PROCEDURA WHISTLEBLOWING
(EX D.LGS. 10 MARZO 2023 N. 24)

Codice:	**PR21**	Rev: **00**
Stato di Emissione:	Data di Emissione:	n° pag:
Emesso	**[19/06/2025]**	**18**

Autore:
Studio Legale
PedersoliGattai
(Consulente esterno)

Verificato da:
Fabio Cocchieri
(Quality Assurance)

Approvato da:
Giorgio Finaurini
(CEO)

Avviso di riservatezza: questo documento è riservato. Contiene informazioni di carattere strettamente confidenziale di proprietà di Ksenia Security S.p.A. Né questo documento né nessuna delle informazioni qui contenute, possono essere riprodotto o divulgate in nessuna circostanza, senza l'esplicita autorizzazione scritta di Ksenia Security S.p.A. (Strada Provinciale Valtesino, 49 - 63065 – Ripatransone - AP - Italia).

Elenco Revisioni

REVISIONE	DATA	AUTORE	DESCRIZIONE DELLA MODIFICA
00	[19/06/2025]	Studio Legale PedersoliGattai	Primo rilascio

Nota: Il documento è conforme all'originale cartaceo completo di firme e archiviato presso il RC.

© Ksenia Security S.p.A.

Sommario

1. QUADRO NORMATIVO E DEFINIZIONI RILEVANTI 4
1.1 Quadro normativo 4
1.2 Definizioni rilevanti 4
2. DESTINATARI DELLA PROCEDURA WHISTLEBLOWING 6
3. PRINCIPI GENERALI 6
4. COSA SI PUÒ SEGNALARE? 7
4.1 Contenuto delle segnalazioni 7
4.2 Tipologia di violazioni rilevanti ai sensi del Decreto Whistleblowing 7
5. DOVE POSSO EFFETTUARE LA SEGNALAZIONE? 9
5.1 Canale di segnalazione interna 9
5.2 Segnalazioni trasmesse su canali e/o a soggetto non competente 10
5.3 Canale esterno (ANAC) 10
6. COME VIENE GESTITA LA SEGNALAZIONE INTERNA? 11
6.1 Gestore della segnalazione 11
6.2 Processo di gestione della segnalazione 11
7. CONFLITTO DI INTERESSI 13
8. OBBLIGO DI RISERVATEZZA 13
9. TUTELA DEL SEGNALANTE E DELLE PERSONE COLLEGATE 14
9.1 Riservatezza del segnalante 14
9.2 Divieto di ritorsione 14
9.3 Condizioni per beneficiare delle misure di protezione 15
9.4 Ulteriori soggetti cui sono estese le misure di protezione 15
9.5 Contenuto delle misure di protezione 16
10. COMUNICAZIONE DEI RISULTATI E REPORTISTICA 16
11. TRATTAMENTO DEI DATI PERSONALI 16
12. CONSERVAZIONE DELLA DOCUMENTAZIONE 17
13. FORMAZIONE 17
14. SANZIONI DISCIPLINARI E ALTRI PROVVEDIMENTI 18
15. PUBBLICAZIONE E DIFFUSIONE DELLA PROCEDURA WHISTLEBLOWING 18

© Ksenia Security S.p.A.

1. QUADRO NORMATIVO E DEFINIZIONI RILEVANTI

1.1 Quadro normativo

Il Decreto Legislativo del 10 marzo 2023, n. 24 «Attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali», entrato in vigore a far data dal 30 marzo 2023, disciplina compiutamente lo strumento del c.d. "whistleblowing" prevedendo l'obbligo per determinati soggetti (sia pubblici sia privati) – tra i quali rientra anche Ksenia Security S.p.A. – di provvedere a:

a. istituire specifici canali di segnalazione interna, tali da consentire di effettuare segnalazioni in forma scritta, anche con modalità informatiche, e orale, tramite linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante incontro diretto;
b. garantire la riservatezza dell'identità delle persone segnalanti, delle persone coinvolte e/o comunque menzionate nella segnalazione e della relativa documentazione;
c. affidare la gestione dei canali di segnalazione ad un ufficio interno autonomo, ovvero ad un soggetto esterno autonomo, prevedendo l'impiego di personale specificamente formato;
d. valutare ed istruire le segnalazioni, raccogliendo le informazioni ulteriori necessarie e adottando ogni misura, anche a livello disciplinare, nei confronti del segnalato (se la segnalazione si rivela fondata) o del segnalante (se la segnalazione risulta infondata per malafede o con colpa grave);
e. non adottare alcuna Misura Ritorsiva nei confronti dei soggetti che effettuano la segnalazione (sempre che detta segnalazione non risulti strumentale, in malafede o effettuata con colpa grave);
f. informare in maniera chiara ed efficace i destinatari della presente Procedura, garantendo la più ampia diffusione e accessibilità della stessa ai propri dipendenti ed anche ad ogni ulteriore soggetto (fornitori, consulenti, lavoratori autonomi, ecc..) che intrattenga rapporti con Ksenia Security, ai sensi dell'art. 3, co. 3 D.Lgs. 24/2023.

Il legislatore ha disposto che debbano essere approntati all'interno degli enti cui si applica la normativa appositi "canali interni" per ricevere le segnalazioni.
Il ricorso a questi canali viene incoraggiato, in quanto più prossimi all'origine delle questioni oggetto della segnalazione.
La preferenza accordata ai canali interni si evince anche dal fatto che, solo ove si verifichino particolari condizioni specificamente previste allora i segnalanti possono ricorrere al "canale esterno" di segnalazione attivato presso ANAC usufruendo delle medesime tutele.
Nell'ottica di consentire di scegliere il canale di segnalazione più adeguato in funzione delle circostanze del caso, e quindi di garantire una più ampia protezione, è prevista, al ricorrere di determinate condizioni, anche la divulgazione pubblica.
Rimane salvo il potere (e in alcuni casi il dovere) di rivolgersi all'Autorità giudiziaria ove ne ricorrano i presupposti.
In materia whistleblowing assumono infine rilevante valore anche le Linee guida approvate dall'ANAC con delibera del 12 luglio 2023, agevolmente consultabili accedendo al sito web istituzionale dell'ANAC stesso, ed in particolare alla sezione "Consulta documenti", oppure tramite il link:

https://www.anticorruzione.it/-/del.311.2023.linee.guida.whistleblowing

1.2 Definizioni rilevanti

ANAC: si intende l'Autorità Nazionale Anti-Corruzione.

Canali di Segnalazione: i canali messi a disposizione da Ksenia Security per inoltrare le Segnalazioni garantendo la riservatezza dell'identità del Segnalante.

© Ksenia Security S.p.A.

Codice Etico: è un documento adottato dalla Società con cui vengono enunciati l'insieme dei diritti, doveri e responsabilità dell'ente rispetto a tutti i soggetti con i quali entra in relazione per il conseguimento del proprio scopo istituzionale. Il Codice Etico fissa "standard" etici di riferimento e norme comportamentali che i destinatari devono rispettare nei rapporti con l'ente.

Codice Privacy: il D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al GDPR, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", e sue successive integrazioni e modificazioni.

Destinatari: i soggetti di cui al paragrafo n. 2 della presente Procedura.

Decreto 231: il D.Lgs. 8 giugno 2001, n. 231, e sue successive integrazioni e modificazioni.

Decreto whistleblowing: il D.Lgs. 10 marzo 2023, n. 24, recante «Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali».

Direttiva whistleblowing: la Direttiva (UE) n. 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

Divulgazione Pubblica: rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

Facilitatore: si tratta di una persona fisica che assiste il Segnalante nel processo di Segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.

GDPR: il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Gestore delle Segnalazioni o Gestore: soggetto responsabile per la gestione delle segnalazioni in conformità alle disposizioni del D.Lgs. n. 24/2023.

Informazioni sulla Violazione: informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante intrattiene un rapporto giuridico nei termini previsti dalla presente Procedura, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.

Ksenia Security o la Società: Ksenia Security S.p.A., con Sede Legale in Ripatransone (AP), Strada Provinciale Valtesino n. 49 – 63065.

Linee Guida ANAC: "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne" - Delibera ANAC n. 311 del 12 luglio 2023.

Modello 231: il modello organizzativo di gestione e controllo, adottato dalla Società ai sensi del Decreto 231.

OdV: l'Organismo di Vigilanza, nominato dalla Società ed istituito ai sensi del Decreto 231.

Persona Coinvolta: la persona fisica o giuridica menzionata nella Segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente o per la quale è stata presentata denuncia all'autorità giudiziaria.

Procedura whistleblowing o Procedura: la presente procedura.

Ritorsione o Misure Ritorsive: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione o della denuncia all'autorità giudiziaria o contabile e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

© Ksenia Security S.p.A.

Segnalante: il soggetto che effettua la Segnalazione.

Segnalazione: tutte le comunicazioni, scritte od orali, di informazioni sulle violazioni.

Segnalazione Anonima: quando le generalità del Segnalante non sono note né altrimenti individuabili per volontà del Segnalante.

Segnalazione Interna: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite i canali di segnalazione interna di cui al Capitolo 5 della Procedura.

Segnalazione Esterna: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite i canali di segnalazione esterna indicati al Capitolo 5 della Procedura.

Segnalazione whistleblowing: la segnalazione di una violazione che rientra nell'ambito applicativo definito agli artt. 2 e 3 del D.lgs. 24/2023.

Segnalazioni Ordinarie: sono le segnalazioni che si riferiscono a comportamenti, atti od omissioni che non rientrano nell'ambito di applicazione di cui al Decreto whistleblowing che tuttavia siano relative a: (a) un reato o un illecito, una violazione o un tentativo di nascondere una violazione di un impegno internazionale regolarmente ratificato o approvato dall'Italia; (b) una violazione di un atto unilaterale di un'organizzazione internazionale adottato sulla base di un impegno internazionale regolarmente ratificato.

Violazioni: i comportamenti e gli illeciti richiamati dalla Procedura al paragrafo n. 4.2.

2. DESTINATARI DELLA PROCEDURA WHISTLEBLOWING

La Procedura whistleblowing si rivolge ai Destinatari. In particolare:

a. agli organi sociali, nonché ai titolari di qualifiche formali (di direzione, gestione e controllo di Ksenia Security o di una unità organizzativa delle stesse) riconducibili alla definizione di "soggetti apicali";
b. ai soggetti che esercitano tali funzioni (di direzione, gestione e controllo) anche solo di fatto;
c. a tutto il personale di Ksenia Security, intendendo per tale: (*i*) i dipendenti subordinati, incluso il top management; (*ii*) i soggetti che, pur non essendo legati a Ksenia Security da un rapporto di lavoro subordinato, pongono in essere la propria attività nell'interesse e per conto della Società, sotto la direzione della stessa (e.g. collaboratori legati da contratto a termine, collaboratori atipici e in stage, lavoratori parasubordinati in genere); (*iii*) chiunque agisca in nome e per conto di Ksenia Security e/o sotto la sua direzione e vigilanza;
d. ai soggetti esterni che, in forza di rapporti contrattuali, prestano la loro collaborazione a Ksenia Security per la realizzazione delle proprie attività. Per soggetti esterni si intendono, a titolo esemplificativo e non esaustivo: i lavoratori autonomi, i professionisti, i consulenti, i fornitori e i partner commerciali.

3. PRINCIPI GENERALI

La Procedura si basa sui seguenti principi fondamentali: (*i*) la protezione dalle Segnalazioni in malafede; (*ii*) la protezione del Segnalante; (*iii*) la tutela della riservatezza della Segnalazione.
Le persone coinvolte nella presente Procedura whistleblowing operano nel rispetto del sistema normativo e organizzativo, dei poteri e delle deleghe interne e sono tenute ad operare in conformità con la legge ed i regolamenti vigenti e nel rispetto dei principi di seguito riportati:
Conoscenza e consapevolezza
La Procedura whistleblowing rappresenta un elemento fondamentale per garantire piena consapevolezza ed un efficace presidio dei rischi, nonché per orientare i mutamenti della strategia e del contesto organizzativo.
Protezione dalle segnalazioni in malafede
Tutti i soggetti sono tenuti al rispetto della dignità, dell'onore e della reputazione di ciascuno. A tal fine, è fatto obbligo al Segnalante di dichiarare se ha un interesse privato collegato alla Segnalazione. Più in generale è garantita adeguata protezione dalle Segnalazioni in "malafede", sono censurate simili condotte e si informa

© Ksenia Security S.p.A.

che le Segnalazioni inviate allo scopo di danneggiare e/o altrimenti recare pregiudizio, nonché ogni altra forma di abuso sono fonte di responsabilità, in sede disciplinare e nelle altre sedi competenti. Nell'ambito delle Segnalazioni whistleblowing i soggetti segnalati godono delle tutele previste dal Decreto whistleblowing.

Imparzialità, autonomia e indipendenza di giudizio

Tutti i soggetti che ricevono, esaminano e valutano le Segnalazioni sono in possesso di requisiti morali e professionali e assicurano il mantenimento delle necessarie condizioni di indipendenza e dovuta obiettività, competenza e diligenza nello svolgimento delle loro attività.

Tutela della riservatezza

Ksenia Security (e, per conto di essa, tutti i soggetti che prendono parte al processo di whistleblowing), in ogni fase e attività disciplinata dalla presente Procedura, tutela rigorosamente la riservatezza delle Informazioni sulla Violazione, dell'identità del Segnalante e delle altre persone (fisiche o giuridiche) ad esso collegate (e.g. Facilitatori), nonché della Persona Coinvolta, in stretta aderenza al disposto dell'art. 12 del Decreto whistleblowing e nella più scrupolosa osservanza dei limiti ed obblighi di legge applicabili al caso concreto.

4. COSA SI PUÒ SEGNALARE?

4.1 Contenuto delle segnalazioni

Le Segnalazioni devono essere circostanziate e fondate su elementi di fatto precisi e concordanti. Si invitano i Segnalanti a fornire il maggior numero di informazioni possibili (inclusi tutti gli elementi utili a consentire ai soggetti preposti di effettuare le verifiche necessarie per accertare la fondatezza dei fatti segnalati), ma non è indispensabile che la persona segnalante disponga di prove sufficienti a dimostrare il fatto riportato.

Fatto salvo il diritto all'anonimato del Segnalante, le Segnalazioni dovrebbero contenere i seguenti elementi:

- le generalità del soggetto che effettua la Segnalazione, con indicazione della posizione o funzione svolta nell'ambito di Ksenia Security, o del rapporto che lo lega a quest'ultima (qualora non si effettui una segnalazione anonima);
- una chiara e completa descrizione dei fatti oggetto della Segnalazione (i.e., segnalato, oggetto, modalità della condotta illecita, natura periodica o continuativa della Segnalazione);
- se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi o potrebbero essere commessi i fatti segnalati;
- se conosciute, le generalità o comunque altri elementi che consentano di identificare il soggetto cui è ascritta la condotta segnalata (e.g. qualifica, rapporto di lavoro, etc.);
- potenziali testimoni o altri elementi di prova (e.g. fotografie/screenshots, copia di documenti, etc.);
- ogni altra informazione utile a riscontrare la sussistenza dei fatti segnalati.

È consentita la possibilità di presentare Segnalazioni anonime, tenendo tuttavia in considerazione che, laddove fossero necessarie ulteriori informazioni per verificare le Violazioni segnalate, la condizione di anonimato potrebbe comportare l'impossibilità di stabilire un contatto con il Segnalante (anonimo). Laddove non sia possibile accertare autonomamente i fatti, si potrebbe arrivare all'archiviazione della verifica. In ogni caso, come spiegato nel pertinente paragrafo (v. *infra*, par. 9.2 e 9.3), le tutele previste dalla normativa (e dalla Procedura) contro misure o atti ritorsivi sono estese, al ricorrere delle condizioni richieste, anche ai Segnalanti anonimi la cui identità sia comunque emersa a seguito della Segnalazione.

La Procedura whistleblowing si applica sia per la gestione delle Segnalazioni whistleblowing sia per la gestione delle Segnalazioni Ordinarie, ma le tutele previste dal Decreto whistleblowing saranno applicabili, nelle condizioni ivi previste, solo alle prime.

4.2 Tipologia di violazioni rilevanti ai sensi del Decreto Whistleblowing

Ai sensi degli articoli 2 e 3 del Decreto whistleblowing per i soggetti del settore privato – tra i quali rientra anche Ksenia Security – le violazioni oggetto di segnalazione si riferiscono a comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

© Ksenia Security S.p.A.

A) *Violazioni delle disposizioni normative nazionali:*

- illeciti penali, civili, amministrativi o contabili diversi rispetto a quelli specificamente individuati come violazioni del diritto UE, come sotto meglio definite;
- condotte illecite rilevanti ai sensi del Decreto 231 o violazioni del Modello 231 o del Codice Etico.

A titolo esemplificativo e non esaustivo si pensi a:

- reati (e.g. corruzione, frode, malversazione, furto, appropriazione indebita);
- violazione della normativa antitrust o della normativa in materia di commercio internazionale;
- violazioni di diritti umani, molestie sessuali o violazione della normativa anti-discriminazione;
- violazione della normativa ambientale;
- violazioni gravi di obblighi di riservatezza;
- atti od omissioni che causano pregiudizi economici rilevanti alla Società;
- atti od omissioni che causano pregiudizi rilevanti all'immagine di Ksenia Security (e.g. che abbiano una risonanza mediatica negativa a livello nazionale e/o internazionale);
- atti od omissioni che determinino la risoluzione di contratti esistenti (o l'esclusione da futuri contratti, e.g. inserimento in black-list, interdizione dallo svolgimento di attività economiche, classificazione come "soggetto non gradito" o simili);
- atti od omissioni che determinino l'avvio di procedimenti da parte di soggetti pubblici (e.g. autorità indipendenti, procure);
- gravi violazioni dell'obbligo di coinvolgimento di membri del Consiglio di amministrazione o dirigenti (in particolare, violazione degli obblighi di supervisione e controllo).

B) *Violazioni della normativa europea*

- illeciti commessi in violazione della normativa dell'UE indicata nell'Allegato 1 al Decreto whistleblowing e di tutte le disposizioni nazionali che ne danno attuazione (anche se queste ultime non sono espressamente elencate nel citato allegato). Si precisa che le disposizioni normative contenute nell'Allegato 1 sono da intendersi come un riferimento dinamico in quanto vanno naturalmente adeguate al variare della normativa stessa.
  In particolare, si tratta di illeciti relativi ai seguenti settori: contratti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi.
  A titolo esemplificativo, si pensi ai cd. reati ambientali, quali, scarico, emissione o altro tipo di rilascio di materiali pericolosi nell'aria, nel terreno o nell'acqua oppure raccolta, trasporto, recupero o smaltimento illecito di rifiuti pericolosi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione Europea (art. 325 del TFUE lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'UE) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE.
  Si pensi, ad esempio, alle frodi, alla corruzione e a qualsiasi altra attività illegale connessa alle spese dell'Unione;
- atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE).
  Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle imprese e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle imprese;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori indicati ai punti precedenti. In tale ambito vanno ricondotte, ad esempio, le pratiche abusive quali definite dalla giurisprudenza della Corte di Giustizia dell'UE.

© Ksenia Security S.p.A.

5. DOVE POSSO EFFETTUARE LA SEGNALAZIONE?

I Destinatari della presente Procedura possono liberamente decidere di effettuare una Segnalazione tramite (*i*) i canali interni messi a disposizione da Ksenia Security e, al ricorrere dei presupposti di cui si dirà infra, (*ii*) tramite i canali ANAC o (*iii*) tramite divulgazione pubblica e/o denuncia all'Autorità Giudiziaria.

5.1 Canale di segnalazione interna

Piattaforma informatica
Ksenia Security mette a disposizione dei Destinatari una piattaforma informatica raggiungibile al seguente link:

https://private.mygovernance.it/mywhistleblowing/ksenia/54468

dedicata alla segnalazione di Violazioni, ai sensi del Decreto whistleblowing, che consente di effettuare segnalazioni (*i*) in forma scritta, (*ii*) mediante registrazione vocale e (*iii*) richiedendo la fissazione di un incontro di persona.
È prevista la possibilità di effettuare le Segnalazioni anche in forma anonima, fermo quanto già osservato (*v. supra*, par. 4.1) circa i limiti all'accertamento dei fatti potenzialmente derivanti da tale condizione.
La persona che intende segnalare una Violazione può:

- accedere alla piattaforma tramite il link indicato;
- cliccare sul pulsante "segnala" e scegliere se effettuare la segnalazione in forma scritta, in forma orale oppure richiedendo un incontro di persona.

Una volta completata ed inviata la Segnalazione, il Segnalante otterrà un codice identificativo (c.d. token) quale credenziale personale per accedere, sempre tramite il medesimo link, all'area dedicata alla sua Segnalazione e monitorare lo stato di avanzamento della Segnalazione, integrare la segnalazione effettuata con informazioni aggiuntive, nonché scambiare messaggi privati con l'incaricato della gestione delle segnalazioni, mantenendo la massima riservatezza.

© Ksenia Security S.p.A.

Sempre attraverso la piattaforma:

- è possibile allegare documentazione a supporto della propria Segnalazione;
- l'avviso di presa in carico della Segnalazione verrà comunicata al Segnalante entro sette giorni dalla sua effettuazione;
- entro tre mesi dal ricevimento dell'avviso di presa in carico della Segnalazione, il Gestore fornisce un riscontro sulla medesima (*e.g.,* risultanze, azioni intraprese, eventuale archiviazione) al Segnalante.

5.2 Segnalazioni trasmesse su canali e/o a soggetto non competente

Eventuali segnalazioni che dovessero pervenire al di fuori dei canali di cui sopra e/o a soggetti diversi da quello competente ad esaminarle saranno trasmesse, entro sette giorni dal loro ricevimento, al Gestore delle Segnalazioni dandone contestuale notizia al Segnalante.

5.3 Canale esterno (ANAC)

Condizioni per la Segnalazione Esterna
A determinate condizioni è possibile trasmettere una segnalazione esterna all'ANAC ed usufruire della tutela prevista dal Decreto whistleblowing.
La persona segnalante può effettuare una Segnalazione Esterna se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

1. i canali di segnalazione interni previsti dalla presente Procedura non sono attivi;
2. il Segnalante ha già effettuato una Segnalazione Interna e la stessa non ha avuto seguito;
3. il Segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero possa determinare il rischio di ritorsione;
4. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Canale di Segnalazione Esterna
Per effettuare una Segnalazione Esterna è necessario accedere, al servizio whistleblowing sul sito istituzionale di ANAC (https://www.anticorruzione.it/-/whistleblowing) che prevede la possibilità:

- di effettuare una segnalazione tramite apposita piattaforma informatica ANAC;
- di effettuare una segnalazione orale, utilizzando il servizio con operatore specializzato;
- richiedere un incontro di persona con il personale ANAC entro un termine ragionevole.

Tutte le informazioni necessarie all'utilizzo dei canali di segnalazione di cui sopra sono reperibili dai Destinatari nelle Linee Guida ANAC (v. ivi, Parte Seconda, pp. 50 e ss.), all'indirizzo https://www.anticorruzione.it/-/del.311.2023.linee.guida.whistleblowing

© Ksenia Security S.p.A.

5.4 Divulgazione pubblica e denuncia all'autorità giudiziaria

Divulgazione pubblica
Con la Divulgazione Pubblica le informazioni sulle Violazioni sono rese di pubblico dominio tramite la stampa o mezzi elettronici o di diffusione in grado di raggiungere un numero elevato di persone. Potrà procedersi alla Divulgazione Pubblica, usufruendo comunque delle tutele previste dal Decreto Whistleblowing, se ricorre almeno una delle seguenti condizioni:

1. ad una Segnalazione Interna a cui l'amministrazione/ente non abbia dato riscontro nei termini previsti abbia fatto seguito una Segnalazione Esterna ad ANAC la quale, a sua volta, non ha fornito riscontro al Segnalante entro termini ragionevoli;
2. la persona ha già effettuato direttamente una Segnalazione Esterna ad ANAC la quale, tuttavia, non ha dato riscontro al Segnalante entro termini ragionevoli;
3. la persona effettua direttamente una Divulgazione Pubblica in quanto ha fondato motivo di ritenere, ragionevolmente, sulla base di circostanze concrete, e quindi non su semplici illazioni, che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse;
4. la persona effettua direttamente una Divulgazione Pubblica poiché ha fondati motivi di ritenere che la Segnalazione Esterna possa comportare il rischio di ritorsioni o non avere efficace seguito.

Denuncia all'Autorità Giudiziaria
Il Decreto whistleblowing, in conformità alla precedente disciplina, riconosce ai soggetti tutelati anche la possibilità di rivolgersi alle Autorità Giudiziarie, per inoltrare una denuncia di condotte illecite di cui siano venuti a conoscenza in un contesto lavorativo pubblico o privato rilevante per l'applicazione del D.Lgs. 24/2023.
Si precisa che, qualora il Segnalante rivesta la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, anche laddove lo stesso abbia effettuato una segnalazione attraverso i canali interni o esterni previsti dal decreto, ciò non lo esonera dall'obbligo – in virtù di quanto previsto dal combinato disposto dell'art. 331 c.p.p. e degli artt. 361 e 362 c.p. – di denunciare alla competente Autorità Giudiziaria i fatti penalmente rilevanti e le ipotesi di danno erariale.

6. COME VIENE GESTITA LA SEGNALAZIONE INTERNA?

6.1 Gestore della segnalazione

Ksenia Security ritiene di individuare nell'Organismo di Vigilanza ("**OdV**") della Società l'organo deputato a gestire il processo di segnalazione (il "**Gestore delle Segnalazioni**" o anche solo "**Gestore**").
Le verifiche e gli accertamenti successivi alla ricezione della Segnalazione sono svolti dal Gestore con l'eventuale supporto degli organi aziendali di volta in volta interessati dalla segnalazione e/o di consulenti esterni, estendendo ad essi l'obbligo di tutelare la riservatezza del Segnalante, della Persona Coinvolta e delle Informazioni sulla Violazione.
Qualora all'esito delle verifiche svolte emerga la fondatezza della Segnalazione potrà procedersi all'instaurazione di un procedimento sanzionatorio nei confronti della Persona Coinvolta nel rispetto della normativa, della contrattazione collettiva eventualmente applicabile e del Modello 231.

6.2 Processo di gestione della segnalazione

Più nello specifico, il processo di gestione della Segnalazione è articolato come segue.

- *FASE 1 – AVVIO DELL'INDAGINE*: il processo di gestione della Segnalazione viene avviato nel momento in cui il Gestore viene a conoscenza della Segnalazione attraverso i canali sopramenzionati.

© Ksenia Security S.p.A.

Appena ricevuta, e comunque **entro sette giorni dalla data di ricezione**, il Gestore:

- valuta l'eventuale presenza di conflitti d'interesse che possano minare l'indipendenza e l'imparzialità nella gestione della Segnalazione;
- rilascia al Segnalante avviso di ricevimento della Segnalazione.

Qualora vi sia un conflitto d'interesse, il Gestore viene escluso dalla gestione della Segnalazione, informando la funzione Quality Assurance & Compliance, che provvederà essa stessa a gestire la Segnalazione in conformità alla presente Procedura.

- *FASE 2 – VALUTAZIONE PRELIMINARE:* il Gestore, a seguito della Fase 1, effettua una prima valutazione relativa alla riconducibilità della Segnalazione nell'ambito del Decreto whistleblowing. All'esito può decidere di:
  - chiedere al Segnalante ulteriori informazioni/integrazioni, specialmente se quanto segnalato non sia adeguatamente circostanziato per valutare la rilevanza della Segnalazione ai sensi del Decreto whistleblowing; oppure
  - archiviare:
    - in caso di Segnalazione non rilevante ai sensi del Decreto whistleblowing; se rilevante per altre tematiche riguardanti l'attività della Società, informa le persone competenti per l'ambito di riferimento;
    - per manifesta infondatezza/assenza di elementi idonei a giustificare accertamenti;
    - se accerta il contenuto generico della Segnalazione, tale da impedire la comprensione dei fatti, e/o la documentazione non sia appropriata.
  - procedere alla Valutazione nel merito in presenza di una Segnalazione rilevante ai sensi del Decreto whistleblowing.

  In ogni caso, ai sensi dell'art. 5, comma 1, lett. D) del D.Lgs. 24/2023, il Gestore fornisce un **riscontro alla Segnalazione**, direttamente al Segnalante, **entro tre mesi dalla data dell'avviso di ricevimento**. In mancanza di tale avviso, il riscontro in questione è trasmesso al Segnalante entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della Segnalazione.

- *FASE 3 – VALUTAZIONE NEL MERITO*: il Gestore, a seguito della Fase 2, valutata la pertinenza della Segnalazione al Decreto whistleblowing, procede:
  - con l'attività di indagine e di analisi del merito, anche attraverso il supporto delle competenti funzioni aziendali e/o tramite l'ausilio di consulenti nel rispetto dei principi di imparzialità e riservatezza (secondo le previsioni dell'art. 12 del Decreto whistleblowing), nonché con ogni attività ritenuta opportuna (anche dal punto di vista costi-benefici), inclusa l'audizione del Segnalante e/o eventuali altri soggetti che possano riferire sui fatti segnalati. Per quanto concerne la Persona Coinvolta, invece, la comunicazione circa l'avvio e l'esito dell'indagine avviene solo nel caso in cui emerga la necessità di adottare specifici provvedimenti nei suoi confronti e in ogni caso, nel rispetto dello Statuto dei Lavoratori e del CCNL di riferimento, oppure per necessità istruttorie. Ai sensi dell'art. 12 comma 9 Del Decreto whistleblowing, la Persona Coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche con procedimento cartolare (i.e. acquisizione osservazioni scritte e documenti);
  - a formalizzare entro tre mesi dalla data dell'avviso di ricevimento (o in mancanza, entro tre mesi dalla scadenza del termine di sette giorni dalla data di presentazione della Segnalazione) gli esiti degli accertamenti svolti in un apposito documento. Tale documento deve indicare, a titolo esemplificativo e non esaustivo, i seguenti elementi:
    - i dati della Segnalazione;
    - le verifiche svolte, gli esiti delle stesse ed eventuali soggetti terzi coinvolti (interni e/o esterni a Ksenia Security) coinvolti nell'espletamento delle stesse;
    - la valutazione di sintesi con specifica indicazione della condotta illecita accertata o non accertata e delle relative valutazioni.
  - a fornire il riscontro al Segnalante entro i termini di cui sopra.

© Ksenia Security S.p.A.

- *FASE 4 – CONCLUSIONE DELL'INDAGINE*: terminata l'attività della Fase 3, il Gestore deve comunicare l'esito, tramite una relazione scritta, dettagliando l'attività svolta al Consiglio di Amministrazione:
  - in caso di esito negativo, archiviando l'indagine;
  - in caso di esito positivo, suggerendo l'eventuale applicazione di sanzioni disciplinari e/o azioni nei confronti di soggetti terzi all'organizzazione.

- *FASE 5 – MONITORAGGIO E AZIONI SUCCESSIVE*: se dalla Fase 4 dovesse emergere la necessità di azioni correttive sul sistema di controllo interno è responsabilità del management delle aree/processi oggetto di verifica redigere un piano per la rimozione delle criticità rilevate; il Gestore monitora lo stato di attuazione delle azioni correttive.
  Il Gestore tiene traccia di tutte le Segnalazioni ricevute, con indicazione, a titolo meramente indicativo, ma non esaustivo, dei seguenti elementi: (*i*) tipologia di Segnalazione ricevuta (i.e. irregolarità amministrative, frodi, corruzioni etc.); (*ii*) Segnalato e Segnalante; (*iii*) data di ricezione e valutazione della Segnalazione; (*iv*) valutazione preliminare e relativa motivazione.
  La documentazione relativa alle Segnalazioni, predisposta e/o pervenuta durante il processo di gestione delle stesse, è strettamente confidenziale. Tale documentazione è archiviata e conservata nel rispetto delle norme vigenti da parte del Gestore.
  Le Segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della Segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della Segnalazione, nel rispetto degli obblighi di riservatezza di cui all'art. 12 del Decreto whistleblowing e del principio di cui agli artt. 5(1)(e), del GDPR e 3, comma 1, lettera e), del Codice Privacy, fatti salvi tempi di conservazione più lunghi determinati da richieste/ordini delle Autorità o dalla difesa dei diritti di Ksenia Security in giudizio.

7. CONFLITTO DI INTERESSI

Qualora la Segnalazione dovesse coinvolgere, anche indirettamente (e.g. quali testimoni dei fatti) il Gestore delle Segnalazioni, minando quindi l'indipendenza e l'imparzialità nella gestione della Segnalazione, il soggetto in conflitto verrà esonerato dall'incarico di gestire la Segnalazione.
Alcuni esempi di conflitto di interesse:

- il Gestore sia il presunto responsabile della violazione;
- il Gestore abbia un potenziale interesse correlato alla Segnalazione tale da compromettere l'imparzialità e l'indipendenza di giudizio;
- il Gestore sia testimone dei fatti oggetto della Segnalazione.

Una volta rilevato il conflitto di interesse, ancorché potenziale, è inibita la visualizzazione di qualsiasi informazioni pertinente alla Segnalazione al soggetto in conflitto ed è fatto allo stesso di gestire e/o influenzare in alcun modo la Segnalazione.
La funzione Quality Assurance & Compliance gestirà la Segnalazione sostituendo il Gestore e seguendo le indicazioni previste all'interno della presente Procedura.

8. OBBLIGO DI RISERVATEZZA

Le Segnalazioni (e le informazioni in esse contenute) non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.
L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del GDPR e dell'art. 2-quaterdecies del Codice Privacy.

© Ksenia Security S.p.A.

Ksenia Security adotta le medesime modalità di tutela previste a garanzia della privacy del Segnalante anche per il presunto responsabile della violazione, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge che imponga l'obbligo di comunicare il nominativo del segnalato (*e.g.*, le richieste dell'Autorità giudiziaria, etc.).
Nell'ambito del procedimento disciplinare:

- l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.
- qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione dell'identità.
- in quest'ultimo caso, è dato avviso alla persona segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati quando la rivelazione della identità della persona segnalante e/o delle informazioni da cui essa può ricavarsi è indispensabile anche ai fini della difesa della persona coinvolta.

Il Gestore delle Segnalazioni tutela altresì l'identità delle Persone Coinvolte e delle persone menzionate nella Segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione stessa, nel rispetto delle medesime garanzie previste in favore del Segnalante (v. *infra*, Cap. 9).

9. TUTELA DEL SEGNALANTE E DELLE PERSONE COLLEGATE

9.1 Riservatezza del segnalante

Al fine di incoraggiare la Segnalazione di eventuali illeciti, Ksenia Security garantisce la riservatezza del Segnalante anche al fine di preservarlo da eventuali ritorsioni interne o atti discriminatori.
In particolare, la Società garantisce che l'identità del Segnalante non possa essere rivelata senza il suo espresso consenso e che tutti i soggetti coinvolti nella gestione della Segnalazione siano tenuti a tutelarne la riservatezza, ad esclusione dei casi di seguito indicati:

- qualora sia configurabile una responsabilità del Segnalante a titolo di calunnia o di diffamazione ai sensi delle disposizioni del Codice penale;
- il Segnalante incorra in responsabilità civile ai sensi dell'art. 2043 del Codice civile;
- nelle ipotesi in cui l'anonimato non sia opponibile per legge.

La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge.

9.2 Divieto di ritorsione

Il Decreto whistleblowing prevede, a tutela del Segnalante, il divieto di ritorsione definita come «qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto». Si tratta quindi di una definizione ampia del concetto di ritorsione che può consistere sia in atti o provvedimenti che in comportamenti od omissioni che si verificano nel contesto lavorativo e che arrecano pregiudizio ai soggetti tutelati. La ritorsione può essere anche "solo tentata o minacciata".
Segue un'elencazione delle ritorsioni, pur tuttavia con carattere non esaustivo:

- licenziamento, sospensione o misure equivalenti;
- retrocessione di grado o mancata promozione;
- mutamento di funzioni, cambiamento del luogo/orario di lavoro, riduzione dello stipendio;
- sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- note di demerito o referenze negative;
- adozione di misure disciplinari o di altra sanzione, anche pecuniaria;

© Ksenia Security S.p.A.

- coercizione, intimidazione, molestie o ostracismo;
- discriminazione o comunque trattamento sfavorevole;
- mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- mancato rinnovo o risoluzione anticipata di un contratto di lavoro a termine;
- danni, anche alla reputazione della persona, in particolare sui social media, o pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;
- annullamento di una licenza o di un permesso;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità di trovare un'occupazione in futuro;
- richiesta di sottoposizione ad accertamenti psichiatrici o medici.

9.3 Condizioni per beneficiare delle misure di protezione

L'applicazione del regime di protezione contro le ritorsioni prevista dal Decreto whistleblowing è subordinata ad alcune condizioni e requisiti:

a. il soggetto che ha segnalato, denunciato o ha effettuato la Divulgazione Pubblica in base ad una convinzione ragionevole che le informazioni sulle violazioni segnalate, divulgate o denunciate siano veritiere e rientranti nell'ambito di applicazione del Decreto whistleblowing;
b. la Segnalazione, la Denuncia o la Divulgazione Pubblica è stata effettuata nel rispetto della disciplina prevista dal Decreto whistleblowing e di cui anche alla presente Procedura;
c. è necessario un rapporto di consequenzialità tra Segnalazione, Divulgazione Pubblica e denuncia effettuata all'Autorità Giudiziaria e le Misure Ritorsive subite;
d. non sono sufficienti invece i meri sospetti o le "voci di corridoio".

Non rilevano la certezza dei fatti né i motivi personali che hanno indotto il soggetto a segnalare, a denunciare o ad effettuare la Divulgazione Pubblica. In difetto delle condizioni di cui sopra le Segnalazioni, Divulgazioni Pubbliche e denunce non rientrano nell'ambito della disciplina di whistleblowing e quindi la tutela prevista non troverà applicazione.
La protezione prevista in caso di ritorsioni non si applica in caso di accertamento con sentenza, anche non definitiva di primo grado nei confronti del Segnalante, della responsabilità penale per i reati di calunnia o diffamazione o comunque per i medesimi reati commessi con la denuncia, ovvero della responsabilità civile, per aver riferito informazioni false riportate intenzionalmente con dolo o colpa. Nei casi di accertamento delle dette responsabilità, al Segnalante e denunciante è inoltre applicata una sanzione disciplinare.
Per effetto delle misure di protezione previste dagli art. 17 e ss. Del Decreto whistleblowing i Segnalanti, ove abbiano rispettato la disciplina prevista per la segnalazione della violazione e versino nelle condizioni, anche di buona fede soggettiva, previste dalla medesima, non possono subire alcuna Ritorsione in ragione dell'avvenuta presentazione della Segnalazione.

9.4 Ulteriori soggetti cui sono estese le misure di protezione

Le misure di protezione previste dal Decreto whistleblowing si applicano anche:

- ai Facilitatori che hanno assistito il Segnalante nel processo di segnalazione;
- alle persone del medesimo contesto lavorativo del Segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile ovvero di colui che ha effettuato una Divulgazione Pubblica e che sono legate ad essi da uno stabile legame affettivo/parentela entro il quarto grado;
- ai colleghi di lavoro del Segnalante o della persona che ha sporto una denuncia all'Autorità giudiziaria o contabile o ha effettuato una Divulgazione Pubblica, che lavorano nel medesimo contesto lavorativo e che hanno con detta persona un rapporto abituale e corrente;

© Ksenia Security S.p.A.

- agli enti di proprietà del Segnalante (o di colui che ha effettuato una denuncia all'autorità giudiziaria o contabile o ha effettuato una Divulgazione Pubblica) o per i quali egli lavora, nonché agli enti che operano nel medesimo contesto lavorativo del Segnalante.

9.5 Contenuto delle misure di protezione

Con specifico riferimento al contenuto della protezione, gli artt. 17 e ss. Del Decreto Whistleblowing prevedono che:

a. nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati ai sensi del presente articolo nei confronti delle persone segnalanti (e/o dalle altre persone, a loro legate, cui è esteso il regime di protezione), si presume che siano stati posti in essere a causa della Segnalazione o denuncia all'autorità giudiziaria o contabile. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee è a carico chi li ha realizzati;
b. in caso di domanda risarcitoria presentata all'autorità giudiziaria dai Segnalanti (e/o dalle altre persone cui è esteso il regime di protezione) se dimostrano di aver effettuato, ai sensi del Decreto whistleblowing, una Segnalazione, una Divulgazione Pubblica o una denuncia all'autorità giudiziaria o contabile e di aver subito un danno, si presume, salvo prova contraria, che il danno sia conseguenza della Segnalazione, Divulgazione Pubblica o denuncia all'Autorità;
c. le rinunce e le transazioni, integrali o parziali, che hanno per oggetto i diritti e le tutele previsti dal Decreto whistleblowing non sono valide, salvo che siano effettuate nelle forme e nei modi di cui all'articolo 2113, quarto comma, del Codice civile.

Le misure o atti ritorsivi eventualmente subiti dalle persone segnalanti (e/o dalle altre persone, a loro legate, cui è esteso il regime di protezione) possono essere comunicate dagli interessati all'ANAC che, ove le riscontri, potrà applicare le sanzioni previste dall'art. 21 del Decreto whistleblowing.

10. COMUNICAZIONE DEI RISULTATI E REPORTISTICA

I risultati complessivi delle attività di gestione delle Segnalazioni, incluse le verifiche e i provvedimenti sanzionatori eventualmente adottati, sono condivisi dal Gestore nell'ambito del reporting periodico al Consiglio di Amministrazione di Ksenia Security, ovvero laddove da questi richiesto.
In particolare, il Gestore fornisce all'organo amministrativo della Società (annualmente, o con altre tempistiche eventualmente definite da quest'ultimo) un apposito report riepilogativo delle segnalazioni pervenute, contenente l'esito delle analisi, inclusa l'adozione (o la mancata adozione) di provvedimenti disciplinari da parte di Ksenia Security.

11. TRATTAMENTO DEI DATI PERSONALI

Nell'ambito del processo descritto nella Procedura, Ksenia Security potrà trattare eventuali dati personali, relativi sia al soggetto segnalante – salvo non ricorra alla Segnalazione anonima (al riguardo v. *supra*, par. 4.1) – sia alle ulteriori persone fisiche coinvolte e menzionate nella Segnalazione (e.g. Persona Coinvolta). Inoltre, qualora a seguito delle verifiche scaturite dalla Segnalazione risultasse fondata la condotta illecita, i dati personali raccolti potranno essere trattati anche per la difesa di un diritto in sede giudiziaria da parte della Società.
La fonte da cui saranno raccolti gli eventuali dati personali è il Segnalante (c.d. *whistleblower*).
Ksenia Security potrebbe trattare le seguenti categorie di dati personali:

a. dati c.d. comuni (e.g. nome, cognome, dati di contatto, etc.) relativi al Segnalante e alle persone indicate nella Segnalazione;
b. ogni altra informazione, qualificabile quale dato personale, che il Segnalante dovesse decidere di condividere con la Società per meglio circostanziare la propria Segnalazione (tali dati, potrebbero includere anche categorie particolari di dati personali o dati relativi a condanne penali e reati).

© Ksenia Security S.p.A.

Il trattamento dei dati personali è lecito ai sensi degli artt. 6(1)©, 9(2)(b) e 10 del GDPR (D.Lgs. n. 24/2023 e Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23/10/19).
Qualora i dati personali raccolti nell'ambito della Segnalazione, venissero trattati per accertare, esercitare o difendere un diritto in sede giudiziaria, il trattamento è lecito ai sensi degli artt. 6(1)(f), 9(2)(f) del GDPR e 2-octies, comma 3, del Codice Privacy.
I dati personali che dovessero essere manifestamente non utili al trattamento di una specifica Segnalazione non saranno raccolti o, se raccolti accidentalmente, saranno cancellati immediatamente.
Il trattamento è effettuato da Ksenia Security, tramite soggetti interni all'organizzazione del Titolare appositamente autorizzati e istruiti a svolgere le attività di trattamento descritte nella presente Procedura, nonché da soggetti esterni alla Società che, per conto della Società medesima, svolgono servizi di varia natura e che appartengono alle categorie di seguito indicate.
I dati potranno essere comunicati alle seguenti categorie di destinatari:

- responsabili del trattamento, ex art. 28 del GDPR, di volta in volta nominati (e.g. società di gestione della piattaforma utilizzata per le Segnalazioni);
- Organismo di Vigilanza, ex D.Lgs. n. 231/2001 di Ksenia Security;
- Organi sociali di Ksenia Security;
- Società e professionisti di cui la Società si avvale per la tutela di un proprio diritto (e.g. avvocati, investigatori privati, consulenti tecnici, ecc.);
- giudici e tribunali, in ragione di qualsiasi richiesta o nell'ambito di un processo;
- autorità pubbliche autorizzate dalla legge, per verifiche, accertamenti e/o ispezioni.

L'elenco completo di tali soggetti o categorie di soggetti è disponibile presso la sede del Titolare.
Tutti gli interessati a cui si riferiscono i dati personali trattati da Ksenia Security potranno esercitare i diritti previsti ai sensi degli artt. Da 15 a 22 e 77 del GDPR, nei limiti di quanto previsto dall'articolo 2-undecies del Codice Privacy. Eventuali richieste avanzate, per l'esercizio dei diritti, potranno essere inoltrate a Ksenia Security.
Il reclamo all'Autorità (Garante) potrà essere promosso secondo le modalità indicate dalla stessa. I dati personali non saranno trasferiti al di fuori dell'Unione Europea e/o dello Spazio Economico Europeo (SEE).

12. CONSERVAZIONE DELLA DOCUMENTAZIONE

Le Segnalazioni Interne, e la relativa documentazione sono conservate per il tempo necessario alle finalità di trattamento, indicate nella presente Procedura, e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura, nel rispetto degli obblighi di riservatezza, ai sensi degli artt. 12 del Decreto whistleblowing, 5(1)(e) del GDPR e 3, comma 1, lettera e), del Decreto Legislativo n. 51 del 2018.
Se per la Segnalazione si utilizza il sistema di messaggistica vocale, la stessa verrà registrata garantendo l'anonimato del Segnalante, attraverso sistemi di manipolazione della voce del Segnalante (c.d. morphing vocale).
Quando, su richiesta del Segnalante, la Segnalazione è effettuata oralmente in un incontro con il personale addetto, essa, previo consenso del Segnalante, è documentata a cura dal personale mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto o con verbale. In caso di verbale, il Segnalante può verificare, rettificare e confermare il verbale dell'incontro con la propria sottoscrizione.

13. FORMAZIONE

I Destinatari devono rispettare la presente Procedura e partecipare alle sessioni di formazione in merito al Decreto whistleblowing.

© Ksenia Security S.p.A.

14. SANZIONI DISCIPLINARI E ALTRI PROVVEDIMENTI

Ksenia Security provvederà a sanzionare ogni comportamento illecito in linea con le previsioni del Decreto whistleblowing, ascrivibile al personale della Società, che dovesse emergere a seguito di attività di verifica di Segnalazioni, condotte secondo quanto previsto dalla presente Procedura, al fine di impedire eventuali condotte che violino la legge e/o il presente documento da parte del medesimo personale della Società.
I provvedimenti disciplinari, come previsto dalla legge e dalla contrattazione collettiva applicabile, saranno proporzionati all'entità e gravità dei comportamenti illeciti accertati e potranno giungere sino alla risoluzione del rapporto di lavoro.
Di seguito sono indicate, a titolo esemplificativo, alcune delle condotte che possono essere oggetto di un procedimento disciplinare:

a. condotte ritorsive nei confronti del Segnalante e/o del Facilitatore;
b. condotte che ostacolino o tentino di ostacolare la Segnalazione;
c. violazione dell'obbligo di riservatezza di cui all'art. 12 del Decreto whistleblowing;
d. mancata verifica e analisi delle Segnalazioni ricevute;
e. diffamazione e/o calunnie compiute dal Segnalante, rilevate anche con sentenza di primo grado, oppure denunciate all'autorità giudiziaria o contabile (anche nel caso di responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave).

15. PUBBLICAZIONE E DIFFUSIONE DELLA PROCEDURA WHISTLEBLOWING

La presente Procedura è pubblicata sul sito web aziendale di Ksenia Security:

https://www.kseniasecurity.com/

Della adozione e pubblicazione della Procedura whistleblowing viene data informativa a tutto il personale della Società tramite comunicazione interna, rinviando alla presente per ogni disposizione di dettaglio.

© Ksenia Security S.p.A.