POLICY WHISTLEBLOWING

v. 07.11.2023

Sommario

1. SCOPO E AMBITO DI APPLICAZIONE

1.1 FINALITA'

Con il termine *Whistleblowing* si fa riferimento alla rivelazione spontanea da parte di un soggetto segnalante, che prende il nome di *whistleblower*, di un illecito che leda l'interesse pubblico o l'integrità dell'ente commesso all'interno del contesto lavorativo e di cui lo stesso si trovi ad essere testimone.

Il decreto legislativo 10 marzo 2023 n. 24 (di seguito, il "*Decreto*"), attuativo della Direttiva UE 2019/1937, persegue la finalità di rafforzare la protezione delle persone segnalanti ed estendere l'ambito di tutela della riservatezza a ulteriori soggetti, diversi dal Segnalante, che tuttavia potrebbero essere destinatari di ritorsioni, intraprese anche indirettamente, in ragione del ruolo assunto nell'ambito del processo di segnalazione e/o del particolare rapporto che li lega al Segnalante. Il Decreto prevede, altresì, che possano essere effettuate segnalazioni anonime.

La presente *policy* disciplina le modalità con cui Zeus Iba S.r.l. (di seguito "la Società") recepisce la normativa in tema di *Whistleblowing* e descrive il processo di gestione delle segnalazioni, pervenute al canale interno da parte di chiunque si trovi a conoscenza di atti e/o fatti, anche solo potenzialmente, contrari alla legge e alle normative interne aziendali.

1.2 DESTINATARI

Sono destinatari delle tutele e della protezione garantite dalla normativa:

- Lavoratori subordinati;
- Lavoratori autonomi che svolgono la propria attività lavorativa presso l'ente;
- Fornitori, subfornitori e dipendenti di questi;
- Liberi professionisti e consulenti;
- Volontari e tirocinanti, retribuiti e non retribuiti;
- Azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto;
- Coloro che ancora non hanno un rapporto giuridico con l'ente (in fase di trattative precontrattuali), nonché coloro il cui rapporto sia cessato o che siano in periodo di prova.

In ragione dell'estensione dell'ambito di applicazione soggettiva della normativa di riferimento, sono altresì destinatari delle tutele e della protezione garantite dalla normativa:

- Facilitatore, persona fisica che assiste (fornisce consulenza o sostegno) il Segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo;
- Persone del medesimo contesto lavorativo del Segnalante che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- Colleghi di lavoro che lavorano nel medesimo contesto lavorativo del Segnalante e che hanno con detta persona un rapporto abituale e corrente;
- Enti di proprietà del Segnalante, in via esclusiva o in compartecipazione maggioritaria di terzi, del Segnalante;
- Enti presso i quali il Segnalante lavora;
- Enti che operano nel medesimo contesto lavorativo del Segnalante.

2. OGGETTO DELLA SEGNALAZIONE

Possono costituire oggetto di segnalazione informazioni sulle violazioni di specifiche normative nazionali e dell'Unione Europea. Non esiste un elenco tassativo di reati o di irregolarità che possono costituire l'oggetto del *whistleblowing*; vengono considerate rilevanti le segnalazioni che riguardano comportamenti, rischi o irregolarità, consumati o tentati, a danno dell'interesse pubblico o dell'integrità dell'ente.

Saranno, pertanto, segnalabili violazione che riguardano comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'ente e che consistono in:

1) Illeciti amministrativi;
2) Illeciti rilevanti ai sensi del d.lgs. 231/2001;
3) Illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione Europea o nazionali (non già disciplinati in via obbligatoria);
4) Atti od omissioni che ledono gli interessi finanziari dell'Unione Europea di cui all'art. 325 del TFUE (ad esempio, frodi e attività illegali);
5) Atti ed omissioni riguardanti il mercato interno, di cui all'art. 26, paragrafo 2 del TFUE (ad esempio, frodi del bilancio dell'Unione Europea e attività corruttive);
6) Atti o comportamenti che vanificano l'oggetto o le finalità delle disposizioni di cui agli atti dell'Unione Europea nei settori indicati nei numeri 3), 4) e 5).

Si precisa che, secondo quanto previsto dal Decreto, la protezione e le tutele previste dalla normativa non si applicano alle segnalazioni relative a:

a) Contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona Segnalante o che attengono esclusivamente ai propri rapporti individuali di lavoro;
b) Violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione Europea o nazionali (a titolo esemplificativo: servizi finanziari, riciclaggio e terrorismo, sicurezza dei trasporti, tutela dell'ambiente, tutela dei consumatori);
c) Violazioni in materia di sicurezza nazionale, nonché appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione Europea.

I soggetti segnalanti dovranno assicurarsi che la segnalazione sia il più possibile circostanziata e che le informazioni relative al soggetto Segnalato quale autore potenziale dell'illecito siano tali da consentirne l'identificazione e l'attribuzione dei fatti segnalati. È possibile allegare documenti alla segnalazione a dimostrazione della veridicità e della fondatezza dei fatti segnalati.

Nel caso di segnalazione generica, non contenente informazioni sufficienti per l'avvio delle attività di indagine, il Gestore dovrà richiedere al Segnalante – mediante l'apposita Piattaforma – di fornire maggiori dettagli. Qualora non sia possibile contattare il Segnalante ovvero lo stesso non fornisca ulteriori dettagli entro quindici giorni lavorativi dalla richiesta, il Gestore procederà ad archiviare la segnalazione.

3. CANALI DI SEGNALAZIONE

La disciplina prevista dal Decreto prevede che siano messi a disposizione del *whistleblower* tre canali di segnalazione:

- Il canale interno, attivato dalla Società;
- Il canale esterno, predisposto da ANAC;
- Le divulgazioni pubbliche, tramite stampa o social media.

La normativa prevede che, in via prioritaria, i segnalanti utilizzino il canale interno e, solo al ricorrere di determinate condizioni, possano effettuare una segnalazione esterna o una divulgazione pubblica.

3.1 CANALE INTERNO

La Società mette a disposizione dei dipendenti e degli *stakeholders* esterni un canale di segnalazione accessibile al link posto nella apposita sezione Whistleblowing all'interno del sito web *www.zeusiba.it* che condurrà direttamente alla Piattaforma informatica dedicata alla ricezione delle segnalazioni (di seguito, anche la "Piattaforma").

Questa modalità consente l'invio di una segnalazione senza creare un account. Il modulo della segnalazione contiene i campi per indicare il nome e il cognome. Tali campi non sono obbligatori, pertanto, la segnalazione fatta con questa modalità può essere inviata in modalità anonima o meno, in base alla scelta dell'utente. I dati del Segnalante, se indicati, vengono nascosti e saranno visualizzabili solo al personale deputato alla gestione delle segnalazioni tramite un'apposita procedura di sicurezza.

Per garantire un anonimato totale al Segnalante, si raccomanda di effettuare la segnalazione da un dispositivo personale tramite rete privata non aziendale.

Al termine della procedura di segnalazione, al Segnalante viene rilasciato un codice che permette di accedere successivamente alla segnalazione effettuata e di verificarne lo stato di avanzamento.

Non dovranno essere aperte più segnalazioni per lo stesso fatto. Eventuali integrazioni dovranno essere inserite all'interno della medesima segnalazione.

3.1.1. PERSONALE INTERNO DEPUTATO ALLA GESTIONE DELLE SEGNALAZIONI

Il Personale interno deputato alla gestione delle segnalazioni (il "Gestore") è competente a ricevere e a gestire le segnalazioni in considerazione delle competenze professionali e delle funzioni ricoperte. Nel rispetto dei principi di imparzialità e riservatezza compie ogni attività ritenuta opportuna per la valutazione della segnalazione, inclusa l'audizione dei soggetti che possono riferire sui fatti segnalati.

3.1.2. FASE ISTRUTTORIA E INDAGINI INTERNE

Il Gestore riceve le segnalazioni tramite la Piattaforma e rilascia un avviso di presa in carico al Segnalante entro sette giorni dalla data di ricezione. Contestualmente, si instaura un canale di comunicazione tra il Segnalante e il Gestore per eventuali richieste o integrazioni. In ragione di ciò, il Segnalante deve accedere regolarmente alla Piattaforma e monitorare lo stato dell'istruttoria inserendo il numero di ricevuta rilasciato al termine della compilazione del form di segnalazione.

Il Gestore, nel rispetto dei principi di imparzialità e riservatezza, potrà decidere, al fine di dare diligente seguito alle segnalazioni, di coinvolgere dei Collaboratori (es. altre strutture aziendali, soggetti terzi specializzati), anch'essi specificamente formati e autorizzati, per verificare:

- che il Segnalante rientri tra i soggetti qualificati ad effettuare una segnalazione;
- che la violazione rientri tra quelle segnalabili;
- la fondatezza della segnalazione, archiviandola se infondata, procedendo con le indagini interne se ritenuta fondata.

Il Gestore fornirà riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Nell'ambito delle indagini interne, al fine di verificare la fondatezza delle segnalazioni e la veridicità dei fatti segnalati, il Gestore può analizzare le banche dati per individuare possibili collegamenti tra Segnalato e terzi; raccogliere documenti aziendali rilevanti; analizzare i *device* assegnati al Segnalato per verificare la sussistenza di prove a conferma della segnalazione, come e-mail o messaggi, secondo quanto previsto dal Regolamento aziendale per l'utilizzo dei dispositivi informatici; effettuare interviste a persone che possono riferire informazioni impattanti per provare le violazioni segnalate.

Ai fini dell'attività di verifica, il Gestore può conferire mandato di approfondimento a Uffici specialistici e/o a soggetti terzi, avendo cura di:

- conferire mandato formale, definendo il perimetro di azione e precisando le informazioni che intende ottenere dall'approfondimento richiesto;
- omettere qualsiasi informazione che possa, anche indirettamente, ricondurre all'identità del Segnalante;
- omettere qualsiasi informazione relativa al Segnalato, laddove non strettamente necessaria al corretto svolgimento dell'incarico affidato;
- ribadire al soggetto incaricato l'obbligo di riservatezza dei dati trattati (nel caso di soggetti esterni alla Società detto obbligo dovrà essere formalizzato nel contratto di prestazione di servizi).

Per una completa trasparenza del processo, le segnalazioni archiviate come non rilevanti sono annotate riportando l'oggetto della segnalazione e le motivazioni per cui non si è proceduto con le successive indagini.

3.2 ALTRI CANALI DI SEGNALAZIONE

È possibile, al ricorrere di particolari condizioni indicate nel Decreto, procedere all'utilizzo di altri canali di segnalazione: il canale esterno predisposto da ANAC e la divulgazione pubblica.

Segnalazione esterna

Il Segnalante può effettuare una segnalazione attraverso il canale esterno attivato da ANAC (Autorità Nazionale Anticorruzione) se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

a) non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto stabilito dalla normativa;

b) il Segnalante ha già effettuato una segnalazione interna seguendo la procedura stabilita dalla propria organizzazione ma la stessa non ha avuto seguito;

c) il Segnalante ha fondati motivi per ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare un rischio di ritorsione;

d) il Segnalante ha fondato motivo per ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le segnalazioni esterne sono effettuate in forma scritta tramite la piattaforma informatica messa a disposizione dall'ANAC oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta del Segnalante, mediante un incontro diretto fissato entro un termine ragionevole. Le modalità di gestione delle segnalazioni sono state stabilite all'interno del Regolamento ANAC adottato con delibera n. 301 del 12 luglio 2023. La segnalazione esterna presentata ad un soggetto diverso dall'ANAC è trasmessa a quest'ultima, entro sette giorni dalla data del suo ricevimento, dando contestuale notizia della trasmissione al Segnalante.

Divulgazione pubblica

Il Segnalante ha facoltà di effettuare una divulgazione pubblica al ricorrere di una delle seguenti condizioni:

a) il Segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro nei termini previsti;

b) il Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;

c) il 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.

4. CONSERVAZIONE DELLA DOCUMENTAZIONE

I dati e la documentazione eventualmente allegata alla segnalazione saranno conservati per il tempo necessario alla gestione e alla valutazione della segnalazione, comunque non oltre il termine di cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

5. TUTELA DEL SEGNALANTE

L'identità del Segnalante e degli altri soggetti ai quali la normativa in materia di *whistleblowing* estende l'ambito di tutela non potrà essere rivelata a persone diverse dal Gestore se non specificamente autorizzate.

Le misure adottate a garanzia della riservatezza del soggetto segnalante non si limitano a proteggere i dati identificativi, ma anche tutti gli elementi della segnalazione dai quali si possa evincere, anche indirettamente, la sua identità. Un eventuale disvelamento dell'identità del Segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni o comunque autorizzate avverrà con il consenso espresso del Segnalante.

La Società si impegna a garantire la protezione da qualsiasi atto di ritorsione, discriminazione o penalizzazione, diretto o indiretto, nei confronti del Segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. Tutto il personale coinvolto, a qualsiasi titolo, nelle diverse fasi afferenti alla gestione delle segnalazioni è tenuto a garantire il massimo livello di riservatezza sui contenuti delle medesime e sulle persone coinvolte nella segnalazione.

La tutela del Segnalante non potrà essere garantita qualora sia accertata l'infondatezza e il carattere diffamatorio della segnalazione, configurando in tal modo un comportamento doloso del Segnalante.

6. PROTEZIONE DALLE SEGNALAZIONI DIFFAMATORIE E TUTELA DEL SEGNALATO

Al fine di tutelare la dignità, l'onore e la reputazione di ognuno, la Società si impegna ad offrire massima protezione dalle segnalazioni diffamatorie.

In tale contesto, qualora al termine della fase di verifica della segnalazione, ne venga accertata l'infondatezza ed il contestuale dolo e/o colpa grave del Segnalante, la Società intraprenderà idonee iniziative a tutela propria e dei propri dipendenti.

La Società adotta analoghe forme di tutela a garanzia della privacy del Segnalante anche per il presunto responsabile della violazione, fatte salve le previsioni di legge applicabili.

7. MISURE E PROVVEDIMENTI SANZIONATORI

Qualora dalle verifiche delle segnalazioni condotte ai sensi del presente documento si riscontri un comportamento illecito ascrivibile a personale dipendente, la Società agirà con tempestività ed immediatezza, attraverso misure e provvedimenti sanzionatori adeguati e proporzionati, tenuto conto della gravità nonché della rilevanza penale di tali comportamenti e dell'instaurazione di un procedimento penale nei casi in cui costituiscano reato ai fini della normativa nazionale vigente.

Qualora le indagini condotte evidenzino comportamenti dolosi/colposi in capo a soggetti terzi, che hanno avuto e/o hanno in essere rapporti con la Società, la stessa agirà tempestivamente disponendo tutte le misure individuate come necessarie per la propria tutela.

8. PROTEZIONE DEI DATI PERSONALI

Informativa resa ai sensi degli artt. 13 e 14 del Regolamento UE 679/2016 (GDPR) sul trattamento dei dati personali relativi alle persone fisiche

Con la presente informativa, la Società fornisce informazioni relative al trattamento dei dati personali del Segnalante e degli altri soggetti interessati, menzionati o coinvolti nella segnalazione stessa, tra cui i potenziali

responsabili degli illeciti oggetto di segnalazione (di seguito, "il Segnalato"). Il trattamento sarà improntato ai principi di correttezza, liceità, trasparenza e tutela della riservatezza.

TITOLARE DEL TRATTAMENTO

Titolare del trattamento è **ZEUS IBA S.r.l.**, in persona del rappresentante legale p.t., sede legale in Via Bibbiena n. 12/14 - 50142, Firenze (FI)- P.IVA 06617940488 – e-mail: ***infomail@zeusiba.it.***

FONTE DEI DATI TRATTATI

Le informazioni possono essere fornite:

- nella segnalazione, dal Segnalante;
- nel corso delle necessarie attività istruttorie (a titolo esemplificativo, da fonti pubbliche, terzi intervistati, etc.);
- durante il processo di gestione della segnalazione;
- attraverso log di traffico sulle connessioni alla piattaforma di segnalazione registrati sui sistemi aziendali della Società.

Per garantire un anonimato totale al Segnalante, si raccomanda di effettuare la segnalazione da un dispositivo personale tramite rete privata non aziendale.

TIPOLOGIA DEI DATI TRATTATI

- Qualora il Segnalante non decida di conservare l'anonimato possono essere trattati dati personali allo stesso riferibili, nello specifico:
    - dati anagrafici;
    - dati di contatto;
    - eventuali dati di natura particolare ai sensi dell'art. 9 GDPR, in quanto *idonei a rivelare uno stato generale di salute (assenze per malattia, maternità, infortunio, etc.), l'idoneità allo svolgimento di specifiche mansioni, l'adesione ad un sindacato e/o ad un partito politico, la titolarità di cariche pubbliche elettive, le convinzioni religiose ecc.;*
    - eventuali dati c.d. giudiziari ai sensi dell'art. 10 GDPR, in quanto relativi *a condanne penali e a reati o a connesse misure di sicurezza;*
    - qualsiasi dato personale contenuto nell'oggetto della segnalazione.

- A seguito della segnalazione possono essere trattati dati personali riferiti a terzi soggetti (potenziali autori di un illecito o di una irregolarità che rientrano tra quelle segnalabili o soggetti informati sui fatti), nello specifico:
    - dati anagrafici;
    - dati di contatto;
    - eventuali dati di natura particolare ai sensi dell'art. 9 GDPR, in quanto *idonei a rivelare uno stato generale di salute (assenze per malattia, maternità, infortunio, etc.), l'idoneità allo svolgimento di specifiche mansioni, l'adesione ad un sindacato e/o ad un partito politico, la titolarità di cariche pubbliche elettive, le convinzioni religiose ecc.;*
    - eventuali dati c.d. giudiziari ai sensi dell'art. 10 GDPR, in quanto relativi *a condanne penali e a reati o a connesse misure di sicurezza;*
    - qualsiasi dato personale contenuto nell'oggetto della segnalazione.

- I dati personali che dovessero emergere dalle successive attività istruttorie;
- Log di traffico riguardanti le connessioni alla piattaforma di segnalazione registrati sui sistemi aziendali *(In generale, i log sono file che registrano – e quindi permettono di ricostruire – l'intera "storia" delle operazioni effettuate da un utente o da una macchina. Tramite i log, infatti, vengono registrate tutte le operazioni, in ordine cronologico, svolte nel normale utilizzo di un software, di un applicativo o più*

semplicemente di un computer. Il log registra anche tutte le operazioni che un computer svolge in autonomia, senza necessità di intervento umano. La gestione dei log a livello aziendale permette di monitorare una serie di attività, tra cui gli accessi al sistema effettuati in un dato lasso temporale (anche quelli fuori dall'orario di lavoro, quelli non andati a buon fine o quelli tramite VPN), le transazioni fallite, eventuali anomalie (sia software che hardware) e possibili minacce malware. Tali informazioni sono necessarie per comprendere lo stato della sicurezza informatica aziendale: sia in caso di normale funzionamento della macchina ma, soprattutto, in caso di errori e problemi, come eventuali attacchi hacker, permettendo così alla funzione IT di indagarne le cause e trovare una risoluzione, evitando o bloccando tempestivamente situazioni pregiudizievoli.).

Saranno acquisiti i soli dati personali strettamente necessari e pertinenti al raggiungimento delle finalità di seguito indicate, nel rispetto del principio di minimizzazione di cui all'art. 5, comma 1, lett. c) GDPR.

FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO

Il Titolare tratterà i dati personali suindicati:

- al fine di gestire e dare diligente seguito alle segnalazioni ricevute, ivi incluse le attività di accertamento e le indagini interne legate alla verifica delle condotte oggetto di segnalazione e l'instaurazione di procedimenti, anche disciplinari, nei limiti di quanto richiesto dalle norme applicabili. Inoltre, i dati personali potranno essere trattati per dare seguito a richieste da parte dell'autorità amministrativa o giudiziaria competente e, più in generale, dei soggetti pubblici nel rispetto delle formalità di legge. I dati saranno trattati, altresì, per prevenire e contrastare efficacemente comportamenti fraudolenti e condotte illecite o irregolari.
  Pertanto, la base giuridica che giustifica la liceità del trattamento è rappresentata dalla necessità di adempiere ad obblighi di legge e di eseguire compiti di interesse pubblico cui è sottoposto il Titolare del trattamento e disposizioni di Autorità legittimate dalla legge [art. 6, par. 1, lett. c) ed e); art. 9, par. 2, lett. b) e g); art. 10 GDPR].
  Un eventuale disvelamento dell'identità del soggetto Segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni o comunque autorizzate avverrà con il consenso espresso del Segnalante [art. 6, par. 1, lett. a) GDPR].

- al fine di: i) soddisfare esigenze di controllo interno del Titolare e di monitoraggio dei rischi aziendali, nonché per l'ottimizzazione e l'efficientamento dei processi gestionali aziendali e amministrativi interni; ii) accertare, esercitare o difendere un diritto o un interesse legittimo del Titolare in ogni sede competente a garanzia dell'esercizio del diritto di difesa ex art. 24 della Costituzione; iii) gestire la sicurezza informatica e tutelare il patrimonio e la sicurezza dei dati, l'assistenza degli utenti e la manutenzione dei sistemi di sicurezza e protezione perimetrale dei log di traffico riguardanti le connessioni alla Piattaforma di *whistleblowing* registrati sui sistemi aziendali.
  Pertanto, la base giuridica che giustifica la liceità del trattamento è rappresentata dalla necessità di perseguire un legittimo interesse del Titolare [art. 6, par. 1, lett. f) GDPR].

MODALITA' DI TRATTAMENTO

Le informazioni come sopra individuate vengono trattate da soggetti appositamente autorizzati e adeguatamente formati.
La raccolta dei dati avviene con modalità informatiche, mediante l'apposita Piattaforma di segnalazione secondo quanto definito nella Policy Whistleblowing, in modo da garantire la riservatezza dei segnalanti e

degli eventuali altri soggetti coinvolti e la confidenzialità delle informazioni presenti all'interno delle segnalazioni.

DESTINATARI E AMBITO DI COMUNICAZIONE DEI DATI

Possono venire a conoscenza dei dati personali raccolti altri soggetti il cui coinvolgimento sia necessario per compiere le dovute attività istruttorie, volte a verificare la fondatezza del fatto oggetto della segnalazione, nonché l'adozione di eventuali provvedimenti. In tal caso, saranno coinvolti soggetti specificamente istruiti e autorizzati a compiere operazioni di trattamento, quali a titolo esemplificativo consulenti esterni, responsabili dell'area in cui opera il Segnalato, Ufficio IT.
Si ricorda che le informazioni e i dati raccolti potranno essere trasmessi alle Autorità competenti.
Un eventuale disvelamento dell'identità del soggetto Segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni o comunque autorizzate avverrà con il consenso espresso del Segnalante.

L'elenco dei soggetti terzi incaricati in qualità di Responsabili del trattamento (ai sensi dell'art. 28 GDPR) per la fornitura di servizi esternalizzati dal Titolare (servizi informatici, sviluppo e manutenzione della Piattaforma dedicata, servizi di comunicazione ecc.) è disponibile previa richiesta. Tali soggetti terzi tratteranno i dati personali nei limiti dell'attività svolta e secondo le istruzioni del Titolare.

NATURA OBBLIGATORIA DEL CONFERIMENTO E CONSEGUENZA DI EVENTUALI RIFIUTI

Al fine di effettuare una segnalazione, il conferimento di dati personali è facoltativo; tuttavia, se conferiti, in taluni casi può rendersi necessario un loro utilizzo da parte del personale autorizzato per il perseguimento delle suddette finalità. Il mancato conferimento dei dati necessari a dare seguito alla segnalazione impedirà l'esecuzione delle attività.

TRASFERIMENTO DATI ALL'ESTERO

Il Titolare del trattamento non trasferisce i dati personali in Paesi terzi. Nel caso in cui si rendesse necessario un trasferimento di dati extra UE, la Società verificherà che i fornitori prestino garanzie adeguate, così come previsto dagli artt. 44 e seguenti GDPR.

TEMPI DI CONSERVAZIONE DEI DATI

I dati personali raccolti saranno conservati per il tempo strettamente necessario ad espletare le finalità già indicate nei precedenti paragrafi e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della segnalazione, salvo il caso in cui una conservazione ulteriore si renda necessaria in virtù di obblighi previsti dalla legge (ad esempio, qualora sia in corso un procedimento giudiziario o disciplinare, fino alla conclusione dello stesso). Il Titolare, giunto tale termine, provvederà alla cancellazione dei dati personali.

DIRITTI DELL'INTERESSATO

Il Titolare informa gli interessati che, in via generale e previa prova della propria identità, possono esercitare i diritti di cui agli artt. 15 e ss. GDPR, in particolare: i) diritto di accesso; ii) diritto di rettifica; iii) diritto alla cancellazione; iv) diritto alla limitazione del trattamento; v) diritto di opposizione; vi) diritto di non essere sottoposto a processo decisionale automatizzato; vii) revoca del consenso. L'esercizio dei diritti può avvenire contattando il Titolare attraverso l'invio di una richiesta all'indirizzo e-mail *infomail@zeusiba.it.*

Nel caso di specie, tuttavia, ai sensi degli artt. 2-undecies e 2-duodecies del d.lgs. 196/2003 "Codice Privacy", il Titolare si riserva la facoltà di limitare o ritardare l'esercizio di tali diritti, nei limiti di quanto stabilito dalle disposizioni di legge applicabili, in particolare laddove sussista il rischio che possa derivare un pregiudizio

effettivo, concreto e non altrimenti giustificato alla riservatezza dell'identità del Segnalante e che si possa compromettere la capacità di verificare efficacemente la fondatezza della segnalazione o di raccogliere prove necessarie.

In particolare, l'esercizio di tali diritti:

- sarà possibile conformemente alle disposizioni di legge o di regolamento che regolano il settore (tra cui il d.lgs. 231/2001 e ss.mm.ii.);
- potrà essere ritardato, limitato o escluso con comunicazione motivata e senza ritardo all'interessato, a meno che la comunicazione possa compromettere le finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare la riservatezza dell'identità del Segnalante.

Gli interessati hanno, inoltre, diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali.