

Deep Blue

**PROCEDURA DI GESTIONE DELLE
SEGNALAZIONI IN MATERIA
WHISTLEBLOWING E INFORMATIVA
IN MATERIA DI TRATTAMENTO DEI
DATI PERSONALI**

1. SCOPO E OBIETTIVI

La presente procedura recepisce il D.Lgs. n. 24/2023 e definisce le modalità per la ricezione e la gestione delle segnalazioni di violazioni e irregolarità all'interno di Deep Blue. Lo scopo è incoraggiare la comunicazione di illeciti riscontrati nel contesto lavorativo, garantendo la massima riservatezza e proteggendo le persone segnalanti da qualsiasi forma di ritorsione.

2. CHI PUÒ EFFETTUARE LA SEGNALAZIONE

Le procedure di whistleblowing incoraggiano a segnalare chiunque acquisisca, nel contesto dell'attività lavorativa, informazioni sugli illeciti commessi dall'organizzazione o per conto dell'organizzazione. Lo scopo della procedura è quello di facilitare la comunicazione di informazioni relative a violazioni riscontrate durante l'attività lavorativa. A tale scopo lo spettro delle potenziali persone segnalanti è molto ampio. La procedura è volta a garantire a questi soggetti, nel momento in cui segnalino una condotta illecita relativa all'ente.

Possono effettuare una segnalazione:

- Dipendenti, collaboratori e collaboratrici
- Lavoratori e lavoratrici autonomi, liberi professionisti e professioniste e consulenti.
- Tirocinanti, retribuiti o non retribuiti.
- Soggetti con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza.
- Fornitori, subfornitori e il loro personale dipendente.
- Persone candidate in fase di selezione ed ex dipendenti.

3. COSA PUÒ ESSERE SEGNALATO

Possono essere segnalati fatti illeciti di cui si sia venuti a conoscenza nel contesto della propria attività lavorativa. Possono essere riportati anche sospetti (qualificati) di reati o altre violazioni di disposizioni di legge o potenziali rischi di commissione degli stessi.

Non viene richiesto alla persona segnalante di dimostrare in modo completo la commissione di un illecito ma le segnalazioni devono essere quanto più possibile circostanziate, al fine di consentire un accertamento dei fatti comunicati da parte delle persone riceventi. Allo stesso tempo, non si invitano le persone segnalanti ad attuare attività di investigazione che possano esporli individualmente.

Le segnalazioni possono riguardare illeciti penali, civili, amministrativi o contabili, così come le violazioni di normative comunitarie.

Non rientrano nell'oggetto di questa procedura le segnalazioni di carattere personale, per esempio inerenti al proprio contratto di lavoro.

4. GESTIONE DELLE SEGNALAZIONI

Il Gestore delle segnalazioni è il soggetto responsabile della ricezione e gestione delle segnalazioni di illecito. Il Gestore può essere coadiuvato da soggetti del suo gruppo di supporto specificamente nominati con atto interno e al bisogno.

La persona designata alla ricezione e gestione delle segnalazioni in Deep Blue è Damiano Taurino. Qualora la segnalazione riguardi il Gestore stesso o vi sia un conflitto di interessi, la segnalazione dovrà essere indirizzata al Destinatario Alternativo, individuato nella figura di Micol Biscotto.

Il Gestore riceve le segnalazioni e dialoga con la persona segnalante per chiarire e approfondire quanto ricevuto. Il dialogo con la persona segnalante continua anche durante le fasi di accertamento.

Il Gestore, con eventuale supporto di collaboratori, dopo una valutazione iniziale, svolge un'attività di accertamento delle informazioni segnalate, anche richiedendo specifiche informazioni ad altri uffici e funzioni interni all'organizzazione.

Il Gestore fornisce riscontri periodici alla persona segnalante e, al termine dell'attività di accertamento, comunica l'esito delle attività di accertamento alla persona segnalante. Nella comunicazione dell'esito non sono inclusi riferimenti a dati personali relativi all'eventuale soggetto segnalato.

Tra i possibili esiti che possono essere comunicati alla persona segnalante ci sono:

- Correzione di processi interni
- Avvio di un procedimento disciplinare
- Trasferimento dei risultati delle attività di accertamento alla procura della Repubblica (e/o della Corte dei Conti in caso di danno erariale)
- Archiviazione per mancanza di evidenze

5. CANALI DI SEGNALAZIONE

Deep Blue mette a disposizione delle persone segnalanti canali diversi per le segnalazioni di violazioni ai sensi della presente procedura. In particolare, è possibile effettuare segnalazioni in forma orale e in forma scritta.

Canale scritto: le segnalazioni vanno inviate tramite l'apposita piattaforma informatica, basata sul software open source GlobaLeaks ed erogata in modalità SaaS qualificata dall'Agenzia per la Cybersicurezza Nazionale (ACN), accessibile al link <https://dblue.wbisweb.it>.

Questo strumento garantisce, da un punto di vista tecnologico, l'assoluta riservatezza dell'identità del segnalante e del contenuto attraverso l'utilizzo di una crittografia avanzata end-to-end, in cui le chiavi di decifrazione rimangono nella disponibilità esclusiva del Gestore di Deep Blue. A ulteriore garanzia di riservatezza, la piattaforma non registra i log di sistema che permetterebbero l'identificazione, rimuovendo l'indirizzo IP del dispositivo utilizzato e avvalendosi esclusivamente di cookie tecnici, senza alcun tracciamento o profilazione.

Al termine dell'inserimento, il sistema genera automaticamente un codice univoco identificativo (codice segnalazione) noto solo alla persona segnalante; tramite questo codice sarà possibile accedere in modo sicuro alla propria area personale per monitorare lo stato di avanzamento e scambiare messaggi e documenti con il Gestore in ambiente protetto.

La piattaforma consente anche l'invio di segnalazioni anonime; queste verranno prese in considerazione per ulteriori verifiche solo se risulteranno adeguatamente dettagliate e circostanziate.

Canale orale: è possibile richiedere un incontro diretto o un colloquio telefonico personale con il Gestore (o con il Destinatario Alternativo in caso di conflitto). L'incontro verrà

documentato mediante verbale, che potrà essere verificato e confermato dalla persona segnalante tramite sottoscrizione.

È opportuno ricordare che le segnalazioni in forma orale non offrono la stessa riservatezza tecnologica delle segnalazioni effettuate tramite piattaforma crittografata.

6. FASI E TEMPISTICHE DI GESTIONE DELLE SEGNALAZIONI

1. **Avviso di ricevimento:** il Gestore conferma alla persona segnalante la presa in carico della segnalazione entro 7 giorni dalla ricezione, tramite piattaforma o in risposta alla richiesta di colloquio.

2. **Valutazione e istruttoria:** il Gestore esegue una valutazione preliminare e svolge l'attività di accertamento delle informazioni segnalate, mantenendo un dialogo costante con la persona segnalante per eventuali chiarimenti.

3. **Riscontro:** entro 3 mesi dal giorno dell'avviso di ricevimento, il Gestore comunica alla persona segnalante un riscontro sull'esito o sullo stato di avanzamento delle attività di accertamento.

7. RISERVATEZZA E DIVIETO DI RITORSIONI

Il Gestore è tenuto a trattare le segnalazioni preservandone la riservatezza. Le informazioni relative all'identità della persona segnalante, della persona segnalata e di ogni altra persona menzionata nella segnalazione sono trattate secondo i principi di confidenzialità. Allo stesso modo, sono trattate in modo confidenziale anche tutte le informazioni contenute nella segnalazione.

L'identità della persona segnalante non può essere rivelata senza il suo consenso. La conoscenza delle segnalazioni e dei relativi atti di accertamento sono sottratti anche al diritto all'accesso amministrativo da parte dei soggetti interessati.

L'unico motivo di possibile rivelazione dell'identità della persona segnalante può avvenire nel caso in cui gli atti di accertamento siano inoltrati presso una procura ordinaria o contabile e la conoscenza della stessa sia necessaria ai fini del diritto di difesa durante un procedimento giudiziario ordinario o contabile presso la Corte dei Conti. La riservatezza è garantita attraverso la piattaforma crittografata per le segnalazioni e un protocollo riservato, e all'interno dei processi organizzativi volti a minimizzare la circolazione delle informazioni.

È possibile anche l'invio di segnalazioni anonime. Il soggetto ricevente può decidere se processarle o meno. In ogni caso, le segnalazioni vengono trattate secondo gli stessi principi di riservatezza. Tuttavia, nel caso di segnalazioni anonime, il Gestore non ha conoscenza dell'identità della persona segnalante e potrebbe involontariamente esporla durante le attività di accertamento.

8. GESTIONE DEI DATI PERSONALI

Le segnalazioni ricevute, le attività di accertamento e le comunicazioni tra la persona segnalante e il Gestore sono documentate e conservate in conformità alle prescrizioni in materia di riservatezza e protezione dei dati. Le segnalazioni contengono dati personali e possono essere trattate e mantenute solo per il tempo necessario al loro trattamento: questo tempo comprende l'analisi, le attività di accertamento e quelle di comunicazione degli esiti, oltre a un'eventuale tempistica ulteriore per possibili commenti aggiuntivi. In nessun caso le segnalazioni saranno conservate oltre i 5 anni successivi alla comunicazione dell'esito delle attività di accertamento alla persona segnalante.

Per quanto riguarda l'accesso ai dati personali, questi sono conosciuti solo dal Gestore e, se indicato in specifico atto interno, dai membri dello staff di supporto alla gestione della segnalazione. Nel corso delle attività di accertamento il Gestore può condividere con altre funzioni dell'ente informazioni preventivamente anonimizzate e minimizzate rispetto alle specifiche attività di competenza di queste ultime.

Tutti i dati inseriti nella piattaforma (anagrafiche, contenuti della segnalazione, allegati) sono inviati, trattati e archiviati su server ad alta sicurezza dislocati fisicamente all'interno del

territorio nazionale italiano. Il fornitore del servizio, ISWEB S.p.A., agisce in qualità di Responsabile esterno del Trattamento (Art. 28 GDPR) ed eroga il servizio in conformità agli standard internazionali ISO/IEC 27001 sulla sicurezza delle informazioni. Grazie alle misure crittografiche adottate "by design", né ISWEB S.p.A. né eventuali sub-responsabili dell'infrastruttura di rete hanno tecnicamente la possibilità di accedere in chiaro ai dati personali o ai contenuti delle segnalazioni.

9. SISTEMA SANZIONATORIO

Il Decreto Legislativo n.24/2023 prevede sanzioni amministrative, irrogabili da parte dell'Autorità Nazionale Anticorruzione in caso di violazione delle norme sul whistleblowing. Le sanzioni riguardano in modo specifico eventuali ritorsioni contro le persone segnalanti, violazioni dell'obbligo di riservatezza, il boicottaggio a un tentativo di segnalazione, la mancata presa in carico di una segnalazione o un'insufficiente attività istruttoria avviata in seguito alla stessa.

Sono altresì sanzionabili gli abusi del sistema di segnalazione, con possibili sanzioni per colui che calunnia o diffama un altro soggetto a mezzo della procedura. L'amministrazione può procedere disciplinarmente contro le persone responsabili di queste condotte.

10. TUTELE E PROTEZIONI

La persona cui si fa riferimento nella segnalazione come responsabile del sospetto di illecito beneficia di misure di protezione dell'identità analoghe a quelle della persona segnalante e delle altre persone menzionate nella segnalazione. In aggiunta alla tutela della riservatezza dell'identità della persona segnalante e dei soggetti menzionati nella segnalazione, nonché del contenuto della stessa, esistono altre forme di tutela garantite attraverso questa procedura. Viene infatti garantita protezione alla persona segnalante contro ogni forma di ritorsione o discriminazione che dovesse subire in seguito e a causa di una segnalazione. Per ritorsione si intende qualsiasi azione o omissione minacciata o reale, diretta o indiretta,

collegata o derivante da segnalazioni di illeciti effettivi o sospetti, che causi o possa causare danni fisici, psicologici, danni alla reputazione della persona, perdite economiche.

11. CANALI ESTERNI PER LE SEGNALAZIONI

Al di fuori della procedura interna per le segnalazioni, la legge permette di effettuare anche segnalazioni esterne all'Autorità Nazionale Anticorruzione. La persona segnalante può segnalare esternamente qualora abbia già effettuato una segnalazione a cui non è stato dato seguito, qualora abbia fondati motivi di ritenere che a una segnalazione interna non sia dato seguito o che questa possa determinare un rischio di ritorsione o qualora abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le modalità di segnalazione all'Autorità Nazionale Anticorruzione sono disponibili alla pagina dedicata sul sito dell'ANAC: anticorruzione.it/-/whistleblowing.

INFORMATIVA IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI AI SENSI DEGLI ARTICOLI 13 E 14 DEL REGOLAMENTO (UE) 2016/679

Ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 (GDPR)

1. TITOLARE DEL TRATTAMENTO

Il Titolare del Trattamento è **Deep Blue S.r.l.**, con sede legale in Via Daniele Manin 53, 00185 Roma (RM).

- **Email:** info@dblue.it
- **PEC:** postacertificata@dblue.it

2. TIPOLOGIA DI DATI TRATTATI

La gestione delle segnalazioni comporta il trattamento di:

- **Dati comuni:** nome, cognome, ruolo aziendale e dati di contatto del segnalante (se non anonima) e dei soggetti coinvolti.
- **Dati particolari/giudiziari:** informazioni relative a opinioni politiche, sindacali, dati sulla salute o procedimenti penali, qualora inseriti nel contenuto della segnalazione.

3. FINALITÀ E BASE GIURIDICA

- **Finalità:** Ricezione, analisi e istruzione delle segnalazioni di illeciti per garantire l'integrità aziendale.
- **Base Giuridica:** Adempimento di un obbligo legale ai sensi del **D.Lgs. 24/2023** (Art. 6, par. 1, lett. c del GDPR).

4. GESTIONE DELLE SEGNALAZIONI E RISERVATEZZA

Le segnalazioni sono gestite da personale specificamente formato e autorizzato:

- **Gestori designati:** Damiano Taurino (Titolare) e Micol Biscotto (Sostituto in caso di conflitto).
- **Piattaforma informatica:** Il canale è ospitato su piattaforma **GlobaLeaks** (fornita da ISWEB S.p.A.) con crittografia end-to-end.
- **Garanzia di anonimato:** L'identità del segnalante è protetta e non può essere rivelata senza consenso espresso, salvo obblighi di legge in sede giudiziaria.

5. DESTINATARI DEI DATI

I dati non sono diffusi. Possono essere comunicati solo a:

- Autorità Giudiziaria, ANAC o uffici ispettivi competenti.
- Soggetti interni incaricati dell'istruttoria (in forma anonimizzata ove possibile).

6. CONSERVAZIONE DEI DATI

I dati saranno conservati per il tempo necessario alla gestione della segnalazione e, in ogni caso, **non oltre 5 anni** dalla comunicazione dell'esito finale della procedura.

7. DIRITTI DELL'INTERESSATO

I dipendenti possono esercitare i diritti di accesso, rettifica e cancellazione (artt. 15-22 GDPR) scrivendo a info@dblue.it.

Nota: L'esercizio dei diritti da parte della "Persona Coinvolta" può essere limitato se necessario per proteggere la riservatezza dell'identità del segnalante (art. 2-undecies Codice Privacy).