inteso come strumento facilmente **accessibile/conoscibile da chi sia interessato/a, e costituisce un processo appropriato** che promuove l'*accountability* di EMERGENCY "in modo tale che le comunità e il personale siano in grado di riportare abusi e accedere a un maggior grado di protezione attraverso la deterrenza"¹ predisponendo un **meccanismo equo, spedito e discreto** per l'**emersione, l'indagine e la risposta** su questo tipo di questioni.

Le segnalazioni devono essere fatte **in modo appropriato** tramite i canali interni predisposti – a tale riguardo, si veda quanto già chiarito al paragrafo 3 in merito a canali interni ed esterno, nonché più nel dettaglio sui canali interni il paragrafo 4.1.

Segnalare in modo appropriato richiede:

- Di agire **tempestivamente** (*meglio prima che dopo*) **attraverso i canali e gli strumenti interni predisposti**;
- Di presentare/condividere/discutere le informazioni **solo con le persone autorizzate** ai sensi della presente Policy Whistleblowing, **in Sede o a livello Paese**;
- fin dove possibile, di condividere **tutte** le informazioni già disponibili relative al “**chi, cosa, come, quando e dove**” **in relazione alla condotta oggetto della segnalazione**;
- Di esprimere chiaramente il proprio grado di certezza/incertezza sui fatti/atti/omissioni e condotte riportati (i.e. *ho sentito/ho visto/ero presente/sono certo/ritengo/credo/mi sembra/ etc.*);
- se possibile e facendo sempre attenzione alla tutela della riservatezza per quanto opportuno, di fare menzione di **chi altro/a** fosse eventualmente presente o sappia della questione oggetto di segnalazione oltre alla persona segnalata e la persona che segnala;
- Di allegare **qualsiasi prova materiale** a sostegno della segnalazione che sia **già** in possesso di chi segnala;
- Di riportare **qualsiasi altra fonte di informazioni** che possa agevolare le funzioni responsabili nella verifica dei fatti;
- Di esprimere **le proprie preoccupazioni sui rischi** che si starebbero correndo in ragione della segnalazione e di quelli corsi da persone associabili a chi sta segnalando.

I fatti che potrebbero consistere in violazioni nel contesto di operatività di EMR, **possono essere segnalati** anche qualora **si ignori chi sia autore della violazione!**

Le segnalazioni possono essere anonime.

In questo caso, EMERGENCY farà tutto quanto possibile per indagare la questione segnalata. Tuttavia, si informa che l'anonimato potrebbe compromettere l'abilità di EMERGENCY nello stabilire una chiara direzione per le indagini e, in definitiva, la possibilità di raggiungere una buona cognizione dei fatti accaduti e riportati. Inoltre, la scelta dell'anonimato impedisce ad EMERGENCY di predisporre tutte le misure necessarie a proteggere adeguatamente chi segnala e le persone associabili. I potenziali segnalanti che intendano presentare una denuncia anonima devono essere consapevoli che, in tal caso, è ancora più essenziale fornire dettagli adeguati sulle relative accuse e sui luoghi in EMERGENCY in cui si sarebbe verificato il fatto, oltre che indicare qualsiasi ulteriore fonte di prova affidabile che alla quale EMERGENCY possa risalire per verificare le informazioni denunciate.

Chi segnala può essere assistito/a da una persona di propria fiducia in qualità di facilitatore.

In questo caso, la persona di fiducia prescelta dovrà sottoscrivere un *accordo di riservatezza* e, in quanto facilitatore, ha diritto alle stesse misure di protezione previste per chi segnala, eccetto che per l'inversione dell'onere della prova in caso di ritorsioni, misura questa riconosciuta soltanto e strettamente alla persona segnalante.

Le persone segnalanti non devono svolgere autonomamente e per proprio conto indagini sulle questioni segnalate (o da segnalare), anche se motivate dalla volontà di raccogliere prove materiali a sostegno della segnalazione.

L'indagine è infatti una procedura complessa che implica il rispetto di svariate garanzie ed è quindi di competenza delle persone debitamente formate ed assegnate alle relative funzioni.

Inoltre, chi intenda segnalare può esporsi a rischi maggiori spingendosi ad indagare in proprio un iniziale sospetto.

EMERGENCY ha predisposto questo meccanismo tenendo conto dell'Obbligo di Assistenza e Protezione, di modo da assicurare una debita risposta senza implicare la sovraesposizione di chi vi partecipi attivamente.

4.1 Canali

EMERGENCY ha predisposto i seguenti **canali interni** per trasmettere una segnalazione:

- **Indirizzi di posta elettronica dedicati:**

- **complaintreporting@emergency.it** – reindirizza la posta in entrata a chi rivesta il ruolo di Compliance Manager in sede a Milano.
- A livello di missione Paese, EMERGENCY ha predisposto degli indirizzi di posta elettronica specifici per Paese, nella seguente forma **complaintreporting.paese@emergency.it** composti dalle parti ""complaintreporting.""+ il nome del Paese in inglese (es. afghanistan/sudan/uganda etc). Questo indirizzo è accessibile ai due Complaint Reporting Officer nel Paese.
- **complaintcommittee@emergency.it** - reindirizza direttamente agli indirizzi di posta elettronica di Presidente e Vicepresidente e deve essere utilizzato per segnalare in prima istanza solo quando gli altri due indirizzi indicati sopra siano entrambi gestiti da persone potenzialmente coinvolte dall'oggetto della segnalazione (i.e. non neutrali).

Questo canale consente l'uso di qualsiasi lingua.

Questo canale non può garantire l'anonimato in senso stretto. Tuttavia, si assicura a chi utilizzi questo canale tramite uno pseudonimo, che EMR non indagherà sulla reale identità o sull'IP di provenienza della segnalazione;

- **Complaint box (cassetta per le segnalazioni)** è una cassetta fisica disponibile ad EMERGENCY in ogni struttura e sede, anche ove temporanee. La cassetta viene posizionata in aree ad uso non esclusivo, seppur discreto, questo per assicurare che chi stia trasmettendo una segnalazione con questo canale, non sia immediatamente riconoscibile (vedi *Annex 2 mappatura delle cassette per le segnalazioni nella tua sede*). Vicino alla cassetta sono predisposti i moduli per la segnalazione; in ogni caso possono essere depositate qui anche le segnalazioni in forma libera. Questo canale permette la trasmissione anonima di segnalazioni. La cassetta è chiusa a chiave e viene aperta almeno ogni 14 giorni dai Complaint Reporting Officer a livello Paese (HR Manager e/o Country Admin e/o Country Director) o da chi svolga funzione di Compliance Manager in sede centrale o comunque da persone debitamente autorizzate e formate qualora la cassetta si trovi in unità operative temporanee. Le segnalazioni ivi riscontrate vengono inserite sul Portale

per la Gestione delle Segnalazioni (vedi *Annex 3*) di EMERGENCY (Microsoft Ltd) che i Complaint Reporting Officers condividono con il Compliance Manager presso la Sede Principale.

- **Via posta cartacea** in busta ben chiusa e spedita ad EMERGENCY ONG ONLUS, all'attenzione di Compliance Manager, Via Santa Croce 19, 20122, Milano, Italia. Questo canale consente il pieno anonimato della persona segnalante, qualora desiderato.
- **Hotline** (vedi *Appendice 1 per i numeri relativi ad ogni Paese*) è disponibile per ogni missione-Paese. Si tratta fondamentalmente di un servizio di segreteria telefonica guidato, dove poter trasmettere le segnalazioni 24/24-7/7. I messaggi ivi registrati sono scaricati da chi svolge la funzione di Complaint Reporting Officer e trascritti in un registro per essere poi inseriti sulla Piattaforma di Gestione delle Segnalazioni di EMERGENCY. L'anonimato è qui possibile per quanto concerne la propria identità, sebbene aspetti biometrici (la voce) siano coinvolti. Può essere utilizzata qualsiasi lingua.
- **Segnalazione presentata verbalmente direttamente alle funzioni autorizzate:** le segnalazioni possono essere presentate verbalmente a chi rivesta le funzioni dedicate, ossia Complaint Reporting Officer a livello Paese oppure Compliance Manager a livello della sede centrale. Può essere utilizzata qualsiasi lingua per la segnalazione. Ove sia necessaria la traduzione, si prega di segnalare la necessità di una traduzione o mediazione prima dell'incontro. L'anonimato di chi segnala qui è inevitabilmente escluso; in ogni caso è prevista una serie di consistenti salvaguardie di modo che non si verifichi dispersione di dati personali.

! Qualora almeno una persona delle due investite della funzione di Complaint Reporting Officer a livello Paese sia coinvolta nei fatti oggetto di segnalazione, chi segnala potrà rivolgersi separatamente all'altra persona investita come Complaint Reporting Officer a livello Paese oppure direttamente a chi rivesta il ruolo di Compliance Manager. In caso anche quest'ultima persona sia coinvolta nei fatti riportati, la segnalazione può essere trasmessa direttamente all'indirizzo complaintcommittee@emergency.it

Il personale di EMERGENCY che non sia incaricato di gestire i canali CRM e che riceva una segnalazione rilevante rispetto a questa Policy, **dovrà:**

- trasmettere rapidamente la segnalazione, entro 3 giorni (immediatamente per segnalazioni inerenti SEAH) dalla ricezione, direttamente ai canali indicati sopra (e ai ruoli preposti);
- informare di conseguenza la persona segnalante; e
- alla conferma di ricezione da parte dei ruoli preposti, cancellare definitivamente ogni traccia della segnalazione che si trovi ancora nei suoi file, comunicazioni e strumentazione. Il personale ivi coinvolto potrà trattenere soltanto la conferma di ricezione da parte dei ruoli incaricati, a riprova dell'aver assolto le istruzioni di cui sopra.

Qualsiasi violazione delle indicazioni di cui sopra sarà da considerarsi quale condotta in violazione di questa Policy e soggetta a sanzione.

4.2 Ruoli chiave e Responsabilità connesse

I ruoli chiave deputati a **gestire l'ingresso di una segnalazione e le relative procedure**, sono:

- **Complaint Reporting Officer** (CRO) – previsti nel numero minimo di due persone per ogni missione-Paese, di solito individuate nel HR Manager Field (o Country Admin quando questa figura non sia presente) e Country Director, specificatamente e formalmente incaricate di questa funzione e della relativa gestione dei dati. In caso di barriere linguistiche, di molteplicità di unità operative nel Paese in un territorio frammentato, difficilmente accessibile o remoto, di assenza o impossibilità di una o entrambe le persone assegnate a CRO, i compiti di queste ultime potranno essere assegnati a delegati, anche temporaneamente, se approvato da chi rivesta la funzione di Compliance Manager;
- il **Compliance Manager** (CM), è la persona qualificata a livello sede centrale, specificatamente e formalmente incaricata;
- il **Comitato per le Segnalazioni** (CC) è composto da Presidente e Vicepresidente dell'Associazione.

Questi ruoli sono **assegnati formalmente**, insieme con **l'impegnativa sulla riservatezza e l'atto di autorizzazione alla gestione dei dati**, quest'ultima **graduata in base al ruolo rivestito** (per es. chi rivesta il ruolo di Complaint Reporting Officer ha accesso soltanto alle segnalazioni inerenti al Paese di afferenza e comunque entro il grado di sensibilità che prescrive lo svolgimento dell'indagine a livello Paese). I ruoli e chi li detiene sono previsti nel Registro di Trattamento dei Dati con le relative responsabilità e prerogative.

Le principali responsabilità dei ruoli sopra indicati nella fase di ingresso della segnalazione, sono le seguenti:

- **il Complaint Reporting Officer** (CRO):
 - diffonde e rende accessibile e conosciuta questa Policy Whistleblowing a livello Paese e offre orientamento e formazione su come utilizzarne i canali;
 - assicura che le cassette per le segnalazioni siano debitamente distribuite, propriamente collocate e mantenute, e vengano aperte secondo la frequenza prevista; che *i moduli per la segnalazione* e la *Nota Informativa sulla Riservatezza per Segnalante e Facilitatore (Annex 6)* siano disponibili in cartaceo in prossimità della cassetta per le segnalazioni;
 - assicura che la hotline sia disponibile e funzioni;
 - assicura supporto a chi voglia segnalare qualora venga richiesto;
 - si rende sempre disponibile a ricevere direttamente le segnalazioni in forma verbale;
 - monitora l'ingresso di segnalazioni all'indirizzo di posta elettronica dedicato al livello paese, i.e. complaintreporting.paese@emergency.it;
 - assicura che i dati personali (diretti ed indiretti) siano protetti e condivisi soltanto con le persone autorizzate;
 - assicura la riservatezza sull'ingresso di una segnalazione e sui suoi contenuti;
 - assicura che le segnalazioni eventualmente trasmesse tramite cassetta per le segnalazioni oppure tramite hotline siano tempestivamente raccolte;

- assicura la notifica di ricezione alla persona segnalante entro 7 giorni dalla raccolta (24 ore per segnalazioni inerenti SEAH) insieme con la trasmissione della *Nota Informativa sulla Riservatezza per Segnalante e Facilitatore (Annex 6)*;
- inserisce tempestivamente le segnalazioni raccolte nella Piattaforma di Gestione delle Segnalazioni (vedi Annex 3).

- **il Compliance Manager (CM):**

- assicura l'accessibilità e la conoscenza di questa Policy Whistleblowing a livello generale e nelle sedi centrali, fornisce orientamento e formazione a tutto il personale e ai portatori di interesse su come utilizzarla;
- forma, orienta, coordina e supporta chi riveste il ruolo di Complaint Reporting Officer a livello Paese;
- monitora gli ingressi delle segnalazioni all'indirizzo di posta elettronica dedicato complaintreporting@emergency.it;
- provvede a notificare la ricezione della segnalazione alla persona segnalante entro 7 giorni dalla trasmissione via complaintreporting@emergency.it (24 ore nel caso di segnalazioni inerenti SEAH) insieme con la *Nota Informativa per il Segnalante e il Facilitatore*;
- assicura la visione tempestiva delle segnalazioni inserite dai Complaint Reporting Officer nella Piattaforma di Gestione delle Segnalazioni (vedi Annex 3) e ne profila prontamente il contenuto;
- inserisce le segnalazioni ricevute tramite complaintreporting@emergency.it nella Piattaforma di Gestione delle Segnalazioni (Annex 3);
- relaziona al Comitato per le Segnalazioni sulle segnalazioni escluse da ulteriore indagine, anonimizzandole, in modo da rendere conto di questa attività;
- assicura in ogni momento la minimizzazione dei dati personali, e la riservatezza sull'ingresso e sull'oggetto di qualsiasi segnalazione;
- monitora i canali e la procedura in modo da apprendere le eventuali debolezze e le aree di miglioramento.

- **il Comitato per le Segnalazioni (CC):**

- assicura la notifica di ricezione a chi segnali direttamente tramite complaintcommittee@emergency.it entro 7 giorni dalla ricezione stessa (24 ore per casi inerenti SEAH) insieme con la *Nota Informativa per Segnalante e Facilitatore*;
- assicura la riservatezza dell'ingresso della segnalazione e del suo oggetto, oltre che dei dati personali in essa contenuti.

4.3 Accessibilità

I canali sopra descritti devono essere facilmente accessibili e conoscibili.

Al fine di assicurare adeguata visibilità ai canali saranno prese le seguenti misure:

- pubblicazione sul sito di EMERGENCY (anche in conformità a quanto prescritto al riguardo dal D.Lgs. 24/2023);
- nota in calce nelle email provenienti dalle caselle di posta elettronica della funzione Compliance;
- allegare il riferimento a questa Policy e il CRM a tutti i contratti col Personale, coi Partner e coi Fornitori;
- predisporre moduli specifici di formazione per il personale appena inserito;
- predisporre dei moduli di aggiornamento per tutto il personale;
- Poster e cartelloni nelle strutture delle missioni Paese, adeguati al contesto.

4.4 Riservatezza

Le identità di chi segnala, della persona segnalata e di terze parti che siano coinvolte nella segnalazione, sia come testimoni diretti che come persone informate, devono sempre essere trattate come informazioni **altamente riservate**.

Ciò significa che questi dati personali, ove conosciuti o comunque derivabili, **saranno mantenuti segreti** ed eventualmente rivelati, nel rispetto del *principio di minimizzazione* dei dati, **soltanto tra le persone formalmente incaricate di ricevere e trattare le segnalazioni**.

Il CRO a livello Paese e/o Compliance Manager in sede centrale, anche nelle comunicazioni verso il Comitato per le Segnalazioni, agiranno nel rispetto di **rigorosi standard di protezione** dell'identità delle persone coinvolte – o delle informazioni che potrebbero ricondurvi - che non potranno essere rivelate, a meno che non ne ricorrano le condizioni (i.e. contemporaneamente, consenso + necessità/assenza di altre evidenze oggettive).

Le identità di chi segnala, della vittima e della persona segnalata possono essere condivise con i membri della Squadra per le Indagini (*vedi sotto paragrafo 5 e seguenti*) se e nella misura in cui siano essenziali al piano di indagine.

L'identità della persona segnalata è rivelata alla Squadra per le Indagini e, se del caso, a chi si occupi del procedimento disciplinare.

L'identità dei testimoni e delle persone informate dei fatti saranno condivise soltanto con la Squadra per le Indagini.

Qualora chi segnala o la vittima richieda che la sua identità sia mantenuta segreta, chi rivesta il ruolo di Complaint Reporting Officer o Compliance Manager dovrà proteggere l'identità anche nel rinviare la segnalazione ad indagine. Se la conoscenza di queste identità sia essenziale all'opera della Squadra per le Indagini, Complaint Reporting Officer o Compliance Manager informeranno chi segnala o la vittima che l'indagine potrebbe essere inficiata dalla segretezza sulle loro identità al punto da impedirne l'attuazione, e attenderne la decisione riguardo al rilascio del consenso.

Chi segnala o sia testimone può ricevere tale richiesta di consenso soltanto dalle figure del Complaint Reporting Officer (per il livello Paese) o di Compliance Manager (in generale) e al solo fine di garantire la completezza delle indagini sulla condotta segnalata.

Qualora il contenuto della segnalazione comunque consenta di raccogliere evidenze e indizi che vadano al di là delle dichiarazioni di chi segnala o della vittima, allora l'identità di queste ultime dovrà essere mantenuta segreta, in ogni caso.

Anche la ricezione di una segnalazione deve essere mantenuta altamente riservata.

Le informazioni devono essere condivise soltanto fra le persone autorizzate ed incaricate di funzioni di Compliance (i.e. Complaint Reporting Officer(s), Compliance Manager, Comitato per le Segnalazioni, Squadra per le indagini) con l'aggiunta di DPO od OdV, ove rilevanti.

Altre notifiche, trasmesse per esempio a fini di prevenzione del rischio, saranno effettuate soltanto da Compliance Manager o dal Comitato per le Segnalazioni secondo il paragrafo seguente, e conterranno esclusivamente le informazioni essenziali ad attuare misure di mitigazione del rischio senza ulteriori dettagli su da chi provenga la segnalazione, l'oggetto della segnalazione o le altre persone coinvolte.

Tutti i canali interni descritti sopra sono progettati e predisposti in modo da garantire la protezione dei dati, specialmente delle identità e degli elementi, anche non personali, da cui si possa desumere, anche in modo indiretto, le identità stesse.

Qualsiasi violazione della riservatezza, inclusa quella relativa all'ingresso di una segnalazione ed il suo oggetto, sarà sanzionata quale violazione degli standard di integrità di EMERGENCY nonché della clausola sulla riservatezza contenuta negli accordi di lavoro, collaborazione, consulenza e fornitura.

La confidenzialità sull'identità della persona segnalante, della vittima, della persona segnalata, di testimoni e persone comunque menzionate nella segnalazione è prescritta dalla normativa; la violazione di queste salvaguardie è punita con sanzioni severe dalle autorità che sovrintendono la materia e da EMERGENCY a livello disciplinare.

4.5 Comunicazioni/Notifiche

La notifica di ricezione della segnalazione è dovuta a chi segnala entro 7 giorni (24 ore per segnalazioni inerenti SEAH) dal momento in cui l'esistenza della segnalazione da parte delle funzioni dedicate è acquisita.

La notifica di ricezione dovrà includere la *Nota Informativa* e una breve descrizione del sistema di CRM di EMERGENCY, in modo tale che chi segnala possa conoscere i suoi diritti e in particolare l'accesso alle misure protettive.

La verifica dell'esposizione al pericolo di chi segnala e delle persone associabili, in ragione dell'avvenuta segnalazione, deve essere svolta tempestivamente al momento della notifica di ricezione, a meno che gli elementi necessari non siano già stati espressi insieme alla trasmissione della segnalazione stessa.

Nei casi in cui:

- chi segnala sia personale di EMERGENCY e risulti appropriato applicare misure protettive; e/o

- la persona segnalata appartenga al personale di EMERGENCY e si ritenga necessaria l'applicazione di misure di precauzione in modo da allontanare la persona segnalata dall'ambiente di lavoro e/o dalla vittima;

allora,

la ricezione di una segnalazione sarà comunicata, nel rispetto del principio della *minimizzazione dei dati*, anche al *senior manager* della persona segnalata o della vittima o di entrambe, in modo da coordinare l'applicazione delle misure protettive e di quelle precauzionali, al solo fine di proteggere la sicurezza delle persone coinvolte, quella dell'ambiente di lavoro e l'integrità del processo di verifica dei fatti.

4.6 Profilazione della segnalazione (rilevanza)

- **Una volta ricevuta, la segnalazione viene registrata sulla Piattaforma di Gestione delle Segnalazioni.**

La Piattaforma di Gestione delle Segnalazioni è uno strumento digitale dell'infrastruttura IT di EMERGENCY destinato a supportare la trasmissione appropriata delle informazioni e dei dati tra le persone incaricate a livello Paese e sede centrale, e a tracciare, verificare e archiviare la progressione delle segnalazioni. La Piattaforma permette un accesso illimitato soltanto a chi rivesta la funzione di Compliance Manager (sede centrale) e al Responsabile del Dipartimento IT (che, in ogni caso, non è autorizzato a visualizzarne i contenuti). Chi riveste funzione di Compliant Reporting Officer ha invece un accesso limitato alle segnalazioni inerenti al Paese di appartenenza che siano state caricate da loro o che siano state condivise con loro da chi riveste funzione di Compliance Manager.

- **Entro massimo 20 giorni (24 ore per le segnalazioni inerenti SEAH) dalla ricezione**, chi riveste ruolo di Compliance Manager, o individualmente o in collaborazione con chi riveste ruolo di Complaint Reporting Officer per il livello Paese, conduce la verifica di rilevanza e l'inquadramento della segnalazione che risulti rilevante (*profilazione del caso*).

Questa fase è intesa a:

- **verificare la rilevanza della segnalazione** – con l'esclusione immediata e conseguente delle segnalazioni offensive, illeggibili, manifestamente irrilevanti o che, per loro natura, siano solo commenti (ecc.), in conformità con quanto più specificamente previsto dalla presente Policy Whistleblowing al paragrafo 2;
- **verificare la completezza del contenuto della segnalazione**; quando possibile, CM richiederà direttamente le integrazioni necessarie (indagine preliminare);
- **verificare l'esatta natura delle accuse** al di là di quanto espresso nella segnalazione, quando la segnalazione è rilevante e completa;
- **assegnare il livello di sensibilità alla segnalazione rilevante** ed eventualmente rimandarla alla relativa procedura di gestione;
- **elaborare il Modulo di Profilazione del Caso** (vedi Appendice 3) se la segnalazione è rilevante, per poter avviare ed organizzare le indagini o la decisione.

→ La funzione di Compliance potrebbe **considerare irrilevante una segnalazione** in questa fase, quando:

- il suo contenuto sia offensivo o generico senza la possibilità di ottenere delucidazioni;
- la segnalazione sia illeggibile, deteriorata, espressa in una lingua veicolare in modo talmente impreciso da impedirne la comprensione;
- sia evidentemente una vertenza di lavoro di carattere personale;
- riguardi un conflitto sul lavoro e nelle relazioni gerarchiche che non si sia presentato coi tratti della minaccia, della corruzione, della frode, della molestia o della molestia sessuale o della violazione di altre norme e policy specifiche;
- sia già stato diffuso pubblicamente;
- riguardi l'insoddisfazione sui servizi;
- sia un fatto al di là del controllo e responsabilità di EMERGENCY, **a meno che** non si tratti di un **incidente relativo a SEAH** in altre ONG internazionali o locali **in missioni dove EMERGENCY siede nei cluster o partecipi agli PSEAH Network**.

! Per le segnalazioni su violazione della Policy PSEAH, è sempre obbligatorio procedere ad indagare, indipendentemente dalla consistenza delle informazioni contenute nella prima segnalazione e dal consenso della persona sopravvissuta ad utilizzarne la testimonianza, utilizzo che resta escluso in assenza di consenso.

→ **Una segnalazione irrilevante per la Compliance**, potrà essere riferita (nei limiti di quanto consentito dagli obblighi di riservatezza) **ad altre funzioni competenti** di EMERGENCY, quando:

- si tratti di una vertenza di lavoro o di un conflitto nell'ambiente di lavoro o nelle relazioni gerarchiche o di rendimento lavorativo;
- si tratti di insoddisfazione rispetto a servizi ausiliari (come la mensa, la lavanderia e similari);
- sia, per sua natura, semplicemente un commento;
- sia, per sua natura, una richiesta di informazioni o di orientamento su materie diverse dagli standard legali, etici e di integrità.

Nei casi sopra descritti, la segnalazione sarà indirizzata dalla funzione di Compliance sotto il dipartimento rilevante e gestita secondo le procedure ivi previste e la funzione di Compliance informa il segnalante delle ragioni del rinvio.

→ Nella **fase di profilazione della segnalazione**, chi abbia ruolo di Compliance Manager può cercare di ottenere ulteriori sommarie informazioni che siano necessarie a delineare la rilevanza o la gravità della condotta segnalata, al fine di decidere appropriatamente se la questione segnalata sia da considerarsi irrilevante e/o da trasmettersi sotto altra procedura o, invece, sotto quale grado di sensibilità e delle procedure di Compliance ricada (*si veda la tavola sotto nel par. 4.8*).

A questi fini, tutto il personale e i collaboratori devono garantire il massimo grado di collaborazione con la funzione di Compliance ad EMERGENCY, di modo che la funzione Compliance possa correttamente qualificare la segnalazione ricevuta. Qualsiasi forma di riluttanza, dilazione



ingiustificata, ostruzionismo od opposizione a fronte delle richieste della funzione di Compliance è da considerarsi una condotta gravemente scorretta e potrà essere oggetto di sanzione disciplinare, ove opportuno.

Nel rispetto del principio di riservatezza, la funzione di Compliance non potrà esprimere quali siano le ragioni che danno luogo alla richiesta di informazioni, né la persona eventualmente contattata potrà condividere con altre persone di aver ricevuto una richiesta di informazioni dalla funzione di Compliance, né il loro oggetto.

Il/la Compliance Manager e/o il/la Complaint Reporting Officer hanno la facoltà di contattare chi abbia segnalato, in modo da poter integrare le informazioni necessarie o escludere che si tratti di un caso già gestito attualmente o in precedenza. A questi fini, per accertarsi dei fatti riportati, si potrà anche richiedere un colloquio informativo o una dichiarazione.

Da questo momento, CM e CRO informano chi segnala del diritto di farsi assistere da una persona di propria fiducia, secondo propria preferenza. Qualora chi segnala decida di farsi assistere da una persona di fiducia che non sia il proprio legale, questa persona dovrà firmare *l'Accordo di Riservatezza*.

In questa fase la traduzione può rivelarsi determinante a comprendere la segnalazione stessa, le eventuali prove allegate o per qualificare sotto quale grado di sensibilità ricada la questione segnalata.

La traduzione può essere esperita con risorse interne oppure tramite servizi esterni.

La traduzione esperita con risorse interne può avvalersi di personale di EMERGENCY madrelingua, preferibilmente tra chi rivesta il ruolo di HR Officer nel Paese quando presenti, e con una buona conoscenza della lingua inglese. Qualora non sia raccomandabile coinvolgere chi rivesta ruoli di HR Officer nel Paese – ossia quando si dubiti della loro neutralità, della presenza pregiudizi, di conflitti di interesse o in ragione di altri rischi, etc. – o questo ruolo non sia assegnato nel Paese, ci si potrà avvalere di altro personale madrelingua per questo compito. Chi si veda assegnato il compito di traduzione dovrà precedentemente firmare *l'Accordo di Riservatezza* corredato dalla *Clausola sull'Assenza di Conflitto di Interessi* specificatamente per il caso in oggetto.

Le traduzioni affidate all'esterno saranno necessarie solo quando nessuna risorsa interna potrà essere utilizzata a questi fini. Chi offra il servizio di traduzione dovrà firmare *l'Accordo di Riservatezza* corredato dalla *Clausola sull'Assenza di Conflitto di Interessi* e garantire gli standard di protezione dei dati, sempre che questo fornitore rispetti i minimi standard professionali per esperire il servizio. L'affidamento della traduzione all'esterno è da considerarsi opzione residuale dunque, poiché può ritardare la procedura di gestione della segnalazione e porre rischi maggiori alla riservatezza, dato che sia CM che CRO, prima che la traduzione sia finalizzata, non sono in grado di stabilire quali dati contenuti nella segnalazione sarebbero da oscurare/minimizzare.

4.7 Misure Protettive e Misure Precauzionali

Le misure protettive, già indicate sopra nel paragrafo 3, includono la protezione dalle conseguenze negative che possano derivare dalla trasmissione di una segnalazione e le misure di assistenza durante la fase delle indagini.

Inoltre, EMERGENCY ha previsto le misure precauzionali, che sono dirette a mitigare i rischi sia per chi segnala e le persone associabili, sia per l'eventuale vittima della condotta (ove poi persona diversa da chi segnala), sia per l'interesse pubblico che per l'integrità di EMERGENCY stessa come ente, e applicabili dal momento dell'ingresso della segnalazione fino alla conclusione del caso (incluso la fase di ammissibilità e profilazione, quella di indagine e quella del procedimento disciplinare).

→ In tal senso, dal momento della ricezione di una segnalazione e una volta che le informazioni sulla rilevanza siano chiare, EMERGENCY, attraverso l'identificazione dei rischi svolta dal CM, valuterà i rischi per:

- l'interesse pubblico (si vedano qui i rischi per la salute pubblica, per la sicurezza ecc.);
- segnalante e persone associabili (quando ne sia nota l'identità)
- testimoni e persone informate;
- la persona segnalata;
- le seconde (come i donatori) e le terze parti.

Dopo l'esercizio di identificazione dei rischi, il Comitato per le Segnalazioni insieme a chi rivesta funzione di Compliance Manager, potrà decidere se prendere misure precauzionali. Queste misure sono ampie e possono essere applicate alla persona segnalata, all'ambiente di lavoro, alle operazioni in corso, alla vittima, ed includere l'allontanamento delle persone coinvolte, la diffusione di allerte, la sospensione delle persone da lavoro, etc. La risposta tempestiva ai rischi è applicazione della responsabilità sociale e ricade sotto l'Obbligo di Protezione ed Assistenza.

! In **caso di segnalazione relativa alla Policy PSEAH**, il modello basato su *victim-centered approach* detta che le misure precauzionali siano applicate prima possibile, in modo da poter interrompere la ripetizione della presunta violazione e da prevenire gli ulteriori danni che si possano cagionare alla persona sopravvissuta, alle persone ad essa associabili e alla comunità servita nel suo insieme.

4.8 Conclusione della fase di profilazione della segnalazione – Notifiche e Reportistica

→ Le conclusioni della **fase di profilazione della segnalazione** possono essere le seguenti:

- **Irrilevante** (leggibilità, rilevanza, tipo di irregolarità, grado di controllo da parte di EMR, etc.)
- **Segnalazione rilevante da trattare/indagare a livello Paese;**
- **Segnalazione rilevante da rimandare alla competenza del Comitato per le Segnalazioni per eventuale indagine** (sempre per segnalazioni relative a PSEAH e Protezione di Minori).

→ **La gravità del caso** viene determinata sulla base di un rating prestabilito (si veda nella tabella qui di seguito l'elenco esemplificativo). Ad ogni grado ivi previsto corrisponde il principale livello/organo responsabile della gestione:

GRADO	CASISTICA	RESP/ CORRESP
0	Conflitti interpersonali nell'ambiente di lavoro e relativi alla gestione del lavoro, rendimento lavorativo, adeguatezza al ruolo assegnato, rispetto degli orari e turni di lavoro; Irregolarità ed inaccuranze minori e non sistematiche nell'attuazione dei protocolli operativi e procedurali; Insoddisfazione e malcontento su servizi ausiliari (mensa, lavanderia, ecc.) <i>senza</i> tratti di potenziale frode/corruzione, minaccia alla salute pubblica etc.; Malcontento su appropriatezza culturale/religiosa, <i>se</i> al di sotto della linea dei discorsi d'odio; Uso del logo di EMERGENCY e del ruolo assegnato per tornaconto personale; Gioco d'azzardo; Comportamento occasionalmente eccentrico rispetto all'ambiente o il contesto di lavoro; Piccole e medie scorrettezze rispetto alla riservatezza professionale.	Livello Paese
1	Vertenze <i>collettive</i> nell'ambiente di lavoro, irregolarità, errori e ritardi che affettino le condizioni di lavoro dignitoso (inclusa la sicurezza sociale) e gli standard di salute e sicurezza; Appropriazione indebita; Malversazione; Uso scorretto dell'attrezzatura; Uso ricorrente di alcolici o narcotici; Molestia (<i>senza tratti sessuali</i>); Linguaggio inappropriato, maleducazione; Discorsi d'odio; Gravi scorrettezze nella riservatezza professionale; Colpa grave nel trattamento di dati personali; Violazioni della Policy Whistleblowing; Mobbing e bossing; Falsificazione di documentazione o informazioni per tamponare ritardi e negligenze interne; Rischio per la salute e sicurezza dell'utenza; Impropria gestione dei rifiuti nelle strutture di EMERGENCY,etc.	Livello Paese/CM
2	Violazione dei <i>core humanitarian standards</i>; Violazione del <i>Do no harm</i>; Vizi nel rilascio di servizi <i>col</i> potenziale di scatenare reazioni violente (sicurezza); Quasi-violazioni della normativa su salute e sicurezza; Riluttanza e vizi ingiustificabili nel condurre un'indagine a livello Paese; Scritture contabili ufficiose o mancanti, col potenziale di creare fondi neri; Uso eccessivo ed ingiustificato di denaro contante; Mancato o viziato lancio di una gara di acquisto e della relativa selezione o acquisti al di fuori della gara svolta senza giustificato motivo debitamente comunicato;	CM/CC

	Assenza di contrattualistica ove richiesta; Gestione pericolosa dei rifiuti sanitari; etc.	
3	Violazione dei Principi Umanitari, PSEAH, Protezione Minori, Corruzione, Frode, Protezione dei dati e Privacy, Violazioni gravi della normativa su salute e sicurezza; Riciclaggio e auto-riciclaggio, Finanziamento del Terrorismo, Favoreggiamento dell'immigrazione clandestina; Traffico di esseri umani, Schiavitù moderna, Infibulazione, Inquinamento ambientale, Attentato alla salute pubblica, Macro-crimine, Notifiche di procedimenti di accusa contro EMERGENCY da parte di autorità internazionali, nazionali e locali, Notifiche di procedimenti giudiziari di carattere privato contro EMERGENCY.	CM/CC+DPO (se rilevante) +OdV

→ **La gravità del caso** è assegnata in base alle informazioni disponibili *prima facie*. Nel corso delle indagini, questo grado può essere rivisto, a seconda delle informazioni aggiuntive e/o delle prove che vengono via via raccolte. Qualora, la gravità del caso diminuisca al punto da rientrare nel solo campo di competenza del Livello Paese, si riporterà la gestione della segnalazione a quel livello. Invece, qualora il grado cresca in modo da collocare la gestione della segnalazione in capo alla sede centrale, le indagini proseguiranno sotto gli organi e le procedure previste per questo livello.

In ogni caso, **la persona segnalante dovrà essere informata** sulle conclusioni raggiunte in questa fase ed i successivi passi, ossia indagine o decisione.

! Quando previsto da obblighi contratti con donatori istituzionali, per alcune categorie di violazioni, **il CM dovrà informare il donatore**, attraverso i canali indicati dal donatore nel contratto, della ricezione di una segnalazione risultata rilevante, esplicitando la categoria di presunta violazione e la localizzazione degli eventi, la procedura che si seguirà per la gestione e la tempistica attesa. Non devono invece essere menzionati dettagli relativi agli specifici fatti espressi nella segnalazione e specificatamente, in nessun modo dovrà essere condivisa l'identità di chi ha segnalato, della persona segnalata, di testimoni o persone informate.

4.9 Tracciamento e Conservazione

→ Quando la segnalazione risulti rilevante, il CM o il CRO deve **elaborare il Modulo di Profilazione del Caso** (vedi Appendice 3) e caricarlo nella Piattaforma di gestione delle segnalazioni, tenendo conto del *principio di minimizzazione dei dati*.

Questo documento inquadra infatti le azioni successive, per la Squadra per le Indagini, la definizione e adattamento continuo del perimetro delle indagini, la pianificazione dei compiti relativi e il continuo tracciamento delle progressioni durante lo svolgimento di tutta la procedura.

Il *Modulo di Profilazione del Caso* deve essere condiviso esclusivamente tramite un link generato a partire dalla Piattaforma di Gestione delle Segnalazioni e **non è permesso scaricare il file su proprio supporto o pc**. Questo link generato dalla Piattaforma è accessibile solo tramite le credenziali degli account autorizzati ad EMERGENCY, disponibile sia ai membri del CC che a quelli della Squadra per le Indagini (quando non affidate all'esterno).

Quando le indagini e/o la decisione pertiene soltanto al livello Paese, i CRO afferenti al Paese aggiornano la Piattaforma di Gestione delle Segnalazioni regolarmente sulla progressione e la conclusione. Soltanto CRO rilevanti e CM hanno accesso a questi documenti ed informazioni.

! La Piattaforma di Gestione delle Segnalazioni traccia e registra, a futura verifica, ogni accesso e le relative azioni compiute in questo ambiente.

- **Le segnalazioni profilate come rilevanti (ed eventualmente indagate),** devono essere mantenute **nel registro per massimo 5 anni dalla chiusura del procedimento di gestione, indipendentemente dalle risultanze.**
- **Per le segnalazioni considerate inammissibili o reindirizzate verso altre procedure,** chi rivesta funzione di CM prepara un rapporto anonimizzato mensile e lo invia al Comitato per le Segnalazioni, per rendere conto delle azioni e decisioni intraprese. In questo caso, il CM mantiene, per i **3 mesi successivi all'invio del rapporto mensile**, i dati personali relativi a queste segnalazioni, in modo separato dagli altri elementi della segnalazione stessa e, se nessuna questione emerge, li cancella definitivamente allo scadere dei 3 mesi.
- Una **sezione separata del registro è dedicata alle segnalazioni ritenute inammissibili e mantenuta per 3 anni in versione anonimizzata**, in modo da costituire base di apprendimento e consentire riferimenti incrociati qualora riemergano questioni simili, mentre CM, col supporto dei servizi IT e del DPO, assicura la non recuperabilità dei dati personali inerenti.

5. PROCEDURA DI INDAGINE INTERNA

5.1 Organi dell'indagine

- Quando ad una segnalazione è assegnato il grado di **gravità da 1 a 3**, quest'ultima può (1) o deve (2-3) essere portata alla competenza del **Comitato per le Segnalazioni**, composto da Presidente e Vicepresidente, in consultazione con Compliance Manager.

- Quando ad una segnalazione è assegnato il grado di **gravità da 0 a 1**, la sua gestione è o può essere attribuita **al livello Paese**, e la maggior parte della procedura continua ad essere svolta dai CRO.

Il **Comitato per le Segnalazioni** in sede (**sensibilità 1-3**), oppure se a livello Paese, **CRO insieme a CM (sensibilità 0-1)**, possono concludere che:

- le informazioni già raccolte e verificate sono sufficienti per decidere sui fatti riportati nella segnalazione – il caso dunque viene deciso in modo definitivo e rinviato al procedimento disciplinare (paragrafo 6 a seguire) ove rilevante;

oppure

- è necessario svolgere ulteriori indagini sui fatti riportati.

- Quando **siano ritenute necessarie ulteriori indagini**, i CRO nel caso in cui la segnalazione debba restare gestita a livello Paese (0-1) o il Comitato per le Segnalazioni, se la segnalazione è affidata alla sua competenza (1-3), col supporto del CM, attivano **la Squadra per le Indagini**.

COMPOSIZIONE SQUADRA INDAGINI	
LIVELLO	MEMBRI
PAESE	HR FIELD MANAGER E COUNTRY DIRECTOR, <i>IN CONSULTAZIONE</i> CON COMPLIANCE MANAGER.
SEDE CENTRALE	RESPONSABILE RISORSE UMANE, REFERENTE UFFICIO LEGALE E COMPLIANCE MANAGER.

! Si avvisa la persona segnalante, la persona segnalata e i testimoni che la segnalazione potrebbe essere gestita da consulenti esterni. In questo caso, i consulenti esterni dovranno rispondere ai requisiti di riservatezza previsti dal Decreto Legislativo n. 24/2023 ed inerenti al GDPR, per cui EMERGENCY richiederà ai consulenti di firmare un apposito Accordo sul Trattamento dei Dati.

- La **Commissione per le Indagini** in sede centrale, è composta almeno dai seguenti membri:
- Presidente;
 - Responsabile del dipartimento F.O.D., che presidia la realizzazione delle attività;
- Presidente dell'Organismo di Vigilanza, per l'analisi di fatti rilevanti rispetto alle prescrizioni del decreto legislativo italiano n°231/2001.

La **Commissione per le Indagini** in sede centrale può decidere di aggiungere altri membri sulle seguenti basi:

- Assenza di conflitto di interessi o noti vizi di mente;

- Rilevanza per materia (programma/amministrazione/finanza/logistica/medica/comunicazione/sicurezza/ etc.)
- Aspetti tecnici emergenti dalla segnalazione.

I membri aggiuntivi possono includere, senza limitazioni, le seguenti funzioni ad EMERGENCY:

- Direzione scientifica, per l'analisi di questioni mediche relative al trattamento dei pazienti;
- DPO, quando i fatti riportati delineano una questione di Protezione dei Dati o violazione della Riservatezza;
- Delegato del datore di lavoro per la salute e sicurezza quando la questione segnalata rileva rispetto alla normativa di salute e sicurezza sul lavoro;
- Specialista in servizi psico-sociali, per i casi relativi a PSEAH;
- Responsabile del Dipartimento Amministrazione, quando una questione è inerente ad aspetti economici o finanziari;
- Responsabile del Dipartimento IT o Specialista di sicurezza digitale.

→ Le funzioni interne e/o le terze parti eventualmente coinvolte nella **Commissione per le Indagini** dovranno firmare l'*Accordo di Riservatezza* comprensivo della *Clausola di Assenza di Conflitto di Interessi*.

→ Chi rivesta funzione di Compliance Manager deve informare sul caso la **Commissione per le Indagini**, al termine della procedura di indagine, attraverso il *Report Finale di Indagine* (Appendice 6), anonimizzando tutti i dati personali che non siano essenziali alla decisione, e comunque segretando l'identità di segnalante e vittime – nonché delle informazioni che consentirebbero di risalirvi - quando non sussista il loro consenso alla rivelazione.

→ Qualora il caso sia pronto per essere deciso a prescindere da ulteriori indagini, la **Commissione per le Indagini** viene informata dal Compliance Manager attraverso il *Modulo di Profilazione del Caso*, anonimizzato di tutti i dati personali non essenziali alla decisione sul caso, e comunque segretando l'identità di segnalante e vittime – nonché delle informazioni che consentirebbero di risalirvi - quando non sussista il loro consenso alla rivelazione

! È severamente proibito scaricare i file condivisi dal Compliance Manager nei supporti personali, rimuovere le password da questi file, condividere e trasmettere questi file al di là dei membri della Commissione per le Indagini e delle altre persone autorizzate a gestire questa procedura.

La **Squadra per le Indagini a livello Paese** deciderà sulle risultanze delle indagini e vidimerà la decisione con il Compliance Manager in sede centrale che, ove ne ricorrano i presupposti, potrà notificare il senior management di rilevanza.

5.2 Ruoli Chiave e Responsabilità connesse

La **Squadra per le Indagini** deve:

- stabilire il *piano di indagine*, e tracciare tutte le fasi progressive nel *Modulo di Profilazione del Caso* (Annex 4);
- **!** trattenersi dall'indagare le opinioni politiche, culturali, le preferenze e le credenze religiose della persona segnalata e/o di chi segnala, così come di ogni altro aspetto personale che possa emergere nelle operazioni dell'indagine svolte su attrezzatura di lavoro, posta e comunicazioni, messaggistica, e similari che sia irrilevante rispetto alla verifica dei fatti riportati;
- **!** proteggere la riservatezza durante tutto il processo;
- evitare di notificare/informare altre funzioni o persone, a meno che non si renda necessario per l'applicazione delle misure precauzionali e sempre che la necessità sia stata verificata da chi rivesta funzione di Compliance Manager che eventualmente si occuperà di esperire le relative comunicazioni;
- procedere tempestivamente e rispettare la scadenza di massimo 2 mesi dalla ricezione della segnalazione (per segnalazioni inerenti PSEAH la scadenza raccomandata è di massimo 2 settimane dall'acquisizione della segnalazione)
- **!** tracciare tutte le fasi progressive, le acquisizioni e le risultanze;
- concludere rapidamente, per iscritto e in modo completo e motivato, attraverso il *Rapporto Finale di Indagine*.

La Commissione per le Indagini in sede centrale dovrà:

- **!** riunirsi prontamente alla convocazione del Compliance Manager;
- apprendere e valutare velocemente le risultanze e le conclusioni dell'indagine;
- decidere le misure derivanti (se ne discendano);
- **!** redigere una minuta.

5.3 Misure Protettive e Misure Precauzionali

Vedi paragrafo 4.7 sopra.

5.4 Notifiche

Una volta che la decisione da impartire al caso è stata raggiunta, il Compliance Manager per la sede centrale o il CRO per il livello Paese, dovranno prontamente notificare il raggiungimento delle conclusioni sul caso:

COMUNICAZIONE DELLE CONCLUSIONI DELL'INDAGINE	
→ QUALSIASI CONCLUSIONE DEL PROCEDIMENTO	
DESTINATARI	CONTENUTO E MODALITA'

Persona segnalante di cui si conosca il contatto	i principali tratti della decisione (<i>il caso non sussiste, mancanza di prove, innocenza della persona segnalata, rinvio al procedimento disciplinare o la combinazione di due o più di queste formule</i>) la lista dei carichi definitiva; le fasi previste a seguire; la tempistica assicurando il rispetto del principio di riservatezza
Persona segnalata di cui si conosca il contatto	quando sentita durante l'indagine
Donatori che siano stati precedentemente informati dell'emersione di un caso ammissibile	secondo gli obblighi contrattuali ed i relativi strumenti con questi stabiliti
Senior manager precedentemente contattati in merito a misure di protezione o precauzionali	relativamente alla rimozione o continuazione delle suddette misure
→ SE RINVIO AL PROCEDIMENTO DISCIPLINARE – LIVELLO SEDE CENTRALE	
+ persona responsabile presso il Dipartimento Risorse Umane incaricata di predisporre il procedimento disciplinare	l'estratto del <i>Verbale della Commissione per le Indagini</i> sarà condiviso tramite link generato dalla Piattaforma di Gestione delle Segnalazioni
+ persona segnalante di cui si conosca l'identità e ai testimoni,	acquisirne l'eventuale consenso alla rivelazione della loro identità nel corso del procedimento disciplinare quando i carichi affondino prevalentemente nelle loro dichiarazioni.
→ SE RINVIO AL PROCEDIMENTO DISCIPLINARE – LIVELLO PAESE	
+ Compliance Manager	ai fini di pre-verifica della decisione raggiunta
+ alla persona segnalante di cui si conosca l'identità e ai testimoni	acquisirne l'eventuale consenso alla rivelazione della loro identità nel corso del procedimento disciplinare quando i carichi affondino prevalentemente nelle loro dichiarazioni.

Ogni ulteriore notifica che sia ritenuta necessaria secondo le specifiche del caso, dovrà essere preventivamente discussa con il Comitato per le Segnalazioni in consultazione con il DPO e formalmente approvata prima della sua esecuzione.

5.5 Conservazione

Le regole di conservazione variano a seconda delle conclusioni raggiunte sul caso.

- Ove vi sia chiusura del caso **perché il caso non sussiste**, si prevede la conservazione delle **sole informazioni essenziali all'apprendimento con l'anonimizzazione** e la cancellazione definitiva di ogni prova raccolta. Le informazioni essenziali sono mantenute in una sezione separata del registro nella Piattaforma per la Gestione delle Segnalazioni **per 1 anno** e formeranno i contenuti della relazione annuale della funzione di Compliance al Consiglio Direttivo.
- Qualora il procedimento si concluda **con assoluzione** l'intero dossier del caso è anonimizzato e mantenuto in una sezione separata del registro sulla Piattaforma di Gestione delle Segnalazioni **per 1 anno**, ai soli fini di apprendimento.
- Ove vi sia chiusura del caso **per mancanza di prove**, il dossier del caso sarà mantenuto in una sezione separata del registro sulla Piattaforma per la Gestione delle Segnalazioni **per 3 anni**, specialmente quando il caso fosse relativo a PSEAH, dato che nuove informazioni potrebbero essere reperite successivamente o la ripetizione della condotta potrebbe farne emergere di nuove a valere anche sul caso precedentemente indagato.
- Ove il caso **sia rinviato a procedimento disciplinare** la conservazione del dossier segue la regola stabilita del Decreto Legislativo n. 24/2023, i.e. la documentazione **sarà mantenuta per 5 anni dalla notifica delle conclusioni** del procedimento disciplinare, con le modalità specificamente previste dalla normativa anzidetta.
- La **combinazione delle formule** sopra per uno specifico caso, comporterà un trattamento di **conservazione differenziato per le relative parti del caso**, mantenute ognuna separatamente nella relativa sezione del registro sulla Piattaforma per la Gestione delle Segnalazioni.

6. PROCEDIMENTO DISCIPLINARE (SANZIONI)

Il procedimento disciplinare radica nel diritto dei diritti umani e nel diritto del lavoro.

Secondo il sistema predisposto da EMERGENCY e descritto sopra, il procedimento disciplinare **segue alla decisione di rinvio al procedimento disciplinare** della Commissione per le Indagini in sede centrale o a quella della Squadra per le Indagini a livello Paese.

Nessuna violazione segnalata o rilevata può essere sanzionata senza esperire la fase del procedimento disciplinare.

! Le **sanzioni applicabili** nel procedimento disciplinare possono essere solo quelle:

- permesse dal diritto dei diritti umani (e del *lavoro dignitoso*, in particolare),
- permesse dalla normativa nazionale sul lavoro ed entro i suoi limiti,
- incluse nel sistema sanzionatorio stabilito per l'Organizzazione e diffuso tra il personale, i partner e i fornitori prima che i fatti oggetto di segnalazione siano occorsi.

6.1 Misure conseguenti

Il procedimento disciplinare prende avvio dal *Verbale della Commissione per le Indagini in sede centrale* o dal *Report Finale di Indagine della Squadra per le Indagini a livello Paese*, derivando dalle conclusioni contenute in questi documenti le misure conseguenti.

Il procedimento disciplinare deve essere **eserito tempestivamente, entro massimo 14 giorni dalla comunicazione delle decisioni prese** dalla Commissione per le Indagini in sede centrale o dalla Squadra per le Indagini a livello Paese, e in quest'ultimo caso, come anche validato da Compliance Manager.

Le sanzioni applicabili sono quelle specificatamente previste **in conformità con il sistema disciplinare interno dell'Associazione ed il diritto nazionale, come previsto in particolare dal MOG ex D.Lgs 231/2001 e dal Regolamento Interno adottato in data 22 gennaio 2019**

Le sanzioni sono applicate in modo **motivato** e secondo **i seguenti criteri**:

- sanzione prestabilita dalle policy interne, applicata automaticamente, quando prevista (per es., PSEAH);
- oggettiva gravità della condotta entro un determinato spettro (natura della violazione, qualificazione data dalle norme o dal Codice di Condotta), anche considerando la dimensione e l'impatto del danno causato o potenziale;
- gravità soggettiva della violazione (negligenza, colpa grave, dolo);
- se la violazione è commessa o tentata, ove la differenza sia rilevante (escluso per PSEAH);
- sussistenza di cause scriminanti o di fatti che ragionevolmente determinano una attenuante (discolpa rispetto all'atto/omissione/condotta, stato di bisogno/necessità, inganno, ravvedimento, etc.);
- sussistenza di circostanze aggravanti per la persona segnalata (ruolo, specializzazione, reiterazione, etc.).

Le **misure precauzionali** eventualmente applicate alla persona segnalata prima di questo momento, possono essere continuate, rimosse o considerate sufficienti ad assorbire la sanzione prevista per la violazione da comminarsi in questa fase.

Le **misure di protezione** eventualmente applicate prima a chi abbia segnalato e alle persone associabili, possono essere continuate, rimosse, aumentate o diminuite a seconda delle risultanze di questa procedura e di eventuali cambiamenti avvenuti nelle circostanze del caso (analisi dei rischi e aggiornamento).

La persona delegata per il procedimento disciplinare:

- elabora **le comunicazioni ufficiali alla persona segnalata sulle misure da applicarsi**, corredate da **chiaro e motivato riferimento alla condotta, azione od omissione riscontrate** nei fatti, ed ai criteri utilizzati per soppesare la sanzione da applicarsi;
- **reperisce la firma sulla comunicazione ufficiale** da parte di chi, nell'Associazione, detenga i poteri gerarchici e sanzionatori nei confronti della persona segnalata;
- **informa di conseguenza la persona segnalata.**

6.2 Notifiche

- Chi rivesta funzione di Compliance Manager è informato/a della finalizzazione del procedimento disciplinare e delle misure adottate.
- Quando le violazioni ricadano sotto nell'ambito del MOG e l'OdV non sia stato coinvolto né dalla Commissione per le Indagini né durante il procedimento disciplinare, allora la persona delegata per il procedimento disciplinare deve notificare i membri dell'OdV.
- CM o CRO (se a livello Paese), **notifica la persona segnalante** sulla conclusione del caso, con le sue risultanze (sanzionato/non sanzionato), la tempistica di applicazione e le funzioni responsabili per ulteriori prese in carico e la tempistica relativa. **! I dettagli sul tipo di sanzione applicato** alla persona segnalata non saranno condivisi con la persona segnalante, a meno che quest'ultima non sia anche la vittima diretta di abuso, molestia o sfruttamento da parte della persona segnalata.

6.3 Conservazione

I termini di conservazione sono stabiliti direttamente dalla normativa.

CASISTICA CONSERVAZIONE		
CASISTICA	TERMINI	RESPONSABILE TRATTAMENTO
CASO NON RIMESSO AD AUTORITA' GIUDIZIARIA	5 ANNI DALLA NOTIFICA DI CONCLUSIONE ALLA PERSONA SEGNALANTE	COMPLIANCE MANAGER UFFICIO RISORSE UMANE RILEVANTE
CASO RIMESSO AD AUTORITA' GIUDIZIALE	SECONDO LA DURATA DELLA CONTROVERSIA LEGALE E SUE REGOLE	UFFICIO RISORSE UMANE

MISURE DISCIPLINARI APPLICATE AL PERSONALE DI EMERGENCY	5 ANNI DALLA NOTIFICA DI CONCLUSIONE ALLA PERSONA SEGNALANTE	UFFICIO RISORSE UMANE RILEVANTE
MISURE APPLICATE A CONSULENTI E FORNITORI	DAI 3 AI 5 ANNI A SECONDA DELLA GRAVITA' DELLA SANZIONE COMMINATA	DIPARTIMENTO RILEVANTE

7. FORMAZIONE E DIFFUSIONE

Affinché questa Policy Whistleblowing possa avere un impatto effettivo sulla prevenzione di condotte scorrette o illecite, tutto il Personale di EMERGENCY deve essere edotto e formato sui relativi contenuti.

- A tal fine, questa Policy dovrà essere **allegata ad ogni contratto di lavoro con il personale**. Il Personale attuale e quello futuro dovranno impegnarsi a leggere attentamente questa Policy Whistleblowing e dichiarare di aver letto e compreso i suoi contenuti e di aderire ai termini e le condizioni qui stabilite.
- **Riferimenti a questa Policy Whistleblowing saranno condivisi con le attuali e le future controparti contrattuali** prima che si perfezionino gli accordi. Le controparti contrattuali dovranno dichiarare negli accordi con EMERGENCY, di aver preventivamente letto la Policy Whistleblowing e che vi aderiranno.
- **I partner**, sia progettuali che attuativi (ossia che partecipino ad un consorzio di applicazione di un intervento), almeno quando l'intervento sia finanziato da un donatore istituzionale, dovranno seguire una sessione formativa su questa Policy Whistleblowing, a meno che non siano in grado di provare di averne una propria e che sia stata propriamente diffusa.

Il piano formativo su questa Policy Whistleblowing e le relative procedure attuative in EMERGENCY, sono basati **sull'identificazione dei diversi bisogni formativi** a seconda delle diverse funzioni svolte dal personale, dai compiti relativi e, secondo la prospettiva di compliance, della potenziale esposizione e contatto diretti con l'utenza.

La tabella seguente indica, per ogni categoria di staff rilevante, il tipo e la durata nonché la frequenza della formazione:

Categoria Personale	Tipo di formazione	Frequenza
Complaint Reporting Officer(s)	Formazione Formatori 12 ore	All'inserimento e ogni 18 mesi o anche prima qualora intervengano cambiamenti nella struttura o nella Policy Whistleblowing

Manager che siano o possano essere chiamati/e a sedere nella Commissione per le Indagini o ad occuparsi del procedimento disciplinare	Formazione avanzata 6 ore	All'inserimento e ogni 18 mesi o anche prima qualora intervengano cambiamenti nella struttura o nella Policy Whistleblowing
Personale "in prima linea" (nelle strutture di EMR, o dove i servizi sono rilasciati)	Formazione media 4 ore	All'inserimento e ogni 12 mesi o anche prima qualora intervengano cambiamenti nella struttura o nella Policy Whistleblowing
Manager intermedi/e	Formazione media 3 ore	All'inserimento ed ogni 12 mesi
Altro tipo di personale	Formazione base 2 ore	All'inserimento e ogni 18 mesi o prima ogni volta che questa Policy Whistleblowing è rivista.

Esterni	Tipo di formazione	Frequenza
Partner attuatori o senior manager e CRO(s) dei soggetti finanziati	Formazione media 3 ore	Secondo la tempistica prevista nel MoU
Consulenti e fornitori	Sessione informativa	All'inizio e secondo la tempistica stabilita nel contratto

I moduli formativi potrebbero anche **essere rilasciati tramite strumenti e procedure digitali**, sempre che vi siano gli strumenti adeguati a tracciare l'effettiva presenza e i/le discenti possano interagire in tempo reale con chi somministra la formazione.

I moduli formativi dovranno essere **somministrati da personale specializzato nelle materie** di riferimento e/o dal Compliance Manager. A livello Paese, anche chi rivesta funzione di Complaint Reporting Officer potrà somministrare i moduli, quando abbia già ricevuto la formazione per formatori.

Almeno una volta, nel corso del rapporto lavorativo con EMERGENCY, ogni membro del personale avrà ricevuto la formazione in presenza.

! Le formazioni dovranno essere documentate con apposita agenda sui contenuti, la data e l'orario, e il tracciamento della presenza (schede presenza, lista partecipanti, dichiarazioni ecc.) Questi strumenti di tracciamento sono mantenuti dalla funzione di Gestione del Personale, in sede centrale

o a livello Paese. **!** Tutte le persone che debbano ricevere la formazione devono essere informate che le **loro identità potrebbero essere condivise con i donatori istituzionali e gli auditor** di seconda parte quando richiesto, sulla base di specifici obblighi contrattuali.

- Chi rivesta la funzione di Compliance Manager, con il supporto di Complaint Reporting Officer per il livello Paese, dovrà **mantenere un registro parallelo**. Questo registro indicherà, per ogni sessione formativa, il tipo di formazione rilasciato, il tipo e numero di discenti, l'agenda della formazione, la durata, il giorno e l'orario della somministrazione, il luogo, il metodo e chi sia a rilasciare la formazione, chi detenga la documentazione a supporto e il tipo di documentazione. La conservazione di queste informazioni è di **3 anni dal momento del completamento** della formazione.

8. MONITORAGGIO E APPRENDIMENTO

Il **principio di accountability** richiede che la funzione di Compliance **monitori regolarmente** l'attuazione della presente Policy Whistleblowing.

- Come indicato sopra, **la funzione di Compliance ha il compito di mantenere un registro aggiornato delle segnalazioni**, registrando tutti i casi che siano stati considerati inammissibili, rinviati ad indagine ed eventualmente sfociati in procedimento disciplinare. Questo registro costituisce lo **strumento di base per il monitoraggio della performance** di EMERGENCY nella gestione di queste procedure.
- Almeno una volta l'anno, il/la Compliance Manager renderà conto **al Consiglio Direttivo di EMERGENCY delle risultanze dell'attività di Compliance** sulla base dei dati del registro e dei sondaggi periodici, di modo da fornire le informazioni necessarie per il miglioramento del sistema di Compliance di EMERGENCY, per l'attuazione di piani di audit interno e fissare gli obiettivi in termini di integrità e compliance.
- Una copia di questo rapporto annuale dovrà essere recapitata anche **all'Organismo di Vigilanza**.

Appendice 1

Scheda numeri Hotline

DESTINATARI:

TUTTI



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023
Rev. 1 del 24/10/2023
Pagina 40 di 80

PAESE	NUMERO HOTLINE	DATA ATTIVAZIONE
AFGHANISTAN		06/2022
KRI	<i>in compilazione</i>	11/2022
ITALIA	<i>in compilazione</i>	17/12/2023
SIERRA LEONE	<i>in compilazione</i>	17/12/2023
SUDAN	<i>in compilazione</i>	17/12/2023
UGANDA	<i>in compilazione</i>	17/12/2023

Appendice 2

Collocazione Complaint Box

DESTINATARI:

TUTTI



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 42 di 80

PAESE	SITO	COLLOCAZIONE
AFGHANISTAN	KABUL HOSPITAL	<i>in compilazione</i>
	ANABAH HOSPITAL	<i>in compilazione</i>
	LASHKAR GHA HOSPITAL	<i>in compilazione</i>
	FAP..	<i>in compilazione</i>
	FAP...	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 43 di 80

PAESE	SITO	COLLOCAZIONE
KRI	SULEYMANYA REHABILITATION CENTRE	<i>in compilazione</i>

PAESE	SITO	COLLOCAZIONE
ITALIA	UFFICIO DI MILANO	ANTI BAGNO 2° PIANO DX ANTI BAGNO 4° PIANO SX
	UFFICIO DI ROMA	ANTI-BAGNO
	UFFICIO DI VENEZIA	<i>in compilazione</i>
	LIFE SUPPORT	A BORDO
	NESSUNO ESCLUSO – AMBULATORIO...	<i>in compilazione</i>
	NESSUNO ESCLUSO AMBULATORIO....	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>

PAESE	SITO	COLLOCAZIONE
SIERRA LEONE	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>
	<i>in compilazione</i>	<i>in compilazione</i>

PAESE	SITO	COLLOCAZIONE
SUDAN	SALAM CENTER – KHARTOUM	<i>in compilazione</i>
	PORT SUDAN	<i>in compilazione</i>



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023
Rev. 1 del 24/10/2023
Pagina 44 di 80

	NYALA	<i>in compilazione</i>
PAESE	SITO	COLLOCAZIONE
UGANDA	ENTEBBE HOSPITAL	<i>in compilazione</i>
	OFFICE	<i>in compilazione</i>

Appendice 3

Modulo di Profilazione Caso

DESTINATARI:

MEMBRI DELLA SQUADRA DI INDAGINE

COMPLIANCE MANAGER



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 46 di 80

MODULO DI PROFILAZIONE DEL CASO - 2023

A SUPPORTO DELL'INDAGINE E DELLE COMUNICAZIONI INERENTI

- QUESTO FILE DEVE ESSERE UTILIZZATO SOLTANTO TRA I MEMBRI DELLA SQUADRA DI INDAGINE E CHI SIA AUTORIZZATO E CONDIVISO SOLO TRA LORO, TRAMITE LA PIATTAFORMA DI GESTIONE DELLE SEGNALAZIONI, TRAMITE APPOSITO FOLDER E LINK.
- NELL'IDENTIFICARE LE ACCUSE O LE VIOLAZIONI PER FAVORE RIFERIRSI ALL'ULTIMA VERSIONE DELLE POLICY, NORME O DEL CODICE ETICO E/O DI CONDOTTA.

Caso con codice n°	
Data di ricezione o di redazione della segnalazione:	
Primo ricevente della segnalazione:	
Personale eventualmente implicato	Nome: Ruolo:
Luogo di lavoro della persona implicata:	
Luogo dei fatti segnalati (se conosciuto):	
Data di attivazione della Squadra di Indagine:	
Accuse/Violazioni secondo la segnalazione:	1. [Allegation #1] 2. [Allegation #2] 3. [Allegation #3] 4. [Allegation #4]
Scadenza per il completamento dell'indagine:	
Data di redazione del piano di indagine:	



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023
Rev. 1 del 24/10/2023
Pagina 47 di 80

Nome e ruolo dei membri della Squadra di Indagine			
Piano di indagine:	1. Azione	Spiegazione	Data per il completamento
Breve descrizione dei contenuti della segnalazione iniziale insieme con informazioni di contesto			
Bozza delle domande che devono guidare l'indagine rispetto a fatti rilevanti			
Persone da udire e motivi per l'intervista	Nome	Tipo e scopo di colloquio	Data



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 48 di 80

Aggiornamento delle informazioni in base alla progression dell'indagine			
Data dell'analisi conclusiva della Squadra di Indagine			
Data della redazione del Rapporto Finale di Indagine:			
Persone con cui è stato condiviso il Report Finale di Indagine e modalità della condivisione:			
Misure di precauzione/protezione da attuare e/o mantenere:			
Data di applicazione delle misure derivanti:			

Appendice 4

Nota Informativa sulla gestione della strumentazione di lavoro.

DESTINATARI:

PERSONALE



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA



→ Estratto del Regolamento Interno - Versione 1.4 - del 22 gennaio 2019:

10 – COMPUTER AZIENDALE – POSTA ELETTRONICA - INTERNET

L'utilizzo di Internet e delle e-mail è previsto per soli scopi aziendali.

Si richiamano a questo proposito le procedure contenute nel protocollo "**Sicurezza e regolamento interno privacy**".

Il personale è tenuto a utilizzare **con discrezione e non a fini personali** gli strumenti che Emergency mette a sua disposizione per lo svolgimento delle proprie mansioni, quali, a titolo esemplificativo, computer (fisso e/o portatile), telefono, telefono cellulare, indirizzi mail, etc.

Gli indirizzi mail del personale di Emergency sono raggruppati anche in diverse liste di distribuzione (ad es., per il solo staff della sede di Milano, per quello della sede di Roma, ecc.).

La creazione delle liste di distribuzione è stata prevista per regolare e razionalizzare l'uso delle liste generali o di gruppo, anche al fine di controllare il volume di traffico che comportano sui sistemi informatici interni gli invii di messaggi a un grande numero di destinatari e la conseguente effettiva necessità di utilizzo di tale forma di comunicazione.

L'invio di messaggi attraverso tali liste è consentito solo se preventivamente autorizzato dal proprio Responsabile.

Appendice 5

Informativa sulla riservatezza

DESTINATARI:

SEGNALANTE, PERSONA SEGNALATA, VITTIMA, FACILITATORE



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

	WHISTLEBLOWING POLICY	Ver.1 del 24/10/2023 Rev. 1 del 24/10/2023 Pagina 52 di 80
---	------------------------------	--

in compilazione per aggiornamento Nota Informativa

Appendice 6

Modulo di Report Finale di Indagine

DESTINATARI:

MEMBRI DELLA SQUADRA DI INDAGINE



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 54 di 80

Report Finale di Indagine

Informazioni Generali	Membri della Squadra per le Indagini sui fatti:
	Data di inizio dell'indagine:
	Istruzioni:
	Ragioni dell'indagine:

Processo di indagine	Il procedimento di indagine:
	Persone intervistate:



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 55 di 80

Altre fonti di prova:

Conclusioni	Fatti sostanzati
	Fatti non sostanzati o non sostanziabili:
	Fattori di mitigazione:
	Fattori di aggravamento:
	Altre informazioni rilevanti:
	Misure precauzionali/protettive:
	Debolezze organizzative riscontrate nella genesi dell'incidente e sue potenziali cause:



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 56 di 80

Misure discendenti	Misure contro la persona segnalata:
	Raccomandazioni in risposta alle debolezze organizzative riscontrate:
	Data:

Documentazione a supporto del procedimento di indagine	
---	--

Appendice 7

Sistema Sanzioni (MOG)

DESTINATARI:

PERSONALE, FORNITORI E PARTNER (E LORO PERSONALE)



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

in compilazione per aggiornamento MOG in corso.

Appendice 8

Procedura di Indagine

DESTINATARI:

MEMBRI SQUADRA DI INDAGINE, SEGNALANTE, VITTIMA,
PERSONA SEGNALATA, MEMBRI DELLA COMMISSIONE PER
L'INDAGINE



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

1. Indagine

→ L'indagine è il lavoro di approfondimento svolto sulla condotta, sull'azione o l'omissione **con lo scopo di:**

- ✓ **verificare le notizie** su potenziali violazioni di leggi, policy, procedure o regolamenti interni, in modo da determinare, e fin dove possibile prevenire, la commissione di fatti che possano danneggiare l'interesse pubblico, il personale, i diritti individuali o l'integrità di EMERGENCY e che possano attivare conseguenze legali o danni reputazionali a carico dell'Associazione;
- ✓ **disporre tempestivamente i rimedi.**

→ Solitamente le indagini sono esperite **rispetto a:**

- ✓ **Cosa;**
- ✓ **Dove;**
- ✓ **Quando;**
- ✓ **Chi;**
- ✓ **Come;**
- ✓ **Perché.**

→ Le attività di indagine possono avvenire **attraverso:**

- ✓ **Corporate intelligence:** per es. ricerca su database disponibili o fonti pubbliche o ad accesso non condizionato (come i social media);
- ✓ **Analisi documentale:** su documenti interni rilevanti;
- ✓ **Analisi forensi:** ricerca sui dispositivi (come pc, telefono, tablet, portatile, server, etc.) assegnati alla persona segnalata col fine di individuare prove sulle accuse (quindi, email, documenti, testi, etc.)
- ✓ **Interviste a persone chiave:** a chi segnala, a testimoni, a persone informate, alla persona segnalata, etc.

→ Il **piano di indagine**, contenuto nel **Modulo per la Profilazione del Caso (Appendice 3)** stabilisce quali misure siano da intraprendere per indagare i fatti, le azioni, le omissioni, chi coinvolgere e quando. Il piano di indagine è aggiornato al progredire delle indagini, sia per quanto riguarda le azioni da svolgere che per la relativa tempistica.

! Preferibilmente le audizioni sono videoregistrate, quando vi sia il consenso della persona intervistata.

AUDIZIONI/INTERVISTE - REGOLE

CHI/COSA	REGOLA	RESPONSABILE
→ segnalante, vittima, testimoni, persone informate e persona segnalata	✓ convocazione per iscritto sempre quando <u>sia possibile</u>, rispettando la minimizzazione dei dati, ✓ <u>contestuale richiesta di consenso</u> alla persona da intervistare per videoregistrare l'intervista, da esprimersi per iscritto. oppure (se convocazione orale): ✓ verifica predisposizione al consenso alla videoregistrazione al momento della convocazione orale. ✓ Al momento dell'avvio dell'intervista, richiedere come prima cosa la conferma del consenso alla videoregistrazione e registrarla in quella sede. X In assenza di consenso da parte della persona intervistata, le audizioni non possono essere videoregistrate. → Se consenso limitato – solo registrazione audio (! la sola registrazione video invece è inutile agli scopi di questa procedura) – e qualora la persona intervistata abbia anche accettato che la sua identità sia conosciuta, all'inizio della registrazione si richiederà alla persona intervistata di declinare le generalità mentre i membri della Squadra per le Indagini specificheranno giorno, ora, luogo di svolgimento dell'intervista. ✓ <u>l'audizione deve avvenire nell'ordine descritto accanto</u> fin dove possibile	CM o CRO

persona segnalata	X Non deve venire a conoscenza delle accuse o delle indagini in corso prima che sia convocata dalla Squadra per le Indagini per intervistarla. X Durante l'intervista le informazioni relative al caso, a chi lo abbia segnalato o alla vittima, ai testimoni o alle persone informate devono essere limitate al massimo (bilanciamento tra diritto di difesa e riservatezza su identità altre persone) → Notifica iniziale: ✓ la Squadra per le Indagini sta verificando un caso di condotta scorretta/illecita; ✓ il processo di cui sopra è nella fase di acquisizione delle informazioni; ✓ la Squadra per le Indagini vorrebbe intervistare la persona segnalata al fine di assumere le informazioni in possesso di quest'ultima; ✓ si richiede il consenso alla videoregistrazione; ✓ la persona segnalata può farsi assistere (interprete, avvocato, rappresentante sindacale, rappresentante del personale, ecc.) che, nel caso, dovrà firmare un Accordo di Riservatezza. → Durante l'intervista (solo dopo aver raccolto tutte le altre informazioni disponibili sui fatti riportati, nonché le eventuali prove, di modo che (a) alla persona segnalata possano essere chiaramente descritti i fatti su cui deve esprimersi e/o (b) si possano raccogliere in questa intervista le prove/le indicazioni chiare/gli elementi circostanziali che effettivamente corroborino o invalidino i fatti di cui la si accusa):	CM, CRO e Membri Squadra per l'Indagine
--------------------------	---	--

	✓ la persona segnalata deve essere informata del tipo di accuse ma, ✗ non dovrà venire a conoscenza dell'identità di chi abbia segnalato o della vittima, né di dettagli che consentano questa identificazione e quella dei testimoni. ✗ Nessuna delle prove e testimonianze raccolte deve essere mostrata per l'esame incrociato, poiché la Squadra per le Indagini sta soltanto cercando di ricostruire i fatti. ✗ La persona segnalata ha il diritto di restare in silenzio in questa audizione.	
persona segnalante e/o vittima	→ SE le accuse si avvalgono prevalentemente delle dichiarazioni di queste persone, allora ✗ chi rivesta funzione di CM o CRO dovrà richiedere motivandolo, il rilascio di consenso libero, esplicito, specifico di queste persone, per poter condividere i contenuti delle relative dichiarazioni. ✗ Se queste persone negano il consenso alla condivisione, le indagini, se basate soltanto su queste dichiarazioni devono concludersi con la <i>chiusura del caso per mancanza di prove</i>, in quanto le dichiarazioni non possono essere utilizzate nel procedimento. → SE le indagini invece abbiano consentito di raccogliere prove ed indizi ulteriori rispetto a quanto contenuto alle loro dichiarazioni: ✗ non sarà necessario utilizzare le relative dichiarazioni nell'audizione della persona segnalata. ✓ in base al principio di riservatezza e alle protezioni dovute a chi segnala e alle	CM o CRO



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 64 di 80

	persone associabili, in questo caso i contenuti delle rispettive dichiarazioni dovranno essere mantenuti segreti.	
--	---	--

→ Il **Modulo di Profilazione del Caso** richiede anche di **definire le domande rilevanti rispetto alle accuse nel caso specifico**, di modo da poter direzionare correttamente gli sforzi investigativi e le risultanze relative.

! Ogni prova ed indizio raccolti, **sia a carico che a discarico**, dovranno essere debitamente registrati e archiviati nel dossier di indagine.

→ Il **dossier di indagine** è **alimentato e mantenuto** da chi riveste funzione di Compliance Manager o di CRO, direttamente sulla Piattaforma per la Gestione delle Segnalazioni sulla cartella dedicata al caso, con accesso limitato, al fine di garantire **l'integrità delle informazioni** raccolte e ricevute attraverso tutto il procedimento.

! Le **segnalazioni di PSEAH** sono indagate secondo questa procedura generale per le indagini **integrata con il "Protocollo per la Gestione di Segnalazioni di PSEAH"** (Appendice 9).

2. Fonti di prova

→ Le fonti di prova possono essere:

- **materiali** (cose, documenti, registrazioni, audio/video, etc.)
- **persone** (testimoni).

Le fonti di prova permettono di derivarne circostanze, fatti, comportamenti, condotte.

! Questa parte della procedura di indagine **pone una serie di complesse interazioni** con altre norme, in particolare con **la normativa del lavoro**, quella **penale** e quella della **protezione dei dati**.

La normativa sulla protezione dei dati in combinato con quella del lavoro, **limita sensibilmente la possibilità del Datore di Lavoro di indagare all'interno di attrezzature e mezzi assegnati** al personale, sia in ossequio al diritto d'opinione, e dunque il divieto di indagare le opinioni del personale, (siano esse politiche, sociali, religiose, etc.) sia al divieto di sottoporre a controllo costante il personale nell'esperimento dei propri compiti di lavoro.

→ **La ricerca** e individuazione di prove **all'interno dei mezzi di lavoro** si può esperire soltanto se:

- ✓ il personale utilizzi normalmente quei mezzi, strumenti, applicazioni e indirizzi per lavoro (il che li qualifica quali ordinari mezzi di lavoro), e
- ✓ il personale sia preventivamente informato sulle implicazioni delle previsioni della protezione dei dati quando si tratti di strumenti, applicazioni e documenti di lavoro (*vedi* Appendice 4)

! In ogni caso, le indagini che si svolgano sui mezzi di lavoro **dovranno evitare di coinvolgere software e supporti esterni, applicazioni, indirizzi, informazioni, documenti, etc. di natura**

personale, che si trovino a coesistere all'interno dell'attrezzatura di lavoro con quelli lavorativi, specialmente quando manchino esplicite e specifiche regole in tal senso per l'utilizzo dei mezzi di lavoro o, se presenti, non prevedano il divieto di uso promiscuo del mezzo, tra utilizzo per lavoro e quello di carattere personale.

Predisporre regolamenti interni sull'uso dei mezzi di lavoro in questi termini, specialmente in riferimento alla protezione dei dati e al possibile accesso del datore a quei mezzi, è fondamentale a garantire che l'estrazione di fonti di prova dai mezzi di lavoro ed il loro utilizzo siano adeguati e legittimi (vedi Appendice 4).

! Si fa presente, infatti, che secondo la normativa sulla protezione dei dati, **il consenso eventualmente rilasciato dal lavoratore/dalla lavoratrice ad accedere ai mezzi di lavoro assegnati, non è sufficiente** a legittimare la procedura.

Il legittimo interesse del Datore di lavoro a proteggere l'integrità dell'ente o l'interesse pubblico ove rilevi, può legittimare l'accesso ai mezzi di lavoro e loro contenuto, **solo dopo che sia emerso il sospetto sulla condotta illecita/scorretta e se il personale è stato preventivamente informato** su come si debba utilizzare la strumentazione di lavoro e le circostanze che potrebbero permettere l'accesso del Datore a quei mezzi (vedi Appendice 4).

→ Il **personale che può accedere** ai mezzi di lavoro della persona segnalata ed estrarre le fonti di prova è (ex Art. 29 GDPR) a) **formalmente autorizzato**; b) **chiaramente istruito su come** procedere e sulla clausola di riservatezza; c) **debitamente formato**.

* Qualora siano coinvolti **consulenti esterni nell'indagine**, questi ultimi dovranno (ex Art. 28 GDPR) a) essere **preventivamente valutati** rispetto alle loro abilità di garantire i requisiti del GDPR; b) **essere nominati Titolari Autonomi** del Trattamento; c) **ricevere chiare istruzioni** sulla procedura operativa da seguire e su come rispettare la riservatezza in questo ambito.

3. Conclusioni dell'indagine

→ L'indagine deve essere **debitamente documentata in tutto il suo corso** dalla **Squadra per le Indagini** e, senza pregiudizio del ricorso all'autorità giudiziaria, può condurre alle seguenti conclusioni:

CONCLUSIONI	
TIPOLOGIA	REGOLE
chiusura del caso perchè il caso non sussiste	l'indagine approfondita sui fatti dimostra che le azioni, omissioni o condotte segnalate non costituiscono violazione di leggi, policy, procedure tra quelle indicate nella Policy Whistleblowing;

chiusura del caso per <i>manca</i>za di prove	l'indagine non è riuscita a trarre sufficienti elementi di prova che giustifichino un procedimento disciplinare;
chiusura del caso per <i>innocenza della persona segnalata</i>	l'indagine ha raccolto sufficienti prove a discolta della persona segnalata;
<i>rinvio del caso al procedimento disciplinare</i>	l'indagine ha riscontrato prove che possono giustificare l'applicazione di sanzioni;
una combinazione delle formule sopra indicate.	

Le conclusioni:

- devono essere per iscritto e debitamente motivate (*vedi* Appendice 6);
- devono predisporre una definitiva lista tecnica dei carichi, basata sulle informazioni raccolte;
- ✓ possono identificare responsabili delle accuse differenti o aggiuntivi rispetto a quelli indicati originariamente;
- ✓ possono rilevare ulteriori violazioni avvenute nel corso dei fatti come ricostruiti e aggiungerle ai carichi originariamente previsti sia contro la persona segnalata che contro le ulteriori persone eventualmente identificate, senza dover aprire un nuovo caso;
- ✓ possono determinare se e quali misure correttive servano per migliorare la capacità dell'Associazione di prevenire, individuare e rispondere a condotte simili in futuro, oltre che tutte le altre raccomandazioni che siano conseguenti al caso e si rendano necessarie;
- quando vi sia rinvio al procedimento disciplinare, dovranno indicare quale sia, secondo il sistema di sanzioni stabilito dall'Associazione ed i criteri per calibrare la sanzione sulle specifiche circostanze del caso.

Appendice 9

Procedura di gestione delle indagini per segnalazioni di SEAH

DESTINATARI:

MEMBRI SQUADRA DI INDAGINE, SEGNALANTE, VITTIMA,
PERSONA SEGNALATA



EMERGENCY
MEDICINA, DIRITTI E UGUAGLIANZA

***Protocol on
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 evolvments 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 have to still or already be 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, even when it deals with a pattern of behaviour**.

→ **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.



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023

Rev. 1 del 24/10/2023

Pagina 77 di 80

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 fallout 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 AND 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
Versione: 1.1		24 Ottobre 2023



WHISTLEBLOWING POLICY

Ver.1 del 24/10/2023
Rev. 1 del 24/10/2023
Pagina 80 di 80

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).