

Linee guida sul whistleblowing di Embracer Group

Adottate dal Responsabile della gestione del personale, Responsabile legale e di governance di Embracer Group il 12 settembre 2023

Riviste il:

Tipo di documento: Linee guida

Versione: 1

Proprietario del documento: Responsabile governance e conformità di Embracer Group

Le presenti Linee guida si applicano alle entità di Embracer Group e a tutti i dipendenti di Embracer Group.

Le presenti Linee guida ampliano e dettagliano la routine e lo strumento di whistleblowing all'interno di Embracer Group. Le linee guida a livello locale possono esistere parallelamente a queste Linee guida per integrarle con i requisiti o i processi legali locali.

In caso di domande sulle presenti Linee guida, contattare:

Responsabile governance e conformità, Responsabile legale di Embracer Group

Linee guida sul whistleblowing di Embracer Group

Sommario

1.	Cronologia delle revisioni	3
2.	Introduzione - cos'è il whistleblowing e perché è importante?	3
3.	Quando segnalare?	4
4.	Come segnalare?	5
5.	Il processo investigativo	6
6.	Tutela e Privacy	7
7.	Appendici	9

1. Cronologia delle revisioni

Data	Versione	Descrizione	Autore
2023-09-12	1.0	Prima versione adottata da Responsabile della gestione del personale, Responsabile legale e di governance di Embracer Group	Responsabile governance e conformità

2. Introduzione - cos'è il whistleblowing e perché è importante?

- 2.1 La nostra organizzazione si impegna a raggiungere la trasparenza e un elevato livello di etica aziendale. Embracer Group AB e le sue entità ("Embracer Group") hanno tolleranza zero per atti quali discriminazione, molestie, criminalità, corruzione e criminalità ambientale. La parità di trattamento di tutti i dipendenti di Embracer Group ("Dipendenti"), dei clienti e dei fornitori, nonché una buona etica aziendale sono un elemento chiave.. Questi valori fondamentali sono stati documentati nel nostro Codice di condotta e nel Codice di condotta dei fornitori. I codici descrivono i principi e l'approccio di Embracer Group nei confronti dei dipendenti e dei partner commerciali e di Embracer Group in quanto datore di lavoro e membro della comunità.
- 2.2 Embracer Group incoraggia i suoi dipendenti, partner commerciali, fornitori e altri contatti esterni a informare Embracer Group/l'organizzazione se hanno identificato un problema serio o hanno seri sospetti di frode, corruzione, molestie o irregolarità simili all'interno delle operazioni del Gruppo. I Dipendenti e anche i terzi hanno un ruolo importante nel notificare se sospettano qualcosa che è contrario al Codice di condotta/Codice di condotta dei fornitori di Embracer Group. Ciò offre a Embracer Group/all'organizzazione l'opportunità di prevenire ma anche di correggere se qualcosa è andato storto. Il nostro servizio di whistleblowing offre la possibilità di avvisare Embracer Group/l'organizzazione in merito a sospetti di cattiva condotta in modo confidenziale. Si tratta di uno strumento importante per ridurre i rischi e mantenere la fiducia nelle nostre attività, consentendoci di individuare e agire tempestivamente su eventuali cattive condotte. L'atto di whistleblowing può essere effettuato da chiunque in modo aperto o anonimo.
- 2.3 Lo scopo di queste Linee guida è in parte quello di informare sui nostri canali di segnalazione interni e su come avvengono la segnalazione e il seguito delle segnalazioni, e in parte quello di garantire che adempiamo ai nostri obblighi ai sensi della Direttiva [UE] 2019/1937 del Parlamento Europeo e del Consiglio sulla tutela delle persone che segnalano violazioni del diritto dell'Unione e delle norme applicabili sulla protezione dei dati ("la Direttiva Whistleblowing"), nonché eventuali requisiti locali specifici negli Stati membri dell'UE in cui operiamo. Le presenti Linee guida si applicano a tutti i dipendenti, appaltatori, stagisti, candidati a un posto di lavoro e altri che svolgono o hanno svolto lavoro per e sotto la direzione di Embracer Group nell'Unione Europea.

3. Quando segnalare?

- 3.1 Il servizio di whistleblowing può essere utilizzato per segnalare eventuali violazioni rientranti nelle seguenti aree (le "Aree di Pertinenza"), ovvero:
1. Violazioni del diritto dell'Unione Europea che rientrano nell'ambito di applicazione materiale della Direttiva Whistleblowing, tra cui:
 - Violazioni che rientrano nell'ambito di applicazione degli atti dell'Unione di cui all'allegato della Direttiva Whistleblowing e che riguardano i seguenti ambiti
 - Appalti pubblici;
 - Servizi, prodotti e mercati finanziari e prevenzione del riciclaggio di denaro e del finanziamento del terrorismo;
 - Sicurezza e conformità del prodotto;
 - Sicurezza dei trasporti;
 - Protezione dell'ambiente;
 - Protezione dalle radiazioni e sicurezza nucleare;
 - Sicurezza degli alimenti e dei mangimi, salute e benessere degli animali;
 - Salute pubblica;
 - Protezione del consumatore;
 - Tutela della privacy e dei dati personali e sicurezza delle reti e dei sistemi informativi.
 - Violazioni degli interessi finanziari dell'Unione Europea di cui all'articolo 325 TFUE e come ulteriormente specificati nei pertinenti provvedimenti dell'Unione; e
 - Violazioni relative al mercato interno, di cui all'articolo 26, paragrafo 2, TFUE, comprese le violazioni delle norme dell'Unione in materia di concorrenza e aiuti di Stato, nonché violazioni relative al mercato interno in relazione ad atti che violano le norme sull'imposta sulle società o ad accordi il cui scopo è ottenere un vantaggio fiscale che vanifica l'oggetto o lo scopo della normativa applicabile in materia di imposta sulle società.
 2. Qualsiasi altra violazione nelle aree prescritte dalle leggi nazionali come ulteriormente elencate nelle pertinenti Appendici specifiche per Paese di seguito.
- 3.2 I dipendenti sono invitati a contattare il proprio supervisore delle risorse umane, manager o responsabile locale della conformità o funzione di controllo di conformità per questioni relative all'insoddisfazione sul posto di lavoro o questioni correlate, poiché tali questioni non possono essere indagate nell'ambito di whistleblowing.
- 3.3 Una persona che segnala non ha bisogno di avere prove concrete per esprimere un sospetto. È tuttavia vietata la segnalazione deliberata di informazioni false o dannose. L'abuso del servizio di whistleblowing delle irregolarità può costituire un illecito disciplinare, che può portare ad azioni disciplinari, fino al licenziamento, soggette alla legge locale.

- 3.4 Si prega di notare che l'ambito delle violazioni segnalabili può essere più ampio in alcuni paesi e che possono esistere disposizioni e requisiti specifici per l'utilizzo di un servizio di whistleblowing. Si prega di consultare ulteriori informazioni su <https://report.whistleb.com/embracer> – dove le disposizioni specifiche per Paese verranno mostrate quando si sceglie la lingua e nelle appendici specifiche per Paese alle presenti Linee guida, **Appendici A-O**.

4. Come segnalare?

- 4.1 Esistono diversi modi per segnalare una preoccupazione:

- **Alternativa n. 1:** Contattare un supervisore delle risorse umane, un dirigente o un responsabile della conformità locale o una funzione all'interno della nostra organizzazione.

- **Alternativa n. 2:** Contatto:

Embracer Group AB, Responsabile della gestione del personale, Responsabile legale e di governance, Ian Gulam

Telefono: +46 72 857 70 17 Email: ian.gulam@embracer.com

Una relazione può essere effettuata anche mediante un incontro fisico. Se un dipendente richiede un incontro fisico, l'incontro avrà luogo entro un tempo ragionevole in conformità con la legge locale.

- **Alternativa n. 3:** Messaggi anonimi o riservati attraverso il canale di segnalazione dei Segnalanti del Gruppo al team di whistleblowing: <https://report.whistleb.com/embracer..>
- **Alternativa n. 4:** Segnalazione ai canali esterni gestiti dalle autorità competenti o, ove applicabile, dalle istituzioni, dagli organi o dalle agenzie dell'UE attraverso i loro canali di segnalazione esterna. È possibile effettuare segnalazioni esterne a una determinata autorità a condizione che la condotta illecita rientri nella giurisdizione dell'autorità competente. In caso di segnalazioni esterne, è l'autorità competente ad essere responsabile di ricevere la segnalazione, fornire le informazioni necessarie e dare seguito. Ulteriori informazioni sulla segnalazione esterna sono riportate nelle appendici specifiche per Paese alle presenti Linee guida.

- 4.2 Offriamo la scelta di riferire al canale del Gruppo gestito dalla sede centrale di Embracer Group (Alternativa n. 3), o di riferire a livello di Gruppo Operativo locale/filiale utilizzando i canali disponibili su <https://report.whistleb.com/embrace>. Le segnalazioni tramite i canali sussidiari sono gestite dai rappresentanti di tale soggetto giuridico.

- 4.3 Tutti i messaggi ricevuti verranno gestiti in modo confidenziale. Per coloro che desiderano rimanere anonimi, offriamo canali per la segnalazione anonima. I canali di whistleblowing che consentono la messaggistica anonima sono gestiti da WhistleB, un fornitore di servizi esterno. Tutti i messaggi sono crittografati. Per garantire l'anonimato della persona che invia un messaggio, WhistleB

cancella tutti i metadati, compresi gli indirizzi IP. L'inviante il messaggio resta anonimo anche nel successivo dialogo con i responsabili destinatari della segnalazione. Le segnalazioni possono essere inviate tramite la pagina web dedicata <https://report.whistleb.com/embracer> da qualsiasi dispositivo e in qualsiasi lingua o telefonicamente (servizio opzionale); in tal caso il Segnalante può chiamare e lasciare un messaggio vocale registrato sicuro tramite il nostro servizio di risposta telefonica fornito da WhistleB. I numeri di telefono locali e ulteriori istruzioni sono disponibili su <https://report.whistleb.com/en/message/embracer/phone>.

- 4.4 Si prega di notare che in alcuni Paesi potrebbero esserci requisiti e restrizioni specifici per paese sull'uso di un servizio di whistleblowing. Si prega di consultare ulteriori informazioni su <https://report.whistleb.com/embracer> – dove verranno mostrate restrizioni specifiche quando si sceglie la lingua e nelle appendici specifiche per Paese alle presenti Linee guida, Appendici A-O.

5. Il processo investigativo

5.1 Il team di whistleblowing

- 5.1.1 L'accesso ai messaggi ricevuti attraverso i nostri canali di whistleblowing è limitato alle persone nominate presso Embracer Group AB (la società madre) o a livello di ciascun Gruppo Operativo locale/filiale con l'autorità di gestire i casi di whistleblowing. Le loro azioni vengono registrate e la gestione è riservata. Se necessario, soggetti in grado di apportare competenze possono essere inclusi nel processo investigativo, previo consenso del Segnalante nel caso in cui l'identità della persona segnalante venga divulgata. Queste persone possono accedere ai dati rilevanti e sono inoltre vincolate alla riservatezza.
- 5.1.2 Se una persona solleva una preoccupazione direttamente a un supervisore delle risorse umane, a un dirigente, a un responsabile della conformità locale o funzione di controllo di conformità o contattando personalmente il team di whistleblowing, il messaggio verrà trattato secondo le presenti Linee guida.

5.2 Ricezione di un messaggio

- 5.2.1 Dopo aver ricevuto un messaggio, il team di whistleblowing decide se accettare o rifiutare il messaggio. Se il messaggio viene accettato, verranno adottate misure di indagine adeguate, vedere la sezione 5.3 Indagine di seguito.
- 5.2.2 Il Segnalante riceverà una conferma di ricezione della segnalazione entro sette (7) giorni.
- 5.2.3 Il team di whistleblowing non può indagare sulla condotta cattiva segnalata se:
- la condotta presunta non è una condotta segnalabile ai sensi delle presenti Linee guida sul whistleblowing
 - il messaggio non è stato inviato in buona fede o è dannoso
 - non vi sono informazioni sufficienti per consentire ulteriori indagini
 - l'oggetto del messaggio è già stato risolto

5.2.4 Se un messaggio include questioni non coperte dall'ambito di applicazione delle presenti Linee guida sul whistleblowing, il team di whistleblowing dovrebbe fornire alla persona segnalante le istruzioni appropriate.

5.2.5 Il team di whistleblowing invierà un riscontro appropriato entro tre (3) mesi dalla data di ricezione della segnalazione.

5.2.6 Non includere informazioni personali sensibili su chiunque sia menzionato nel messaggio a meno che non sia necessario per descrivere la propria preoccupazione.

5.3 **Indagine**

5.3.1 Tutti i messaggi vengono trattati seriamente e in conformità con le presenti Linee guida sul whistleblowing.

- Nessuno del team di whistleblowing, o chiunque prenda parte al processo di indagine, tenterà di identificare il Segnalante.
- Il team di whistleblowing può, quando necessario, inviare domande di approfondimento tramite il canale per la comunicazione anonima.
- Un messaggio non verrà indagato da chiunque possa essere coinvolto o collegato all'illecito.
- Il team di whistleblowing decide se e come un messaggio di segnalazione debba essere intensificato.
- I messaggi di segnalazione sono gestiti in modo confidenziale dalle parti coinvolte.

6. Tutela e Privacy

6.1 **Tutela dei Segnalanti**

6.1.1 Una persona che esprime sinceri sospetti o dubbi secondo queste Linee guida non correrà il rischio di perdere il lavoro o di subire di conseguenza qualsiasi forma di sanzione o svantaggio personale. Non importa se il Segnalante si sbaglia, purché agisca in buona fede.

6.1.2 Fatte salve le considerazioni sulla privacy di coloro contro i quali sono state mosse accuse e qualsiasi altra questione di riservatezza, un Segnalante sarà tenuto informato degli esiti delle indagini sulle accuse.

6.1.3 In caso di presunti reati penali, il Segnalante non anonimo sarà informato che la sua identità potrebbe dover essere rivelata nel corso di procedimenti giudiziari.

6.2 **Archiviazione della segnalazione e trattamento dei dati personali**

6.2.1 Indipendentemente dal fatto che la tua segnalazione pervenga direttamente alla funzione Whistleblower o tramite altro canale, le informazioni raccolte vengono trasferite alla funzione Whistleblower per il seguito e l'archiviazione. Questo per garantire la massima protezione dei tuoi dati e per garantire che i tuoi dati vengano cancellati correttamente.

- 6.2.2 I dati personali inseriti nel caso segnalato sono trattati con la base giuridica dell'obbligo di legge per poter ricevere, indagare e dare seguito alla tua segnalazione e adottare eventuali misure a ciò connesse. I dati personali sono trattati durante la prosecuzione del caso e per un periodo di dodici (12) mesi dopo l'archiviazione del caso, salvo che la normativa applicabile preveda un diverso periodo di conservazione. Ciò serve per poter dare seguito ai casi dopo il loro completamento e per poter riaprire i casi se ciò è richiesto dalla legislazione o dalle circostanze del caso.
- 6.2.3 Quando i tuoi dati personali vengono trattati a causa di un obbligo legale, hai il diritto di rettificare i tuoi dati personali e di accedervi.
- 6.2.4 Se hai domande sul trattamento dei dati personali o se desideri esercitare uno dei tuoi diritti, puoi contattare il Responsabile della protezione dei dati di Embracer Group AB all'indirizzo dpo@embracer.com. Hai anche il diritto di presentare un reclamo in merito al trattamento dei dati personali alla tua autorità di controllo locale, che in Svezia è IMY, l'autorità svedese di controllo dei dati personali. www.imy.se.

7. Appendici

Appendici A-O – Appendici specifiche per Paese

Appendice J – Disposizioni specifiche per Paese – Italia

Segnalazione di preoccupazioni

Le presenti Linee guida si applicano alla segnalazione di condotte illecite e irregolarità che rientrano nell'ambito materiale del Decreto Whistleblowing (D.Lgs. n. 24/2023) (il “**Decreto**”); queste sono le seguenti:

1. violazioni amministrative, contabili, civili o penali non ritenute rilevanti ai sensi dei successivi punti (iii), (iv), (v) e (vi);
2. eventuali condotte illecite e irregolarità rilevanti ai sensi del D.Lgs. n. 231/01, ovvero violazioni di eventuali disposizioni rilevanti previste dal modello di gestione aziendale ai sensi del citato D.Lgs. n. 231/01, ove presenti;
3. eventuali condotte illecite e irregolarità rilevanti in violazione delle norme comunitarie o locali, anche se non regolate da alcuna disposizione di legge italiana, relative a: (i) appalti pubblici; (ii) servizi, prodotti e mercati finanziari e prevenzione del riciclaggio di denaro e del finanziamento del terrorismo; (iii) sicurezza e conformità del prodotto; (iv) sicurezza dei trasporti; (v) tutela dell'ambiente; (vi) protezione dalle radiazioni e sicurezza nucleare; (vii) sicurezza degli alimenti e dei mangimi, salute e benessere degli animali; (viii) sanità pubblica; (ix) tutela dei consumatori; (x) tutela della privacy e dei dati personali, nonché sicurezza delle reti e dei sistemi informatici e di rete; (x) ogni altra violazione rilevante ai sensi della normativa amministrativa, penale, civile;
4. qualsiasi condotta illecita o irregolarità rilevante elencata ai sensi dell'articolo 325 del Trattato sul funzionamento dell'Unione europea;
5. eventuali atti o omissioni rilevanti relativi al mercato locale, di cui all'articolo 26, paragrafo 2, del trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea sulla concorrenza e sugli aiuti di Stato, nonché violazioni relative al mercato locale relative ad atti in violazione delle norme o dei meccanismi di imposta sulle società il cui scopo è ottenere un vantaggio fiscale che vanifica l'oggetto o lo scopo della normativa applicabile in materia di imposta sulle società;
6. eventuali atti omissivi rilevanti in violazione dell'oggetto o dello scopo delle disposizioni di eventuali atti dell'Unione Europea nelle materie indicate ai precedenti punti (iii), (iv) e (v).

Sono espressamente esclusi dall'ambito di applicazione delle Linee guida sul whistleblowing

1. fatti, informazioni, documenti, indipendentemente dalla loro forma o mezzo, la cui divulgazione è vietata perché coperti dalla sicurezza nazionale, dal segreto medico, dal segreto delle deliberazioni giudiziarie, dalle indagini giudiziarie o inchieste giudiziarie o dal segreto professionale legale;
2. sono inoltre esclusi i conflitti interpersonali.

I soggetti, nell'ambito di un rapporto di lavoro o professionale, che possono effettuare segnalazioni interne attraverso il canale di segnalazione interno locale di cui al precedente **punto 4**, alle condizioni previste dalle Linee guida sul whistleblowing (“**Segnalanti**”), sono i seguenti:

1. dipendenti, ex dipendenti, lavoratori autonomi;

2. azionisti e membri dell'organo di amministrazione, di direzione o di vigilanza della società interessata, compresi i membri non esecutivi;
3. volontari;
4. tirocinanti retribuiti o non retribuiti;
5. qualsiasi persona che opera sotto la supervisione e la direzione di appaltatori, subappaltatori o fornitori;
6. soggetti che ricevono informazioni durante il processo di reclutamento o le negoziazioni pre-assunzione.

Le tutele previste dal Decreto si applicano ai Segnalanti e si estendono anche a:

1. i legali rappresentanti dei dipendenti nell'esercizio delle loro funzioni di consulenza e supporto al Segnalante;
2. soggetti che, all'interno dell'organizzazione in cui opera il Segnalante, assistono il Segnalante nel processo di segnalazione;
3. soggetti legati al Segnalante e che potrebbero subire ritorsioni, quali colleghi di lavoro o parenti del Segnalante; e
4. soggetti per i quali il Segnalante opera o con i quali intrattiene qualsiasi altro tipo di rapporto in un contesto di lavoro o di cui detiene una partecipazione rilevante.

Aspetti procedurali

Incoraggiamo l'utilizzo dei **canali di segnalazione locale di cui alla Sezione 4.2 delle Linee guida sul whistleblowing** e disponibili su <https://report.whistleb.com/embracer>, quando la segnalazione coinvolge preoccupazioni rilevanti a livello italiano.

Il Segnalante può anche richiedere un incontro di persona per segnalare le preoccupazioni. In tal caso, gli incontri in presenza verranno svolti tramite riunioni online utilizzando un'applicazione dedicata (ad esempio Microsoft Teams, Zoom, ecc.).

Le comunicazioni verbali, comprese quelle effettuate attraverso incontri in presenza, saranno documentate in uno dei seguenti modi, previo consenso del Segnalante:

1. mediante registrazione della conversazione; o
2. mediante una trascrizione completa ed accurata della conversazione (il Segnalante potrà verificare, rettificare ed accettare la trascrizione della conversazione firmandola).

Le trascrizioni ed i verbali potranno essere conservati solo per il tempo strettamente necessario e proporzionato al trattamento della segnalazione ed alla tutela del Segnalante, dei soggetti a cui fanno riferimento e dei terzi da essi menzionati, nonché di tutelare il diritto di difesa della Società, tenuto conto dei tempi necessari per eventuali ulteriori accertamenti.

Tuttavia:

1. la conservazione delle segnalazioni potrà essere estesa per tenere conto di eventuali approfondimenti complementari;
2. i dati relativi alle segnalazioni potranno essere conservati per un periodo superiore a quello necessario purché i dati siano resi anonimi e gli interessati non siano identificati né identificabili.

In ogni caso, i Segnalanti potranno essere sanzionati qualora l'Autorità italiana competente accerti che hanno fornito informazioni false al momento della segnalazione. In tal caso potrebbero essere applicate sanzioni disciplinari.

Le segnalazioni che contengono informazioni ottenute illegalmente (ad esempio, informazioni contenute in documenti rubati) o che, ragionevolmente, sembrano essere ottenute illegalmente non saranno accettate né potranno essere utilizzate da Embracer per adottare misure correttive.

Se il Gruppo Operativo locale ritiene che la segnalazione verrebbe gestita in modo più efficace coinvolgendo un'altra entità legale di Embracer Group o solamente Embracer Group, informerà il Segnalatore che la segnalazione sarà incanalata a:

1. il Canale di Embracer Group; o
2. il Gruppo Operativo locale dell'altro soggetto interessato. Il Gruppo Operativo italiano rimane responsabile del mantenimento della riservatezza, del feedback e della gestione del problema segnalato. In tal caso, la condivisione della Segnalazione sarà subordinata al consenso espresso dal Segnalante.

Se un Segnalante presenta una segnalazione in forma anonima al Gruppo Operativo locale, quest'ultimo dovrebbe etichettare la segnalazione come "anonima" e svolgere le indagini pertinenti garantendo che la riservatezza dell'identità del Segnalante (così come di altre persone coinvolte) sia sempre protetta. Anche nel caso in cui il Segnalante non abbia fornito il proprio nome, l'obbligo di riservatezza si estende a qualsiasi altra informazione dalla quale sia direttamente o indirettamente deducibile l'identità del Segnalante.

Tutela dei Segnalanti

L'identità del Segnalante o qualsiasi informazione da cui tale identità possa essere desunta può essere rivelata solo con il consenso del Segnalante, a meno che tale divulgazione non sia richiesta da un'autorità pubblica (ad esempio, da un Pubblico Ministero). L'identità del Segnalante può essere rivelata ai professionisti interni ed esterni di Embracer (ad esempio, avvocati, squadre forensi, ecc.) coinvolti in qualsiasi indagine interna. Tali soggetti sono soggetti ad un rigoroso obbligo di riservatezza e non possono condividere tali informazioni, salvo specifica autorizzazione del Segnalante. Qualora l'identità del Segnalante debba essere rivelata ad un'autorità pubblica, il Segnalante sarà informato con il dovuto preavviso, a meno che ciò non possa compromettere le indagini o il procedimento legale o violare qualsiasi normativa pubblica rilevante.

Anche l'identità della persona oggetto della segnalazione nonché l'identità di eventuali soggetti terzi menzionati nella segnalazione devono essere trattate in modo riservato, in conformità alle Linee guida sul whistleblowing. Le informazioni raccolte a seguito della segnalazione potranno essere comunicate

a terzi solo se necessario per l'elaborazione della segnalazione e per l'attuazione di misure disciplinari o correttive.

Sono vietati eventuali atti di ritorsione (diretti o indiretti) nei confronti del Segnalante, tra cui a titolo esemplificativo:

1. licenziamento, sospensione o misure equivalenti;
2. retrocessione o mancato avanzamento di carriera;
3. cambiamento di mansioni, luogo di lavoro, riduzione dello stipendio, cambiamento dell'orario di lavoro;
4. sospensione dalla formazione o qualsiasi restrizione all'accesso alla formazione;
5. segnalazioni negative o ammonizioni;
6. provvedimenti disciplinari o sanzioni (anche pecuniarie);
7. coercizione, intimidazione, molestie o ostracismo;
8. discriminazioni o comunque trattamenti meno favorevoli;
9. mancata conferma del personale a tempo determinato qualora il dipendente nutrisse un legittimo affidamento su detta conferma;
10. mancato rinnovo o risoluzione anticipata dei contratti di lavoro a tempo determinato;
11. danni (anche reputazionali), in particolare sui social media, pregiudizi economici (es. perdita di opportunità);
12. inserimento nelle blacklist;
13. risoluzione anticipata o risoluzione di contratti di fornitura di servizi o di beni;
14. annullamento di licenze e autorizzazioni;
15. richieste di visite mediche o psichiatriche.

Tutto il materiale relativo al Segnalante e alla segnalazione sarà trattato in modo da non alterare la segnalazione e garantire che l'identità del Segnalante e di qualsiasi altro soggetto interessato dalla segnalazione non venga divulgata, salvo che ciò sia necessario per dare seguito alle segnalazioni e adottare tutte le relative misure correttive.

I soggetti oggetto o menzionati nella segnalazione devono essere informati dell'esistenza della segnalazione entro un termine congruo. Questa informazione può essere ritardata se è probabile che tale divulgazione possa mettere seriamente a repentaglio le indagini (ad esempio, laddove vi sia il rischio che le prove possano essere distrutte). Nel dare notizia dell'esistenza della segnalazione non può in nessun caso essere rivelata l'identità del Segnalante o di altri soggetti terzi.

È espressamente vietato divulgare informazioni relative a reclami o possibili indagini interne. Parimenti, è garantita la riservatezza della documentazione prodotta nel corso delle indagini.

Il mancato rispetto degli obblighi di riservatezza e l'inosservanza del divieto di ritorsioni costituisce un grave illecito.

Canale di segnalazione esterna

Embracer incoraggia fortemente la presentazione di segnalazioni internamente affinché i problemi possano essere risolti in modo efficace.

Tuttavia, in Italia, se un Segnalante decide di segnalare le proprie preoccupazioni all'esterno nel rispetto delle disposizioni locali applicabili, l'autorità competente è l'Autorità Nazionale Anticorruzione ("**ANAC**").

Le segnalazioni esterne all'ANAC possono essere effettuate su: <https://whistleblowing.anticorruzione.it/#/>

Protezione dei dati

Il Gruppo Operativo locale e i soggetti incaricati delle attività di indagine potranno trattare i dati personali dei Segnalanti, delle persone oggetto delle segnalazioni e di ogni altro soggetto coinvolto nella segnalazione o in eventuali successive indagini.

Titolare del trattamento dei dati personali è **Milestone S.r.l.**, con sede legale in Via Olona n. 2, Milano, Italia.

Lo scopo del trattamento dei dati personali è gestire il canale di segnalazione italiano e indagare sulle segnalazioni in conformità con le disposizioni di legge relative all'implementazione di un sistema di whistleblowing ai sensi del Decreto.

Ai dati personali avranno accesso solo i relativi Gruppi Operativi locali.

Tuttavia, fatti salvi i rigorosi obblighi di riservatezza sopra menzionati, l'accesso ai dati personali potrà essere concesso previo consenso dell'interessato, a titolo esemplificativo, a supervisor di risorse umane, dirigenti, responsabili della conformità locali, funzioni aziendali o qualsiasi altro soggetto coinvolto nelle indagini affinché possano adottare tutte le misure disciplinari necessarie o intraprendere azioni legali per risolvere la questione segnalata.

I Segnalanti, le persone oggetto della segnalazione o altri soggetti interessati possono esercitare i propri diritti sulla privacy dei dati come descritto nelle informative sulla privacy del titolare del trattamento. Tuttavia, nel caso in cui le persone oggetto delle segnalazioni esercitino il diritto di opposizione, si presume che sussistano motivi legittimi cogenti per trattare i loro dati personali, salvo prova contraria.

Dati personali relativi a segnalazioni fuori ambito, categorie particolari di dati personali (salvo ove necessario in ragione della natura della segnalazione), informazioni non veritiere, e dati personali non necessari ai fini dell'indagine non dovrebbero essere raccolti o, se raccolti perché necessari, in prima istanza, saranno distrutti senza indugio.