PROCEDURA PER SEGNALAZIONE DI ILLECITI E IRREGOLARITÀ - WHISTLEBLOWING AI SENSI DEL D.LGS. N. 24/2023

Aggiornamento della procedura approvato dall'Amministratore Unico e Legale rappresentante il 26 febbraio 2025

1. PREMESSA

Il Decreto legislativo 10 marzo 2023, n. 24 recepisce in Italia la 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.

La disciplina in questione si rivolge agli enti del settore pubblico e del settore privato.

Per quanto concerne in particolare il settore privato la normativa si applica a:

- soggetti privati che hanno impiegato nell'ultimo anno la media di almeno cinquanta lavoratori subordinati (con contratti di lavoro a tempo indeterminato o determinato);
- soggetti del settore privato che rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'allegato 1 al D.Lgs. n. 24/2023, anche se nell'ultimo anno non hanno raggiunto la media di almeno cinquanta lavoratori subordinati (con contratti di lavoro a tempo indeterminato o determinato);
- soggetti del settore privato che rientrano nell'ambito di applicazione del D.Lgs. n. 231/2001, e adottano i modelli di organizzazione e gestione ivi previsti, se nell'ultimo anno hanno raggiunto la media di almeno cinquanta lavoratori subordinati (con contratti di lavoro a tempo indeterminato o determinato);
- soggetti del settore privato che rientrano nell'ambito di applicazione del D.Lgs. n. 231/2001 e adottano i modelli di organizzazione e gestione ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di almeno cinquanta lavoratori subordinati (con contratti di lavoro a tempo indeterminato o determinato).

In ottemperanza alla normativa, quindi, gli enti del settore pubblico e di quello privato che rientrano nell'ambito soggettivo di applicazione, sono tenuti ad attivare un canale interno per la trasmissione e la gestione delle segnalazioni.

La finalità è quella di garantire la protezione dei soggetti che effettuano segnalazioni di comportamenti illeciti (cd. violazioni) - sia in termini di riservatezza che di tutela da ritorsioni - in quanto, con la segnalazione delle violazioni, tali soggetti contribuiscono all'emersione di situazioni pregiudizievoli per l'Amministrazione o Ente di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Per tale ragione l'Amministratore Unico e legale rappresentante di Cyber-Bee S.r.l. ha approvato in data 14 dicembre 2023 la Procedura per segnalazioni di illeciti e irregolarità whistleblowing che è stata oggetto di aggiornamento in data 26 Febbraio 2025.

2. RIFERIMENTI NORMATIVI

- D.Lgs. n. 24/2023: 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 (Decreto "***Whistleblowing***");
- 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 - Approvate con Delibera ANAC n. 311 del 12 luglio 2023;
- Modello di Organizzazione, gestione e Controllo ex D.Lgs. 231/2001 di Cyber-Bee S.r.l..
- Codice Etico di R1 Group.

3. SCOPO

Il presente documento (di seguito anche solo "***Procedura***") disciplina le modalità di trasmissione a Cyber-Bee S.r.l. (di seguito, la Società o Cyber-Bee) delle segnalazioni di comportamenti illeciti ai sensi del D.Lgs. n. 24/2023, nonché la gestione delle stesse e le forme di tutela del Segnalante (di seguito anche solo "***Whistleblower***").

4. DEFINIZIONI

- ***Whistleblower***: è il dipendente o altro soggetto che segnala violazioni alle leggi, al codice etico, al Modello di Organizzazione Gestione e Controllo e alle procedure di Cyber-Bee S.r.l., commessi ai danni dell'interesse pubblico, agli organi legittimati ad intervenire;
- ***Whistleblowing****:* è la rivelazione spontanea da parte di un individuo, detto "segnalante" (in inglese "whistleblower") di un illecito o di un'irregolarità commessa all'interno dell'ente, del quale lo stesso sia stato testimone nell'esercizio delle proprie funzioni;
- **OdV**: è l'organo monocratico indipendente, istituito da Cyber-Bee S.r.l., che svolge la vigilanza sull'efficace attuazione del Modello 231 al fine di prevenire la commissione di reati presupposto richiamati nel D.Lgs n. 231/2001 sulla responsabilità amministrativa delle società;
- **Comitato Etico**: composto da una persona interna alla società e da un consulente esterno dotati di imparzialità e indipendenza al quale è affidata la gestione delle segnalazioni nei confronti dell'OdV.

5. SOGGETTI TUTELATI DEL SETTORE PRIVATO

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

Le disposizioni della presente Procedura si applicano alle seguenti persone che segnalano, denunciano all'autorità giudiziaria o contabile o divulgano pubblicamente informazioni sulle violazioni di cui sono venute a conoscenza nell'ambito del contesto lavorativo della Società:

a) i **dipendenti** di Cyber-Bee S.r.l. con contratto di lavoro subordinato;

b) i **lavoratori autonomi**, nonché i **titolari di un rapporto di collaborazione coordinata e continuativa** che svolgono la propria attività lavorativa presso Cyber-Bee S.r.l.;

c) i lavoratori o i collaboratori che svolgono la propria attività lavorativa presso soggetti che forniscono beni o servizi o che realizzano opere in favore di Cyber-Bee S.r.l.;

d) i **liberi professionisti** e **i consulenti** che prestano la propria attività presso Cyber-Bee S.r.l.;

e) i **volontari** e i **tirocinanti**, retribuiti e non retribuiti, che prestano la propria attività presso Cyber-Bee S.r.l.;

f) le **persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza** di Cyber-Bee S.r.l., anche qualora tali funzioni siano state esercitate in via di mero fatto, quali l'Amministratore Unico, il Revisore Legale e l'Organismo di Vigilanza;

g) ai **soci**.

La tutela delle persone segnalanti di cui al comma precedente si applica anche qualora la segnalazione, la denuncia all'autorità giudiziaria o contabile o la divulgazione pubblica di informazioni avvenga nei seguenti casi:

a) quando il rapporto giuridico di cui al comma precedente non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;

b) durante il periodo di prova;

c) successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

Le misure di protezione previste dalla presente Procedura si applicano, altresì:

a) ai **facilitatori**, vale a dire le persone fisiche che assistono il segnalante nel processo di segnalazione, operanti all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;

b) alle **persone del medesimo contesto lavorativo** del segnalante, denunciante o di chi effettua una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;

c) ai **colleghi di lavoro** del segnalante, denunciante o di chi effettua una divulgazione pubblica che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;

d) agli **enti di proprietà** – in via esclusiva o in compartecipazione maggioritaria di terzi – del segnalante, denunciante o di chi effettua una divulgazione pubblica;

e) agli **enti presso i quali il segnalante, il denunciante o chi effettua una divulgazione pubblica lavorano**;

f) agli **enti che operano nel medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica**.

6. VIOLAZIONI RILEVANTI

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

Sono considerate rilevanti le notizie che riguardano comportamenti, rischi, reati o irregolarità, consumati o tentati, a danno dell'interesse pubblico poste in essere in violazione del Modello organizzativo, del codice etico e di comportamento e delle procedure interne di Cyber-Bee S.r.l.

In particolare, possono essere segnalate tutte quelle situazioni in grado di arrecare danno o pregiudizio alla Società come:

- condotte illecite rilevanti ai sensi del D.Lgs.231/01 riconducibili a qualunque reato o tentativo di reato incluso nel novero dei reati presupposto del D.Lgs.231/01 quali ad esempio: corruzione di pubblici ufficiali o incaricati di pubblico servizio, malversazione a danno dello Stato, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, corruzione tra privati, associazione a delinquere, false comunicazioni sociali, riciclaggio, ricettazione, autoriciclaggio, aggiotaggio, frode in commercio, reati in materia di salute e sicurezza sul lavoro, reati ambientali, reati contro la personalità individuale, reati di criminalità informatica;
- violazioni del Modello 231 o del Codice di Condotta adottati dalla Società, poste in essere dai Soggetti Segnalati e di cui siano venuti a conoscenza in ragione delle funzioni svolte. Tali condotte, ancorché non integranti le fattispecie dei reati rilevanti ai sensi del D.Lgs. 231/01, possono ad esempio riguardare violazioni delle Parti Speciali del Modello 231 o degli altri protocolli di prevenzione (ovvero i principi di comportamento e le procedure di controllo che regolamentano lo svolgimento delle attività sensibili) ivi inclusi i provvedimenti interni, gli atti e le procedure operative adottate dalla Società che costituiscono attuazione dei contenuti del Modello 231.

Al fine di agevolare l'identificazione dei fatti che possono essere oggetto di segnalazione, si riporta di seguito un elenco a titolo meramente esemplificativo e non esaustivo di condotte/comportamenti rilevanti:

- falsificazione, alterazione, distruzione, occultamento di documenti;
- irregolarità amministrative e negli adempimenti contabili e fiscali o nella formazione del bilancio di esercizio della Società;
- comportamenti volti ad ostacolare le attività di controllo delle Autorità di Vigilanza (ad es. omessa consegna di documentazione, presentazione di informazioni false o fuorvianti);
- dazione di una somma di danaro o concessione di altra utilità ad un pubblico ufficiale o incaricato di pubblico servizio come contropartita per l'esercizio delle sue funzioni (es. agevolazione di una pratica) o per il compimento di un atto contrario ai propri doveri di ufficio (es. mancata elevazione di un verbale di contestazione per irregolarità fiscali);
- promessa o dazione di danaro, beni, servizi o altro beneficio volti a corrompere fornitori o clienti;
- violazioni in materia di salute e sicurezza sul lavoro e tutela dell'ambiente;
- accordi con fornitori o consulenti per far risultare come eseguite prestazioni inesistenti;
- falsificazione di note spese allo scopo di creare provviste per attività illegali (es. rimborsi "gonfiati" o per false trasferte);
- condotte in violazione di regolamenti e procedure operative di Cyber-Bee S.r.l..

7. CANALE DI SEGNALAZIONE INTERNO

La gestione delle segnalazioni è affidata all'OdV o al Comitato Etico (quest'ultimo in caso di segnalazioni nei confronti dell'OdV), i quali possono interagire per lo svolgimento dell'attività istruttoria con collaboratori individuati dalla Società e specificatamente formati sulla materia.

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

Le segnalazioni sono effettuate in forma scritta oppure in forma orale attraverso i seguenti CANALI INFORMATIVI.

Per segnalazione che non riguardano membri dell'OdV mediante:

a) **piattaforma informatica** appositamente adibita per le segnalazioni di illecito raggiungibile accendendo nella sezione RESPONSIBILITY del sito istituzionale della Società indirizzo https://whistleblowing.cyber-bee.it. La piattaforma è dotata di un sistema di crittografia automatica della identità che consente il mantenimento dell'anonimato del segnalante. Il whistleblower accede alla piattaforma attraverso il link sopra indicato. All'interno della piattaforma è presente il template che, una volta compilato, consente l'invio di una segnalazione e di allegarvi documenti. **Inviata la segnalazione, la piattaforma non invia notifiche ma fornisce un NUMERO DI CODICE[1] con cui il whistleblower potrà controllare lo stato della propria segnalazione e dialogare con l'OdV senza bisogno di utilizzare alcun account e-mail.**;

b) **incontro diretto con l'OdV**, previo appuntamento da concordare tramite messaggio da inviare sempre sulla piattaforma dedicata alle segnalazioni.

Qualora le segnalazioni riguardino l'OdV le stesse dovranno essere rivolte al Comitato Etico mediante la seguente modalità:

- **tramite posta cartacea**, da inviare all'indirizzo Via Monte Carmelo 5 CAP 00166 ROMA, inserendo in una busta chiusa con sopra apposta la dicitura "STRETTAMENTE CONFIDENZIALE. RISERVATA AL COMITATO ETICO WHISTLEBLOWING", due ulteriori buste, una contenente un documento d'identità e i recapiti del soggetto segnalante, l'altra il contenuto della segnalazione. Sarà poi cura del Comitato Etico dare riscontro al segnalante e procedere con le indagini del caso.

Le segnalazioni devono avere contenuto circostanziato e devono essere fondate su elementi di fatto precisi, ovvero non suscettibili di interpretazioni differenti, e concordanti, ovvero convergenti nella medesima direzione.

Le segnalazioni non possono riguardare meri sospetti o notizie meramente riferite da terzi o comunque che non abbiamo elementi di fatto o documenti univoci a supporto degli stessi.

In ogni caso, non è necessario che la persona segnalante sia certa dell'effettivo avvenimento dei fatti segnalati e dell'autore degli stessi, essendo sufficiente che, in base alle proprie conoscenze e in buona fede, ovvero sulla base di una ragionevole convinzione fondata su elementi di fatto e circostanziati, lo ritenga altamente probabile.

Per essere considerate valide è necessario che le segnalazioni abbiano quali elementi essenziali:

- una precisa descrizione dell'oggetto della segnalazione, con indicazione delle circostanze di tempo e luogo in cui sono stati commessi/omessi i fatti;
- gli elementi che consentano, ove possibile, una chiara identificazione del soggetto segnalato ritenuto il presunto autore della condotta illecita e/o della violazione del Modello.

Le segnalazioni anonime, vale a dire prive di elementi che consentano di identificare il loro autore, verranno prese in considerazione solo se relative a fatti di particolare gravità e con un contenuto che risulti adeguatamente dettagliato e circostanziato qualora:

a) siano effettuate a tutela dell'integrità dell'Azienda;
b) segnalino una situazione di cui si è venuti a conoscenza in ragione della propria attività e delle funzioni svolte;

[1] **Si precisa che è indispensabile conservare il NUMERO DI CODICE fornito dalla piattaforma al momento dell'invio della segnalazione al fine di poter monitorarne lo stato e dialogare con l'OdV. NEL CASO IN CUI VENGA SMARRITO IL CODICE E NON SIANO STATE FORNITE LE PROPRIE GENERALITÀ NON SARÀ POSSIBILE RISALIRE ALLO STATO DI LAVORAZIONE DELLA SEGNALAZIONE E IL WHISTLEBLOWER NON POTRÀ RICEVERE RISCONTRI ALLA PROPRIA SEGNALAZIONE.**

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

c) siano adeguatamente circostanziate e fondate su elementi di fatto precisi e concordanti;

d) siano indicate le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Resta fermo il requisito della veridicità dei fatti o situazioni segnalati, a tutela del denunciato.

La persona segnalante può indicare i seguenti ulteriori elementi:

- eventuali altri soggetti che possono riferire sui fatti oggetto della segnalazione e ai quali devono essere di conseguenza accordate le tutele previste dalla presente procedura in caso di ritorsioni;
- eventuali documenti che possono confermare la fondatezza di tali fatti;
- ogni altra informazione che possa agevolare la raccolta di evidenze su quanto segnalato.

Alla segnalazione può essere allegata ogni eventuale documentazione utile a meglio circostanziare i fatti denunciati.

Nell'ambito della gestione del canale di segnalazione interna, l'OdV e il Comitato Etico, nel caso di segnalazioni nei confronti dell'OdV, svolgono le seguenti attività:

a) rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;

b) mantiene le interlocuzioni con la persona segnalante e può richiedere a quest'ultima, se necessario, integrazioni;

c) dà diligente seguito alle segnalazioni ricevute;

d) fornisce 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.

La segnalazione non deve assumere toni ingiuriosi o contenere offese personali o giudizi morali volti ad offendere o ledere l'onore e/o il decoro personale e/o professionale della persona o delle persone a cui i fatti segnalati sono riferiti. È vietato in particolare:

- il ricorso ad espressioni ingiuriose;
- l'invio di segnalazioni con finalità puramente diffamatorie o calunniose;
- l'invio di segnalazioni che attengano esclusivamente ad aspetti della vita privata, senza alcun collegamento diretto o indiretto con l'attività aziendale/professionale del soggetto segnalato;
- l'invio di segnalazioni di natura discriminatoria, in quanto riferite ad orientamenti sessuali, religiosi e politici o all'origine razziale o etnica del soggetto segnalato;
- l'invio di segnalazioni effettuate con l'unico scopo di danneggiare il soggetto segnalato.

8. GESTIONE DELLE SEGNALAZIONI

L'attribuzione all'Organismo di Vigilanza del compito di esaminare e valutare le segnalazioni garantisce che le stesse siano ricevute, esaminate e valutate da un soggetto autonomo e indipendente non gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato.

Nell'ipotesi in cui l'Organismo di Vigilanza abbia un interesse connesso alla Segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio, dovrà astenersi dal processo di gestione delle Segnalazioni e la stessa dovrà essere gestita dal Comitato Etico.

Nell'ipotesi in cui le segnalazioni riguardino l'OdV l'attribuzione al Comitato Etico del compito di esaminare e valutare le segnalazioni garantisce che le stesse siano ricevute, esaminate e valutate da un soggetto imparziale e indipendente.

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

Il processo di gestione delle segnalazioni governato dall'OdV o dal Comitato Etico si articola sulle seguenti fasi:

- ricezione e registrazione della segnalazione;
- valutazione preliminare e classificazione della segnalazione;
- verifiche e indagini interne;
- conclusione del processo;
- reporting ai vertici aziendali;
- archiviazione delle Segnalazioni e della correlata documentazione rilevante.

L'OdV o il Comitato Etico, nell'ambito delle segnalazioni di rispettiva competenza, al ricevimento di una segnalazione, indipendentemente dal canale utilizzato, provvede con tempestività a compilare il registro delle segnalazioni in cui vengono riportati:

1. il numero identificativo progressivo che ne consente l'identificazione univoca;
2. la data di ricezione;
3. il canale di ricezione utilizzato;
4. la classificazione della segnalazione, in base alla valutazione preliminare del suo contenuto (Rilevante, Carente, Non Pertinente);
5. risultanze emerse e conclusioni.

Le segnalazioni sono preliminarmente classificate dall'OdV o dal Comitato Etico, nell'ambito delle segnalazioni di rispettiva competenza, nelle seguenti tipologie:

- ✓ **RILEVANTE**: segnalazione sufficientemente circostanziata e pertinente da consentire l'avvio delle indagini di riscontro;
- ✓ **CARENTE**: segnalazione di contenuto insufficiente ad avviare le indagini di riscontro. L'OdV o il Comitato Etico devono chiedere alla persona segnalante ulteriori informazioni al fine di avviare gli accertamenti sui fatti denunciati, riclassificando la segnalazione come Rilevante qualora la documentazione venga integrata. Il mancato invio di quanto richiesto da parte della persona segnalante non comporta l'automatica archiviazione della segnalazione, essendo l'OdV e il Comitato Etico tenuti a valutare le eventuali ragioni sottese al rifiuto, qualora indicate, nonché a verificare la possibilità di ottenere le informazioni necessarie mediante il ricorso ad altri canali;
- ✓ **NON PERTINENTE**: segnalazione non attinente al campo di applicazione della normativa in materia di whistleblowing in quanto si riferisce a persone segnalate non aventi rapporti con Cyber-Bee S.r.l., o a fatti, azioni o comportamenti che non riguardano condotte illecite ai sensi del paragrafo "Violazioni Rilevanti". In tali casi l'OdV o il Comitato Etico qualora ritengano fondata e circostanziata la segnalazione, possono trasmetterla alle funzioni dell'Ente ritenute competenti per le opportune verifiche.

Per le segnalazioni classificate RILEVANTI l'OdV o il Comitato Etico svolgono gli opportuni accertamenti interni per verificare la fondatezza dei fatti denunciati. Nel caso lo ritengano necessario l'OdV o il Comitato Etico possono avvalersi di consulenti esterni, tenuti all'obbligo di riservatezza sui fatti di cui vengono a conoscenza nell'espletamento dell'attività di consulenza e sull'identità delle persone coinvolte. Qualora la segnalazione risulti fondata, l'OdV e il Comitato Etico sono tenuti a contestare tempestivamente e formalmente le violazioni denunciate alla persona segnalata, la quale può, entro trenta giorni dalla ricezione della contestazione, chiedere di essere sentita ovvero presentare osservazioni scritte e documenti.

Al termine degli accertamenti l'OdV e il Comitato Etico predispongono una apposita relazione per l'Amministratore Unico in cui è formalizzato il contesto, il quadro normativo e procedurale di riferimento, le attività di verifica svolte, i relativi risultati emersi, i documenti e/o altri elementi comprovanti la condotta illecita o la violazione commessa, l'eventuale proposta di sanzione.

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

Nel caso di segnalazioni vietate, effettuate con dolo o colpa grave, che si rivelino palesemente infondate, l'OdV e il Comitato Etico comunicano tale circostanza all'Amministratore Unico per l'avvio del procedimento disciplinare nei confronti della persona segnalante. In tale caso l'OdV e il Comitato Etico ne dànno comunicazione al soggetto segnalato, per consentirgli l'esercizio dei diritti di difesa.

Per tutti i casi in cui venga avviato un procedimento di irrogazione delle sanzioni sono applicate le disposizioni contenute nel Codice Disciplinare adottato da Cyber-Bee S.r.l..

9. CANALE DI SEGNALAZIONE ESTERNA

La persona segnalante può effettuare una segnalazione esterna, attraverso apposito canale attivato dall'ANAC, se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

a) la persona segnalante ha già effettuato una segnalazione interna ai sensi del precedente par. 7 e la stessa non ha avuto seguito;

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

c) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

10. RISERVATEZZA DELLA PERSONA SEGNALANTE E DEGLI ALTRI SOGGETTI COINVOLTI NELLA PROCEDURA

I canali di segnalazione interna, nonché i soggetti interessati dal processo di gestione e accertamento dei fatti denunciati, garantiscono la riservatezza della segnalazione, nonché dell'identità della persona segnalante, del soggetto segnalato e delle persone menzionate nella segnalazione in qualità di facilitatori o persone informate sui fatti, fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

A tal fine, tutto il personale di Cyber-Bee S.r.l. viene specificatamente formato in merito agli obblighi riservatezza previsti dalla normativa in materia di whistleblowing.

Le segnalazioni 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 artt. 29 e 32, par. 4, del Regolamento (UE) 2016/679, e dell'art. 2-quaterdecies del Codice in materia di protezione dei dati personali.

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 della propria identità.

Può, inoltre, non essere rispettata la riservatezza della Persona Segnalante nei casi in cui:

- la persona segnalante dia il consenso espresso alla rivelazione della sua identità;

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

- venga accertata con sentenza di primo grado la responsabilità penale della persona segnalante per reati di calunnia o diffamazione o comunque per reati commessi con la segnalazione, ovvero la sua responsabilità civile per lo stesso titolo nei casi di dolo o colpa grave;
- l'anonimato non sia opponibile per legge e l'identità della persona segnalante sia richiesta dall'Autorità Giudiziaria.

11. TRATTAMENTO DEI DATI PERSONALI

Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dalla presente Procedura, deve essere effettuato a norma del Regolamento (UE) 2016/679, del Decreto Legislativo 30 giugno 2003, n. 196 e del Decreto Legislativo 18 maggio 2018, n. 51, con particolare riguardo a quanto previsto dal Garante per la Privacy nello specifico provvedimento sul Whistleblowing n. 304 del 6 luglio 2023. Nello specifico:

- le attività di trattamento legate alla gestione della Segnalazione sono svolte nel rispetto dei principi stabiliti dagli articoli 5 (Principi applicabili al trattamento dei dati personali), 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) e 35 (Valutazione d'impatto sulla protezione di dati personali) del GDPR;
- sono adottate misure tecniche (es. cifratura nell'ambito della Piattaforma Whistleblowing) e organizzative, che a seguito di specifica Valutazione d'impatto sono risultate adeguate a garantire la sicurezza dei dati personali, in conformità alla normativa vigente, durante tutto il loro ciclo di vita e tutto il processo relativo alle segnalazioni che beneficiano della tutela prevista dalla normativa Whistleblowing è stato sottoposto a Valutazione d'impatto sulla protezione dei dati ex. art. 35 del GDPR, le cui risultanze sono gestite nell'ambito del Modello Organizzativo ai sensi del Regolamento UE 2016/679 di cui l'Organizzazione è dotata;
- l'esercizio di alcuni dei diritti dell'interessato previsti dal GDPR nel contesto del processo di whistleblowing risulta essere parzialmente sospeso, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, ai sensi dell'articolo 2-undecies del Codice Privacy nel caso in cui da tale esercizio possa derivare un pregiudizio effettivo e concreto alla *"riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo 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 ",* per maggiori dettagli si rimanda alla specifica informativa presente sul sito web aziendale;
- sul sito web aziendale sono presenti le specifiche informative sia per i soggetti segnalanti (qualora decidessero di rendere nota la loro identità), sia per gli altri soggetti che verranno menzionati nelle segnalazioni. Tali informative, redatte per essere chiare e di facile comprensione, contengono tutte le informazioni previste dagli art.13 e 14 del GDPR, ossia l'identità e i dati di contatto del Titolare e del DPO, finalità e base giuridica dei trattamenti effettuati, periodo di conservazione dei dati, presenza di eventuali soggetti cui i dati saranno trasferiti, specificando se tali soggetti risiedono all'infuori del territorio dell'Unione, nonché le modalità per esercitare i diritti previsti dal Regolamento.

12. CONSERVAZIONE DELLA DOCUMENTAZIONE INERENTE ALLE SEGNALAZIONI

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

Le segnalazioni, interne ed esterne, 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 procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui ai precedenti par. 10 e 11.

Quando la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, essa, previo consenso della persona segnalante, è documentata mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro.

Fermo quanto previsto nell'articolo precedente la documentazione viene conservata attuando misure tecniche e organizzative adeguate al fine di impedire la loro perdita, distruzione o danno accidentali nel rispetto dei principi di integrità e riservatezza di cui all'art. 5 del Regolamento (UE) 2016/679.

13. DIVULGAZIONI PUBBLICHE

Ai fini della presente Procedura, per divulgazione pubblica si intende il rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

La persona segnalante che effettua una divulgazione pubblica beneficia della protezione prevista dalla presente Procedura se, al momento della divulgazione pubblica, ricorre una delle seguenti condizioni:

a) la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna ad ANAC, alle condizioni e con le modalità previste dalla presente Procedura e non è stato dato riscontro nei termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;

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

c) la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto.

14. DENUNCIA ALL'AUTORITÀ GIUDIZIARIA

Il Decreto legislativo 10 marzo 2023, n. 24, 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.

In linea con le indicazioni già fornite da ANAC nelle LLGG n. 469/2021, si precisa che qualora il whistleblower 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.

Resta fermo che, laddove il dipendente pubblico denunci un reato all'Autorità giudiziaria ai sensi degli artt. 361 o 362 c.p. e poi venga discriminato per via della segnalazione, potrà beneficiare delle tutele previste dal decreto per le ritorsioni subite.

Le stesse regole sulla tutela della riservatezza e del contenuto delle segnalazioni vanno rispettate dagli uffici delle Autorità giudiziarie cui è sporta la denuncia.

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

15. CONDIZIONI PER LA PROTEZIONE DELLA PERSONA SEGNALANTE

Le misure di protezione previste si applicano alle persone di cui al precedente par. 5 quando ricorrono le seguenti condizioni:

a) al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica, la persona segnalante o denunciante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate fossero vere e rientrassero nell'ambito oggettivo di cui al precedente par. 6;

b) la segnalazione o divulgazione pubblica è stata effettuata sulla base di quanto previsto dal par. 13.

I motivi che hanno indotto la persona a segnalare o denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

Salve le limitazioni di responsabilità previste dalla normativa vigente, quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele previste dalla normativa non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare.

La disposizione di cui al presente articolo si applica anche nei casi di segnalazione o denuncia all'autorità giudiziaria o contabile o divulgazione pubblica anonime, se la persona segnalante è stata successivamente identificata e ha subito ritorsioni, nonché nei casi di segnalazione presentata alle istituzioni, agli organi e agli organismi competenti dell'Unione europea, in conformità alle condizioni di cui al precedente par. 9.

16. DIVIETO DI RITORSIONE

Le persone di cui al precedente par. 5 non possono subire alcuna ritorsione da parte di Cyber-Bee S.r.l., da intendersi come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile 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.

Di seguito sono indicate talune fattispecie che, qualora siano riconducibili al precedente comma, costituiscono ritorsioni come indicate nelle Linee Guida Anac menzionate nei riferimenti normativi:

a) il licenziamento, la sospensione o misure equivalenti;

b) la retrocessione di grado o la mancata promozione;

c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;

d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;

e) le note di merito negative o le referenze negative;

f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;

g) la coercizione, l'intimidazione, le molestie o l'ostracismo;

h) la discriminazione o comunque il trattamento sfavorevole;

i) la 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;

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved

j) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;

k) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;

l) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;

m) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;

n) l'annullamento di una licenza o di un permesso;

o) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Gli atti assunti in violazione del presente articolo sono nulli. Le persone di cui al precedente par. 5 che siano state licenziate a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile hanno diritto a essere reintegrate nel posto di lavoro, ai sensi della normativa vigente, in ragione della specifica disciplina applicabile al lavoratore.

Le persone di cui al precedente par. 5 possono comunicare le ritorsioni che ritengono di avere subito all'ANAC, la quale adotta i provvedimenti di propria competenza ai sensi della normativa vigente.

17. AGGIORNAMENTO E APPROVAZIONE DEL DOCUMENTO

Il presente documento è sottoposto all'approvazione dell'Amministratore Unico. La revisione del documento può avvenire su sua proposta e deve essere sempre approvata dallo stesso.

Firmato

Il Legale rappresentante

Luca Gabrielli

©2023 Cyber-Bee S.r.l. A Company by of R1 Group | P. IVA 14559061008 | All rights reserved