



**Omnia
Technologies**

Enabling Evolution

WHISTLEBLOWING POLICY

**PROCEDURA PER L'EFFETTUAZIONE E LA GESTIONE
DELLE SEGNALAZIONI DI VIOLAZIONI**

| | | | |
|--|--|--------------|------------|
| Scopo | Definire il processo di gestione di eventuali segnalazioni effettuate dai dipendenti e collaboratori alla Società, fornire indicazioni operative circa ambito, contenuti, modalità di trasmissione, destinatari, nonché forme di tutela per gli attori del processo. | | |
| Ambito: | | | |
| Edizione: | 1 | Data: | 01/10/2024 |
| Revisione: | 2 | Data: | 11/12/2025 |
| Riesame | Annuale | | |
| Numero di riferimento: | | | |
| Politiche riferimento incrociate: | <ul style="list-style-type: none"> - Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01 - Codice Etico | | |
| Ulteriori informazioni: | | | |
| Autorizzato per il rilascio: | | | |

INDICE

I - DISPOSIZIONI COMUNI

| | |
|------------------------------------|---|
| 1. Premessa..... | 4 |
| 2. Scopo..... | 4 |
| 3. Destinatari..... | 4 |
| 4. Adozione | 4 |
| 5. Comunicazione e diffusione..... | 4 |
| 6. Riferimenti normativi..... | 5 |
| 7. Definizioni | 5 |
| 8. Sanzioni..... | 6 |

I - EFFETTUAZIONE DELLA SEGNALAZIONE

| | |
|---|----|
| 9. Oggetto della segnalazione..... | 7 |
| 10. Soggetti legittimati alla segnalazione | 8 |
| 11. Misure di protezione del segnalante | 8 |
| 11.1. Riservatezza dell'identità del segnalante | 8 |
| 11.2. Divieto di ritorsione | 8 |
| 11.3. Protezione dalle ritorsioni | 9 |
| 11.4. Limitazioni della responsabilità | 9 |
| 11.5. Misure di sostegno | 10 |
| 12. Segnalazione interna..... | 10 |
| 13. Segnalazione anonima | 10 |
| 14. Segnalazione esterna e divulgazioni pubbliche | 10 |

II - GESTIONE DELLA SEGNALAZIONE

| | |
|---|----|
| 15. Soggetto incaricato della gestione della segnalazione | 11 |
| 16. Ricezione e presa in carico della segnalazione | 11 |
| 17. Valutazione preliminare della segnalazione | 12 |
| 18. Richiesta di informazioni integrative | 12 |
| 19. Prioritizzazione della gestione delle segnalazioni (c.d. triage) | 13 |
| 20. Accertamento della violazione segnalata | 13 |
| 21. Valutazione e prevenzione del rischio di ritorsioni | 14 |
| 22. Esito degli accertamenti svolti dal gestore | 14 |
| 23. Azioni conseguenti all'accertamento della violazione o della ritorsione | 14 |
| 24. Procedimento disciplinare conseguente alla segnalazione | 15 |
| 25. Trattamento dei dati personali | 15 |
| 26. Conservazione della documentazione inerente alle segnalazioni..... | 16 |

I - DISPOSIZIONI COMUNI

1. Premessa

Il Gruppo Omnia Technologies ha interesse a conoscere eventuali violazioni che possono verificarsi all'interno della propria organizzazione al fine di porvi efficace rimedio. A tal fine invita tutti coloro che ne fanno parte a confrontarsi liberamente su ogni criticità che dovessero riscontrare nella propria attività lavorativa, certi che nessuno attuerà per questo ritorsioni nei loro confronti.

Tuttavia, laddove vi sia la volontà di mantenere riservata la propria identità e/o il timore di subire ritorsioni da parte di altri componenti dell'organizzazione, il Gruppo Omnia Technologies consente di effettuare segnalazioni in maniera protetta secondo le modalità previste dalla presente procedura.

2. Scopo

Il presente documento ha lo scopo di disciplinare le modalità di effettuazione e gestione delle segnalazioni di violazioni di disposizioni normative nazionali o europee che ledono l'interesse pubblico o l'integrità delle Società del Gruppo Omnia Technologies, nonché le misure di protezione delle persone che effettuano segnalazioni.

3. Destinatari

Il presente documento si applica ai dipendenti delle Società del Gruppo Omnia Technologies e, in virtù di apposita clausola contrattuale, a tutti coloro che intrattengono con la Società rapporti di lavoro autonomo, di collaborazione e di consulenza professionale, nonché a tutte le persone che prestano la loro attività presso le Società del Gruppo Omnia Technologies.

Il presente documento si applica, altresì, agli azionisti delle Società del Gruppo Omnia Technologies e a tutte le persone che svolgono, anche di fatto, funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza della Società.

4. Adozione

L'adozione e l'aggiornamento del presente documento spetta dell'Organo dirigente, previa consultazione delle rappresentanze sindacali aziendali o delle organizzazioni sindacali di cui all'art. 51 d.lgs. 81/2015 in merito al canale di segnalazione interno individuato¹.

5. Comunicazione e diffusione

Il presente documento è portato a conoscenza del personale aziendale all'atto dell'adozione, in caso di aggiornamento e comunque in fase di selezione e al momento dell'assunzione.

All'atto di prima adozione verrà data contestuale comunicazione al personale aziendale del superamento o meno da parte di ciascuna Società della soglia dimensionale rilevante rispetto all'individuazione delle violazioni oggetto di possibile segnalazione e dei canali di segnalazione attivabili (numero di dipendenti impiegati nell'anno precedente). Eventuali variazioni future verranno comunicate entro il 30 gennaio di ciascun anno.

Per i terzi, tale informazione è reperibile presso la competente Camera di commercio, industria, artigianato e agricoltura.

¹ Art. 4 comma 1 d.lgs. 24/2023.

Il presente documento è reso facilmente accessibile al personale aziendale mediante affissione in bacheca e pubblicazione su sito Intranet Aziendale.

Sul sito web delle Società del Gruppo Omnia Technologies che ne sono dotate sono pubblicate informazioni chiare sul canale, sulle procedure e sui presupposti per poter effettuare le segnalazioni interne ed esterne.

I menzionati adempimenti assolvono all'onere informativo del gestore del canale di segnalazione interna².

6. Riferimenti normativi

- Decreto legislativo 8 giugno 2001, n. 231, recante «Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300»;
- Direttiva (UE) del Parlamento europeo e del Consiglio del 23 ottobre 2019, n. 1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;
- Decreto legislativo 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»;
- Regolamento (UE) del Parlamento e del Consiglio del 27 aprile 2016, n. 679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati;
- Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali;
- UNI ISO 37002:2021 - Whistleblowing management systems - Guidelines;
- Linee guida ANAC «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 n. 311 del 12 luglio 2023;
- «Nuova disciplina "Whistleblowing" - Guida operativa per gli enti privati» di Confindustria di ottobre 2023.

Nelle note a piè di pagina del presente documento sono indicati i riferimenti normativi da cui sono tratte le rispettive previsioni.

7. Definizioni

Ai fini del presente documento, si intendono per:

- a) «divulgazione pubblica»: 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;
- b) «gestore»: soggetto incaricato della ricezione e gestione delle segnalazioni effettuate attraverso il canale di segnalazione interno delle Società del Gruppo Omnia Technologies;
- c) «informazioni riservate»: informazioni coperte dall'obbligo di segreto, dalla tutela del diritto d'autore o dalla protezione dei dati personali;

² Art. 5 comma 1 lett. e d.lgs. 24/2023.

- d) «modello»: modello di organizzazione, gestione e controllo adottato da ciascuna Società del Gruppo Omnia Technologies ai sensi del d.lgs. 231/2001;
- e) «persone connesse»:
- 1) persone operanti nel medesimo contesto lavorativo che assistono il segnalante nel processo di segnalazione (cc.dd. facilitatori);
 - 2) persone del medesimo contesto lavorativo legate al segnalante da uno stabile legame affettivo o di parentela entro il quarto grado;
 - 3) colleghi che lavorano nel medesimo contesto lavorativo del segnalante e che hanno col medesimo un rapporto abituale e corrente;
 - 4) enti di proprietà del segnalante, per i quali il segnalante lavora o che operano nel medesimo contesto lavorativo del segnalante (es.: società appartenente al medesimo gruppo imprenditoriale);
- f) «riscontro»: comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione;
- g) «ritorsione»: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità 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;
- h) «segnalante»: la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo;
- i) «segnalato»: la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente;
- j) «segnalazione effettuata in mala fede» o «segnalazione in mala fede»: segnalazione effettuata da parte del segnalante che, al momento dell'effettuazione della segnalazione, della denuncia o della divulgazione pubblica, non aveva fondato motivo di ritenere che le informazioni sulla violazione oggetto di segnalazione, denuncia o divulgazione fossero vere;
- k) «seguito»: l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate.

8. Sanzioni

Le violazioni della presente procedura assumono rilevanza disciplinare e saranno sanzionate secondo quanto previsto dal sistema disciplinare interno. A titolo esemplificativo, costituisce violazione punibile:

- a) l'effettuazione della segnalazione in mala fede;
- b) l'effettuazione di una segnalazione di cui l'Autorità giudiziaria abbia accertato la natura diffamatoria o calunniosa³;
- c) la rivelazione dell'identità del segnalante, delle persone connesse e di ogni altra informazione dalla quale possa evincersi la loro identità;
- d) ogni comportamento volto a ostacolare la segnalazione;
- e) il tentativo di identificare il segnalante⁴;
- f) la mancata gestione della segnalazione per dolo o colpa grave, ivi compreso il mancato rimedio, da parte di chi ne abbia i poteri, alle violazioni o alle ritorsioni segnalate;

³ Art. 16 comma 3 d.lgs. 24/2023.

⁴ UNI ISO 37002:2021, § 8.4.2.

g) l'adozione di comportamenti ritorsivi.

Le violazioni della presente procedura da parte di soggetti terzi, non dipendenti dell'ente, potranno essere sanzionate in virtù di apposita clausola contrattuale.

II - EFFETTUAZIONE DELLA SEGNALEZIONE

9. Oggetto della segnalazione

Posso essere oggetto di segnalazione⁵, secondo le modalità indicate nel presente documento, le violazioni o i rischi di violazione⁶ di disposizioni normative nazionali o europee che ledono l'interesse pubblico o l'integrità delle Società del Gruppo Omnia Technologies. In particolare:

- a) condotte illecite rilevanti ai sensi del d.lgs. 231/2001;
- b) violazioni del Modello, anche non costituenti reato, (come ad esempio violazioni del Codice Etico e politiche relative alla diversità, equità, inclusione, ecc.)

Se l'azienda ha impiegato, nell'ultimo anno, più di 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, possono essere altresì segnalati:

- c) illeciti rientranti nell'ambito della normativa europea e nazionale relativa ai seguenti settori:
 - appalti pubblici;
 - servizi, prodotti e mercati finanziari;
 - 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;
 - protezione dei dati personali;
 - sicurezza delle reti e dei sistemi informativi;
 - misure restrittive dell'Unione Europea (trade compliance).
- d) atti od omissioni che ledono gli interessi finanziari dell'Unione europea o riguardanti il relativo mercato interno (es.: violazioni in materia di concorrenza e di aiuti di Stato);
- e) atti o comportamenti che vanificano l'oggetto o le finalità delle menzionate disposizioni normative.

Sono escluse dall'ambito di applicazione del presente documento le contestazioni, rivendicazioni o richieste legate a un interesse di carattere personale del segnalante che attengono esclusivamente ai propri rapporti di lavoro ovvero ai propri rapporti con le figure gerarchicamente sovraordinate⁷. Tali rimostranze potranno essere comunicate nelle forme ordinarie alle competenti funzioni aziendali.

Sono in ogni caso vietate le segnalazioni infondate effettuate con dolo o colpa grave⁸. In tali casi, al segnalante non verranno riconosciute le misure di protezione previste dal presente documento

⁵ Artt. 1-3 d.lgs. 24/2023.

⁶ UNI ISO 37002:2021, Introduzione.

⁷ Art. 1 comma 2 d.lgs. 24/2023.

⁸ Art. 16 commi 1 lett. a e 3 d.lgs. 24/2023.

e verrà applicata nei suoi confronti una sanzione, secondo quanto previsto dal sistema disciplinare interno.

10. Soggetti legittimati alla segnalazione

Le segnalazioni possono essere effettuate da parte di coloro che intrattengono o hanno intrattenuto rapporti di lavoro con le Società del Gruppo Omnia Technologies⁹. In particolare:

- a) dipendenti;
- b) lavoratori autonomi;
- c) collaboratori;
- d) liberi professionisti e consulenti;
- e) volontari e tirocinanti;
- f) azionisti;
- g) persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza.

Le segnalazioni possono essere effettuate anche prima e a prescindere dall'instaurazione del rapporto di lavoro, laddove abbiano a oggetto informazioni acquisite durante il periodo di selezione e/o di prova¹⁰.

11. Misure di protezione del segnalante

Al segnalante e alle persone connesse sono riconosciute le tutele previste dal presente documento, purché la segnalazione sia stata effettuata in buona fede e, in caso di segnalazione esterna o divulgazione pubblica, in presenza dei relativi presupposti¹¹.

I motivi che inducono la persona a segnalare sono irrilevanti ai fini della sua protezione¹².

Le misure di protezione si applicano anche nei casi di segnalazione anonima, se il segnalante è stato successivamente identificato e ha subito ritorsioni¹³.

11.1. Riservatezza dell'identità del segnalante

L'identità del segnalante non viene mai rivelata, senza il suo espresso consenso, a persone diverse da quelle competenti a ricevere o a dare seguito alla segnalazione¹⁴, salvo che, all'esito degli accertamenti svolti dal gestore, il segnalante risulti aver effettuato la segnalazione in mala fede ovvero emerga la sua responsabilità, anche in concorso con altri, per la violazione segnalata.

La medesima riservatezza è assicurata per qualsiasi altra informazione da cui possa evincersi l'identità del segnalante.

11.2. Divieto di ritorsione

Il segnalante non può subire nessuna ritorsione per il fatto di aver effettuato la segnalazione¹⁵.

Costituiscono, in via esemplificativa, ritorsioni¹⁶:

- a) il licenziamento, la sospensione o misure equivalenti;

⁹ Art. 3 commi 3 e 4 d.lgs. 24/2023.

¹⁰ Art. 3 comma 4 lett. a e b.

¹¹ Art. 16 comma 1 d.lgs. 24/2023.

¹² Art. 16 comma 2 d.lgs. 24/2023.

¹³ Art. 16 comma 4 d.lgs. 24/2023.

¹⁴ Art. 12 comma 2 d.lgs. 24/2023.

¹⁵ Art. 17 comma 1 d.lgs. 24/2023.

¹⁶ Art. 17 comma 4 d.lgs. 24/2023.

- 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;
- l) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- m) 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;
- n) 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;
- o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- p) l'annullamento di una licenza o di un permesso;
- q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Il divieto di ritorsione si applica anche alle persone connesse al segnalante¹⁷.

11.3. Protezione dalle ritorsioni

Le ritorsioni eventualmente subite possono essere comunicate all'ANAC, che ne dà informazione all'Ispettorato Nazionale del Lavoro per i provvedimenti di propria competenza¹⁸.

Gli atti ritorsivi sono nulli e il segnalante e le persone connesse hanno diritto alla cessazione della condotta ritorsiva, al risarcimento del danno e, in caso di licenziamento, alla reintegrazione nel posto di lavoro¹⁹.

Nell'ambito delle relative controversie instaurate dal segnalante, che sostenga di aver subito una ritorsione per aver effettuato una segnalazione, dovrà essere il datore di lavoro a provare che l'atto ritenuto ritorsivo sia motivato da altre legittime ragioni, estranee alla segnalazione²⁰.

Le rinunce e le transazioni, integrali o parziali, che hanno per oggetto i diritti e le tutele previsti dal presente documento sono valide solo se effettuate in una delle sedi previste dall'art. 2113 comma 4 c.c. (es.: Ispettorato Territoriale del Lavoro; Commissione di certificazione; Sede sindacale)²¹.

11.4. Limitazioni della responsabilità

Nel caso in cui per effettuare la segnalazione si renda necessario rivelare informazioni riservate od offensive della reputazione dell'ente, è esclusa l'eventuale responsabilità penale, civile e amministrativa del segnalante e delle persone connesse²², purché le informazioni siano collegate alla segnalazione e strettamente necessarie a rivelare la violazione²³.

¹⁷ Art. 17 comma 1 d.lgs. 24/2023.

¹⁸ Art. 19 comma 1 d.lgs. 24/2023.

¹⁹ Art. 19 commi 3 e 4 d.lgs. 24/2023.

²⁰ Art. 17 commi 2 e 3 d.lgs. 24/2023.

²¹ Art. 22 d.lgs. 24/2023.

²² Art. 20 commi 1 e 2 d.lgs. 24/2023.

²³ Art. 20 comma 4 d.lgs. 24/2023.

In ogni caso, le segnalazioni devono avere a oggetto informazioni acquisite lecitamente²⁴.

L'effettuazione della segnalazione non esime comunque il segnalante dalle proprie eventuali responsabilità in relazione alla violazione segnalata²⁵.

11.5. Misure di sostegno

È istituito presso l'ANAC l'elenco degli enti del Terzo settore che forniscono ai segnalanti misure di sostegno consistenti in informazioni, assistenza e consulenza a titolo gratuito sulle modalità di segnalazione, sulla protezione dalle ritorsioni, sui diritti della persona coinvolta nella segnalazione e sulle modalità e condizioni di accesso al patrocinio a spese dello stato²⁶.

12. Segnalazione interna

Le segnalazioni possono essere effettuate mediante l'applicazione *Integrity Line* secondo le seguenti modalità²⁷:

- a) in forma scritta, attraverso la compilazione guidata dei campi all'interno dell'applicazione;
- b) in forma orale, attraverso il sistema di messaggistica vocale registrata;
- c) in forma orale, su richiesta del segnalante, mediante un incontro diretto con il gestore del canale di segnalazione²⁸ in luogo idoneo a garantire la riservatezza²⁹.

L'applicazione *Integrity Line* è accessibile attraverso il collegamento al seguente link <https://omniatechnologiesgroup.integrityline.com/> da qualunque dispositivo, che assegna al segnalante un profilo utente univoco per l'accesso alla propria area riservata e lo guida nella compilazione di alcuni campi informativi per l'effettuazione di una segnalazione quanto più completa e circostanziata possibile oppure per la richiesta di un incontro con il gestore.

A prescindere dalla modalità scelta in concreto, è in ogni caso garantita la riservatezza dell'identità del segnalante, del contenuto della segnalazione e della relativa documentazione.

13. Segnalazione anonima³⁰

Le segnalazioni dalle quali non è possibile ricavare l'identità del segnalante sono considerate anonime.

Le segnalazioni anonime non sono considerate whistleblowing, pertanto il gestore le trasmetterà all'Organo dirigente, così come pervenute, per le eventuali determinazioni conseguenti, fermo il riconoscimento delle tutele del segnalante in caso di identificazione futura.

14. Segnalazione esterna e divulgazioni pubbliche

Se l'azienda ha impiegato, nell'ultimo anno, più di 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, la violazione può essere segnalata all'ANAC³¹, mediante il canale esterno dalla stessa attivato, ovvero divulgata pubblicamente³², quando, alternativamente:

²⁴ Art. 20 comma 3 d.lgs. 24/2023.

²⁵ Cass. civ., sez. lav., 31 marzo 2023, n. 9148 (ord.).

²⁶ Art. 18 d.lgs. 24/2023.

²⁷ Art. 4 commi 1-3 d.lgs. 24/2023.

²⁸ Art. 4 comma 3 secondo periodo d.lgs. 24/2023.

²⁹ UNI ISO 37002:2021, § 8.2.

³⁰ LG ANAC, p. 33 s. e Guida operativa Confindustria, pp. 11 e 17.

³¹ Artt. 6 e 7 d.lgs. 24/2023.

³² Art. 15 d.lgs. 24/2023.

- a) la segnalazione interna e/o esterna, già effettuata, non ha avuto seguito;
- b) il segnalante ha fondati motivi di ritenere che, utilizzando il canale interno e/o esterno, non sarebbe dato efficace seguito alla segnalazione;
- c) il segnalante ha il fondato timore di subire ritorsioni;
- d) la violazione può costituire pericolo imminente o palese per l'interesse pubblico.

III - GESTIONE DELLA SEGNALAZIONE

15. Soggetto incaricato della gestione della segnalazione

La ricezione e gestione delle segnalazioni disciplinate dal presente documento sono affidate all'Organismo di Vigilanza della Società del Gruppo Omnia Technologies interessata e alla Funzione Compliance del Gruppo³³ (nel caso in cui la Società sia dotata di Modello di Organizzazione, Gestione e Controllo ex D.Lgs.231/01) e alla sola Funzione Compliance del Gruppo negli altri casi.

La segnalazione presentata a un soggetto incompetente a riceverla è trasmessa da quest'ultimo entro 7 giorni dal suo ricevimento al gestore del canale di segnalazione, con contestuale notizia della trasmissione al segnalante³⁴.

16. Ricezione e presa in carico della segnalazione

In caso di segnalazione effettuata oralmente su richiesta del segnalante, il gestore, previo consenso del segnalante, documenta la segnalazione mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale, il cui contenuto dev'essere sottoposto al segnalante per sue eventuali modifiche e sottoscrizione³⁵.

In caso di segnalazione effettuata attraverso l'applicazione *Integrity Line*, mediante compilazione dei campi o messaggio vocale registrato, il software protocolla la segnalazione ricevuta e la notifica al gestore, che rilascia al segnalante avviso di ricevimento entro 7 giorni dalla data di ricezione³⁶. L'avviso di ricevimento potrà includere, tra l'altro³⁷:

- a) rassicurazione e richiesta sulle modalità preferite per la prosecuzione dell'interlocuzione (es.: la segnalazione è stata fatta online ma il segnalante preferisce continuare di persona);
- b) informazioni sulle fasi successive del processo di gestione della segnalazione, relative tempistiche e possibili risultati (es.: quali ulteriori riscontri attendersi e quando);
- c) informazioni, anche mediante rinvio alla presente procedura, sulle misure adottate a tutela del segnalante, comprese le misure per proteggere la sua identità, nonché sulle responsabilità di leale collaborazione del segnalante e di effettiva considerazione e tutela da parte dell'ente.

Il gestore dà diligente seguito alla segnalazione ricevuta³⁸ e fornisce riscontro al segnalante entro 3 mesi dalla data di avviso di ricevimento e comunque entro 3 mesi e 7 giorni dalla ricezione della segnalazione³⁹.

³³ Art. 4 comma 2 d.lgs. 24/2023.

³⁴ Art. 4 comma 6 d.lgs. 24/2023.

³⁵ Art. 14 comma 4 d.lgs. 24/2023.

³⁶ Art. 5 comma 1 lett. a d.lgs. 24/2023.

³⁷ UNI ISO 37002:2021, § 8.1.

³⁸ Art. 5 comma 1 lett. c d.lgs. 24/2023.

³⁹ Art. 5 comma 1 lett. d d.lgs. 24/2023.

Laddove gli accertamenti non possano essere completati tempestivamente, per esempio perché particolarmente complessi, entro il medesimo termine il gestore aggiorna il segnalante sullo stato della segnalazione e lo informa dell'ulteriore periodo di tempo necessario a completarli⁴⁰.

I termini per l'invio dell'avviso di ricezione e riscontro sono sospesi in corrispondenza delle chiusure aziendali e comunque dal 1° agosto al 31 agosto e dal 23 dicembre al 7 gennaio. Qualora uno dei termini di cui al presente articolo scada durante il periodo di sospensione feriale dei termini, riprenderà a decorrere dal primo giorno lavorativo successivo a ciascun periodo di sospensione.

17. Valutazione preliminare della segnalazione

Il gestore effettua un esame preliminare della segnalazione al fine di verificare se abbia a oggetto possibili violazioni o ritorsioni rientranti nell'ambito di applicazione oggettivo e soggettivo della presente procedura⁴¹.

Nel caso in cui il segnalante non sia identificato, il gestore trasmette la segnalazione all'Organo dirigente, così come pervenuta, per le eventuali determinazioni conseguenti, tenendone traccia e conservando la relativa documentazione secondo quanto previsto dall'art. 26 del presente documento per consentirne la rintracciabilità futura⁴².

Nel caso in cui ritenga che la segnalazione non rientri nell'ambito applicativo della presente procedura, il gestore ne dà comunicazione al segnalante, precisandone le ragioni e indicando l'ufficio interno eventualmente competente alla gestione della problematica segnalata. Ai fini della chiusura della segnalazione, il gestore predispone apposito Report destinato all'Organo dirigente e ne tiene traccia anonimizzata nel Registro delle segnalazioni.

Nel caso in cui ritenga che la segnalazione rientri nell'ambito applicativo della presente procedura, il gestore procede all'accertamento della violazione segnalata secondo quanto previsto di seguito.

18. Richiesta di informazioni integrative

Laddove non già presenti nella segnalazione, il gestore chiede al segnalante le seguenti informazioni⁴³:

- Dove ha avuto luogo la violazione?
- Quando si è verificata la violazione (passata, attuale, futura, in corso)?
- Chi è coinvolto nella violazione?
- L'hai segnalata in precedenza? Se sì, cosa, quando e a chi? Che azione è stata intrapresa?
- Qual è l'impatto per l'organizzazione dal tuo punto di vista?
- La direzione è coinvolta o a conoscenza della violazione?
- Avverti rischi per te o per altri?
- Hai documenti o altre prove a supporto della tua segnalazione?
- C'è qualcun altro che è a conoscenza diretta della violazione che possiamo contattare?
- Qualcuno ha provato a nascondere la violazione o a scoraggiarti dal condividere la tua preoccupazione? In tal caso, chi e come?

⁴⁰ UNI ISO 37002:2021, § 8.2.

⁴¹ UNI ISO 37002:2021, § 8.3.1, primo punto dell'elenco "Nota".

⁴² LG ANAC, p. 34 e Guida operativa Confindustria, p. 17.

⁴³ UNI ISO 37002:2021, § 8.2.

19. Prioritizzazione della gestione delle segnalazioni (c.d. triage)

In presenza di più segnalazioni da gestire contemporaneamente, il gestore valuta l'urgenza di intervento in base alla probabilità della violazione e al suo potenziale impatto sull'ente, tenendo conto dei seguenti fattori⁴⁴:

- La violazione può assumere rilevanza penale?
- La violazione è già avvenuta, è in corso o sta per accadere?
- C'è la necessità immediata di interrompere o sospendere le attività commerciali?
- Esiste un rischio immediato per la salute e la sicurezza?
- Esiste un rischio immediato per i diritti umani o per l'ambiente?
- C'è la necessità di assicurare e proteggere le prove prima che vengano cancellate o distrutte?
- Esiste un rischio per le funzioni, i servizi e/o la reputazione dell'ente?
- La segnalazione può impattare sulla continuità aziendale?
- Quale impatto mediatico può avere la segnalazione?
- Sono disponibili ulteriori informazioni a supporto della segnalazione?
- Qual è la natura dell'illecito (tipo e frequenza della violazione; ruolo e anzianità dei soggetti coinvolti nella segnalazione)?
- Qual è la probabilità che la violazione venga segnalata anche al di fuori dell'ente?
- La violazione è già stata segnalata in precedenza?
- In che modo il segnalante ha ottenuto le informazioni: le informazioni sono "di prima mano" o "per sentito dire"?

20. Accertamento della violazione segnalata

Il gestore procede all'accertamento della violazione segnalata mediante il compimento di una o più delle seguenti attività⁴⁵:

- a) coinvolgimento di funzioni aziendali competenti a supporto dell'accertamento (es.: risorse umane; ufficio legale; *audit* interno; responsabile conformità; salute e sicurezza; finanza), salvo che ciò comprometta la fiducia del segnalante, l'imparzialità del gestore o il buon esito dell'indagine;
- b) raccolta di evidenze documentali a riscontro della segnalazione;
- c) intervista di persone in grado di riferire informazioni utili all'accertamento della violazione;
- d) intervista del segnalato, informandolo preventivamente dell'oggetto dell'incontro⁴⁶, cui il gestore deve necessariamente provvedere in caso di richiesta da parte di quest'ultimo, anche mediante l'acquisizione di osservazioni scritte e documenti⁴⁷.

Il gestore documenta per iscritto le interviste effettuate mediante apposito verbale, il cui contenuto dev'essere sottoposto all'intervistato per sue eventuali modifiche e sottoscrizione.

Nel corso dell'accertamento, il gestore mantiene le interlocuzioni con il segnalante e, se necessario, può richiedere a quest'ultimo integrazioni⁴⁸.

In ogni caso, il gestore tutela l'identità delle persone coinvolte e menzionate nella segnalazione, fino alla conclusione del procedimento accertativo⁴⁹.

⁴⁴ UNI ISO 37002:2021, § 8.3.1.

⁴⁵ UNI ISO 37002:2021, § 8.3.1.

⁴⁶ UNI ISO 37002:2021, § 8.4.1.

⁴⁷ Art. 12 comma 9 d.lgs. 24/2023.

⁴⁸ Art. 5 comma 1 lett. b d.lgs. 24/2023.

21. Valutazione e prevenzione del rischio di ritorsioni

Il gestore valuta il rischio di ritorsioni per il segnalante sulla base dei seguenti fattori⁵⁰:

- Qual è la probabilità che venga mantenuta la riservatezza? Per esempio: qualcun altro è al corrente della violazione? La violazione è stata segnalata a qualcun altro? La natura delle informazioni può rivelare la loro identità? Sono gli unici ad avere accesso alle informazioni? La violazione configura un reato la cui prova necessita che venga rivelata l'identità del segnalante?;
- Il segnalante è preoccupato di subire ritorsione? Si sono già verificate condotte ritorsive o percepisce un rischio imminente di ritorsione?;
- Il segnalante è coinvolto nella violazione o l'ha subita?;
- La segnalazione riguarda tipi diversi di violazioni?;
- In che modo il segnalante ha ottenuto le informazioni sulla violazione?;
- Che tipo di rapporto intercorre tra il segnalante e la violazione oggetto della segnalazione?;
- Che tipo di rapporto intercorre tra il segnalante e l'ente?

Il livello di protezione e le relative azioni intraprese dipendono dal tipo e dalla tempistica della segnalazione e dalle potenziali conseguenze della violazione.

Qualora il gestore non abbia il potere di elaborare e attuare strategie per prevenire eventuali danni a carico del segnalante (es.: riorganizzazione interna del personale), gliene dà comunicazione al fine di consentire al segnalante di prestare il proprio consenso alla rivelazione della sua identità nei confronti di chi, all'interno dell'ente, abbia tale potere, ferme comunque le altre tutele previste dalla presente procedura nel caso in cui la ritorsione venga poi effettivamente attuata.

22. Esito degli accertamenti svolti dal gestore

Il gestore conclude il processo di gestione della segnalazione mediante l'emissione di apposito Report destinato all'Organo dirigente, nel quale rendiconta l'iter di gestione della segnalazione e l'esito degli accertamenti svolti con particolare riferimento a:

- a) l'insussistenza della violazione o ritorsione segnalata, precisando se la segnalazione si ritenga essere stata effettuata in mala fede ai fini dell'eventuale applicazione della sanzione disciplinare nei confronti del segnalante;
- b) la sussistenza o il rischio di verificazione della violazione o ritorsione segnalata, precisando il soggetto ritenuto responsabile e gli elementi raccolti.

Nel Report non viene fatta menzione dell'identità del segnalante e di altre informazioni idonee a identificarlo, salvo i casi di segnalazione effettuata in mala fede ovvero di ritenuta responsabilità del segnalante per la violazione accertata.

23. Azioni conseguenti all'accertamento della violazione o della ritorsione

L'Organo dirigente valuta il contenuto del Report e adotta azioni appropriate all'esito degli accertamenti svolti dal gestore. In particolare:

⁴⁹ Art. 12 comma 7 d.lgs. 24/2023.

⁵⁰ UNI ISO 37002:2021, § 8.3.2.

- a) in caso di incompletezza degli accertamenti svolti dal gestore, effettua ulteriori approfondimenti, anche per il tramite delle funzioni aziendali competenti, di un difensore di fiducia o di un consulente esterno;
- b) in caso di accertata violazione o del rischio di violazione, adotta misure idonee a prevenire, interrompere o sanare la violazione, nonché misure disciplinari appropriate nei confronti di ogni soggetto ritenuto responsabile della violazione;
- c) in caso di ritenuta sussistenza di un rischio concreto di ritorsioni, adotta misure idonee a proteggere il segnalante (es.: riorganizzazione interna del personale);
- d) in caso di accertata ritorsione, attuata o anche solo minacciata, nei confronti del segnalante, adotta misure idonee a sanare le ritorsioni subite⁵¹ (es.: reintegra del segnalante nella precedente posizione lavorativa), nonché misure disciplinari appropriate nei confronti di ogni soggetto ritenuto responsabile della ritorsione;
- e) in caso di ritenuta mala fede del segnalante nell'effettuazione della segnalazione, adotta misure disciplinari appropriate nei suoi confronti.

L'Organo dirigente comunica le azioni intraprese al gestore, affinché ne dia tempestivo riscontro al segnalante, e monitora regolarmente l'efficacia delle misure adottate.

Il processo di gestione della segnalazione si conclude con la comunicazione al segnalante in merito all'esito degli accertamenti svolti e alle azioni eventualmente intraprese di conseguenza da parte dell'Organo dirigente.

24. Procedimento disciplinare conseguente alla segnalazione

Nell'ambito del procedimento disciplinare diretto a sanzionare la violazione oggetto di segnalazione, non verrà rivelata l'identità del segnalante senza il suo espresso consenso, anche qualora la conoscenza della sua identità sia indispensabile per la difesa del segnalato⁵².

Al fine di consentirgli di esprimere il inappreso eventuale consenso, il gestore comunica per iscritto al segnalante le ragioni della rivelazione dei dati riservati⁵³.

25. Trattamento dei dati personali

Le attività di ricevimento e gestione delle segnalazioni, comprese le eventuali azioni conseguenti, comportano un trattamento di dati personali, che viene attuato ed organizzato dal Titolare e dai Co-Titolari del trattamento, nel rispetto della normativa vigente e garantendo agli interessati, sulla base di quanto applicabile a tale trattamento, l'esercizio dei propri diritti di cui agli articoli da 15 a 22 reg. (UE) 2016/679 (si veda allegato).

EQS Group Srl con sede in Corso Vercelli, 40 - 20145 Milano (MI), in qualità di fornitore della piattaforma informatica dedicata alla ricezione e gestione delle segnalazioni, è Responsabile del trattamento dei dati personali sulla base di apposita nomina formalizzata per iscritto ai sensi dell'art. 28 reg. (UE) 2016/679.

L'Organismo di Vigilanza delle Società del Gruppo Omnia Technologies e la Funzione Compliance di Gruppo, in qualità di gestori del canale di segnalazione, sono autorizzati al trattamento dei dati personali sulla base di apposita lettera di incarico contenente l'indicazione degli obblighi di riservatezza che devono essere rispettati nell'espletamento della funzione di gestione del canale.

⁵¹ UNI ISO 37002:2021, § 8.4.3.

⁵² Art. 12 comma 5 d.lgs. 24/2023.

⁵³ Art. 12 comma 6 d.lgs. 24/2023.

L' informativa sul trattamento dei dati personali conseguente al ricevimento e alla gestione delle segnalazioni è resa disponibile per tutti gli interessati sull'applicazione *Integrity Line*, consultabile al seguente link <https://omniatechnologiesgroup.integrityline.com/>.

26. Conservazione della documentazione inerente alle segnalazioni

Le segnalazioni non vengono utilizzate oltre quanto necessario per dare adeguato seguito alle stesse⁵⁴. In particolare, i dati personali che non sono utili al trattamento di una specifica segnalazione, ove possibile, non vengano raccolti e, se raccolti accidentalmente, vengono cancellati immediatamente.

Il gestore conserva le segnalazioni e la relativa documentazione per il tempo necessario al trattamento delle stesse e comunque non oltre 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione⁵⁵.

Al fine di dare evidenza dell'efficace attuazione del sistema, il gestore tiene traccia anonimizzata delle segnalazioni ricevute e gestite in apposito Registro delle segnalazioni.

⁵⁴ Art. 12 comma 1 d.lgs. 24/2023.

⁵⁵ Art. 14 comma 1 d.lgs. 24/2023.

ALLEGATO

Informativa ai sensi della normativa sulla protezione dei dati personali (artt.13-14) Whistleblowing

Il presente documento contiene l'informativa prevista dagli articoli 13 e 14 del Regolamento UE 679/2016 (GDPR), in relazione al trattamento dei dati personali degli interessati che vengono coinvolti, a vario titolo, nelle segnalazioni di violazioni rilevanti ai sensi della Procedura Whistleblowing di Gruppo OMNIA TECHNOLOGIES.

Vesti Privacy

Titolare del trattamento dei dati personali connessi alle segnalazioni di illeciti rilevanti ai sensi del D.Lgs.24/2023, relative alla società OMNIA TECHNOLOGIES SPA è la stessa società.

Co-Titolari del trattamento dei dati personali connessi alle segnalazioni di illeciti rilevanti ai sensi del D.Lgs.24/2023 relative alle altre società del Gruppo sono le seguenti società:

| SOCIETA' | SEDE LEGALE |
|--------------------------|--|
| Omnia Technologies SpA | Via Feltrina 72, Trevignano (TV) - Italia |
| Omnia Components srl | Via Ponte Perez 23 C/D, Zevio (VR) - Italia |
| Ave Tehcnologies srl | Via Della Costituzione 127, Spinea (VE) - Italia |
| Gruppo Bertolaso Spa | Via Stazione 760, Zimella (VR) - Italia |
| Acmi Beverage SpA | Via Enzo Ferrari 1 Ramoscello di Sorbolo (PR) - Italia |
| Acmi Labelling srl | Via Enzo Ferrari 1 Ramoscello di Sorbolo (PR) - Italia |
| Acmi SpA | Via G. Di Vittorio 60, Fornovo di Taro (PR) - Italia |
| Tecnomaco Italia srl | Via della Meccanica 28, Aprilia (LT) - Italia |
| Omnia Life Sciences srl | Via Toscana 22, Poggibonsi (SI) - Italia |
| Meccanica Italiana srl | Via dell'Artigianato 15/A – Morgano (TV) - Italia |
| Pharmagel Technology srl | Strada Statale Mantovana 234/66, San Colombano al Landro (MI) - Italia |

Il rapporto di contitolarità intercorre, di volta in volta, esclusivamente fra la Società capogruppo OMNIA TECHNOLOGIES SPA e la singola Società controllata a cui la segnalazione si riferisce.

Fermo quanto sopra, in particolare, la co-titolarità si riferisce al trattamento dei dati effettuato:

- tramite il ruolo Admin designato da parte di OMNIA TECHNOLOGIES SPA configurato nel back-end del Portale/Software "Integrity Line" di raccolta e gestione delle segnalazioni, erogato in outsourcing da OMNIA TECHNOLOGIES SPA in favore delle società controllate del Gruppo OMNIA TECHNOLOGIES, per finalità di manutenzione tecnica (es. Servizio help desk di 1° livello) e di gestione delle configurazioni funzionali e di sicurezza disponibili nel back-end del Portale (es. modifica testi di front-end, configurazione dei ruoli utenti – admin e case manager - e dei privilegi ad essi rispettivamente associati, emissioni di password temporanee richieste dagli utenti, etc.);
- tramite il Case Manager interno designato da OMNIA TECHNOLOGIES SPA la cui nomina è stata contrattualizzata a livello centrale da parte di OMNIA TECHNOLOGIES SPA anche per conto delle altre società controllate che poi usufruiscono in outsourcing del relativo servizio, e/o
- tramite qualsiasi eventuale Case Manager esterno, il cui mandato professionale venga contrattualizzato in qualsiasi momento da parte di OMNIA TECHNOLOGIES SPA anche per conto di tutte o alcune delle altre società controllate, che poi usufruiranno in outsourcing del relativo servizio;
- tramite qualsiasi altro soggetto tempo per tempo autorizzato da OMNIA TECHNOLOGIES SPA e/o dalla singola società controllata del Gruppo a trattare i dati per le finalità previste nella presente *Informativa Privacy*.

Le condizioni e i termini del rapporto di contitolarità sono disciplinati da un *accordo di contitolarità, contenuto nella Procedura Whistleblowing* del Gruppo OMNIA TECHNOLOGIES raggiungibile tramite il Portale/software <https://omniatechnologiesgroup.integrityline.com/>, o consultabile nell'apposita sezione "whistleblowing" dei seguenti siti web aziendale <https://www.omniatechnologiesgroup.com> e nel sito intranet Aziendale.

La procedura Whistleblowing sarà inoltre distribuita ai dipendenti del Gruppo attraverso i consueti canali di comunicazione interna.

Responsabili esterni del trattamento sono i soggetti terzi destinatari dei dati espressamente indicati a tale titolo nel capitolo "Comunicazione dei dati personali" che segue.

Dati personali

I dati da noi trattati possono comprendere:

- dati personali comuni, tra i quali, ad esempio, i dati anagrafici (nome, cognome, data e luogo di nascita, rapporto lavorativo con la nostra Società o con l'organizzazione terza a cui appartiene il segnalante), i dati di contatto (numero telefonico fisso e/o mobile, indirizzo postale/e-mail), il ruolo/mansione lavorativa, comportamenti o altre circostanze di fatto o di diritto riferibili al segnalante nonché analoghe tipologie di dati riferibili a terze persone fisiche (es. soggetti ritenuti responsabili degli atti o delle omissioni segnalate, testimoni, ecc.);
- dati personali "particolari" di cui all'art. 9 del GDPR, tra i quali, ad esempio, le informazioni relative a condizioni di salute, opinioni politiche, convinzioni religiose o filosofiche, orientamento sessuale o appartenenza sindacale;
- sporadicamente, dati personali "giudiziari" di cui all'art. 10 del GDPR, relativi a reati e condanne penali, o a connesse misure di sicurezza (di regola a seguito della conclusione dell'indagine conseguente alla segnalazione allorché vengano avviati procedimenti di natura penale nei confronti di persone fisiche; inoltre, i dati potranno includere dati e omissioni punibili da un tribunale o da un'autorità amministrativa). Tali dati devono essere trattati solo in caso di assoluta necessità, sono documentati per iscritto e conservati solo nella misura strettamente necessaria dopo che la decisione sul reato è divenuta definitiva in un procedimento in cui sono stati trattati; la conservazione avviene, se possibile, senza rielaborazione.

I dati personali potranno essere acquisiti dalla Società in quanto contenuti nella segnalazione o negli atti e documenti a queste allegati, oppure tramite persone che vengono da noi consultate durante le indagini relative (es. testimoni o altre persone informate dei fatti, gestori della segnalazione).

Le persone a cui si riferiscono i dati personali trattati sono, tra l'altro i) persone a conoscenza dei fatti segnalati, o che comunque vengono richieste di fornire informazioni a fronte di una segnalazione ii) "soggetti coinvolti" (cioè incolpati della violazione oggetto della segnalazione), iii) "soggetti tutelati" (cioè che godono delle tutele inderogabili previste dalla normativa whistleblowing a fronte di una segnalazione), iv) Case Manager persone fisiche, v) altre persone che a vario titolo possono essere messe a conoscenza dell'esistenza e del follow-up della segnalazione.

I segnalanti che trattano dati personali di loro conoscenza al di là di quanto necessario per dare seguito alla segnalazione, assumono la veste di Titolari del trattamento ai sensi dell'art. 4 n 7 del GDPR.

Comunicazione dei dati personali

Il Titolare nel rispetto della tutela della riservatezza dell'identità del segnalante, potrà condividere i dati, in conformità al principio di stretta necessità, proporzionalità e minimizzazione, con:

- a) Altre funzioni interne del Titolare, debitamente autorizzate, che i Case Manager reputino opportuno coinvolgere nelle azioni di sèguito di una segnalazione;

- b) Case Manager, cioè eventuali organi terzi, designati dalla società ricevente ad ammettere e/o esaminare nel merito la segnalazione e/o ad adottare le azioni conseguenti, incluso il riscontro al segnalante;
- c) Soggetti terzi espressamente designati come Responsabili esterni del Trattamento (es. per finalità di hosting, manutenzione o gestione tecnica del datacenter, della piattaforma on-line usata per eseguire e gestire la segnalazione e del relativo database);
- d) Autorità esterne competenti (es. autorità giudiziaria o amministrativa, organi di polizia, guardia di finanza, ANAC – Autorità Nazionale Anticorruzione, etc.) solo nell'ambito di una indagine o di un giudizio penale, amministrativo o civile. In tal caso la comunicazione è soggetta alle garanzie previste dalle norme applicabili in materia. In particolare, il segnalante viene informato prima che la sua identità venga rivelata, a meno che tale informazione non possa compromettere l'indagine o il procedimento giudiziario. Quando l'Autorità competente informa il segnalante gli invia una dichiarazione scritta in cui spiega i motivi della divulgazione dei dati riservati in questione:
- e) Studi e/o consulenti legali, consulenti di compliance aziendale e/o altri soggetti necessariamente coinvolti nel processo di attivazione del sistema di segnalazione o di gestione della segnalazione, nella adozione di misure correttive conseguenti alla stessa, o per l'espletamento dei procedimenti sanzionatori o penali eventualmente applicabili (es. avvocati e studi legali, periti di parte, consulenti tecnici, agenzie investigative, altri soggetti a cui sono delegate le attività di investigazione e/o decisione delle segnalazioni).
- f) Qualunque terzo titolare autonomo legittimato a ricevere e trattare i dati in base alla Procedura Whistleblowing o alla legge.

In ogni caso sarà lecito il trattamento dei dati da parte di altri soggetti, inclusa la comunicazione a terzi, quando necessario per l'adozione di misure correttive da parte delle Società o l'attivazione di procedimenti sanzionatori o penali.

Sicurezza e riservatezza dei dati

Manteniamo misure tecniche e organizzative adeguate per garantire la protezione dei dati e la riservatezza, fatto salvo quanto previsto dall'art. 12 del D. lgs. n. 24/2023 - con particolare riferimento all'identità del segnalante, delle persone coinvolte e/o comunque menzionate nelle segnalazioni, del contenuto delle stesse e relativa documentazione. Il canale di comunicazione internet usato dalla piattaforma è cifrato tramite protocolli avanzati. I dati saranno memorizzati in un formato cifrato presso un datacenter certificato a norma ISO 27001, ubicato in Germania.

I dati sono trattati con modalità analogiche ed elettroniche.

Il diritto a non vedere rivelata la propria identità alle persone a cui i fatti segnalati si riferiscono (fatte salve le limitate eccezioni derivanti da eventuale dolo o colpa grave del segnalante) o a terzi spetta non solo al segnalante ma anche a chi abbia effettuato una eventuale divulgazione pubblica di una violazione prevista dalla Procedura del Titolare.

Diffusione. Trasferimento dati extra-SEE.

I dati non saranno diffusi, se non nei casi specificamente previsti dal diritto nazionale o dell'Unione europea. I dati potranno essere trasferiti in data center in Germania. I dati non verranno trasferiti extra-SEE.

Finalità e base giuridica

I dati saranno trattati per le seguenti finalità: i) valutare l'ammissibilità e fondatezza della segnalazione di illeciti da te comunicata, ii) applicare le misure di tutela e supporto dei soggetti protetti dalla normativa in materia di whistleblowing, iii) dare seguito alla segnalazione e, se possibile, misure di risposta ai risultati di

una segnalazione, iv) applicare eventuali misure disciplinari o altre sanzioni contro chi segnala con dolo o colpa grave, o contro eventuali soggetti coinvolti ai quali sia addebitabile la violazione segnalata, v) difesa o accertamento di nostri diritti nel contesto di procedimenti giudiziari, amministrativi o stragiudiziali e nell'ambito di contenziosi civili, amministrativi o penali sorti in relazione alla segnalazione effettuata, vi) adempiere a qualsiasi obbligo previsto da una legge, da un regolamento o da un'altra normativa applicabile.

Tenuto conto della normativa di riferimento, il trattamento dei dati si fonda sull'obbligo di legge a cui è soggetta la Società in quanto Titolare del trattamento (art. 6, par. 1, lett. c) del GDPR) ai fini del rispetto delle prescrizioni di cui al D. Lgs 24/2023 (nonché, nel caso di società dotate di Modello di Gestione, Organizzazione e Controllo 231, anche ai sensi del D.Lgs. 231/2021 e ss.mm.ii.), e, per quanto concerne eventuali dati particolari riportati volontariamente dal Segnalante, la condizione abilitante è da rinvenirsi nei motivi di interesse pubblico rilevante sulla base del diritto dell'Unione e degli Stati Membri in relazione alla motivazione per cui è stata disposta la normativa whistleblowing (art 9, par. 2, lett. g) del GDPR ed art. 2 sexies par. 1 del D. Lgs 196/03), nonché, in relazione ai dati particolari, nell'assolvimento di obblighi e sull'esercizio di diritti specifici del Titolare del trattamento e dell'Interessato in materia di diritto del lavoro (art. 9, par. 2, lett. b), GDPR).

Ulteriori precisazioni sulle basi legali

Sarà, di caso in caso, richiesto il preventivo consenso del Segnalante (art. 6 par. 1 lettera a) del GDPR) come previsto dal Decreto Whistleblowing, in particolare:

- quando la Segnalazione è effettuata tramite sistema di messaggistica vocale registrato (come previsto nella Procedura), per poter consentire, a cura del personale addetto, la relativa documentazione mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione;
- quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, per cui previo consenso della persona segnalante, la segnalazione è documentata a cura del personale addetto 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 mediante la propria sottoscrizione.

Base giuridica del trattamento per le finalità sub i), ii) e iii) (in relazione alle finalità di attuare misure di risposta ai risultati di una segnalazione, strettamente necessarie per rimuovere le conseguenze della Violazione segnalata) è l'esigenza di adempiere agli obblighi previsti a carico del Titolare dalla legge, da un regolamento o da un'altra normativa.

In relazione alle finalità di attuare misure di risposta ai risultati di una segnalazione, eventualmente diverse da quelle strettamente necessarie per rimuovere le conseguenze della Violazione segnalata, la base giuridica è l'interesse legittimo del Titolare di migliorare l'assetto dell'organizzazione.

In relazione alle finalità disciplinari o sanzionatorie, la base giuridica è l'interesse legittimo del Titolare di perseguire in sede disciplinare o sanzionatoria eventuali inosservanze della Procedura Whistleblowing del Titolare e/o, più in generale, della normativa relativa al whistleblowing.

In relazione alle finalità di difesa o accertamento di nostri diritti nel contesto di procedimenti giudiziari, amministrativi o stragiudiziali e nell'ambito di contenziosi civili, amministrativi o penali sorti in relazione alla segnalazione effettuata, la base giuridica è l'interesse legittimo del Titolare di esercitare la difesa dei propri diritti.

Durata della conservazione

I dati personali che appaiano non ragionevolmente pertinenti e utili al trattamento di una specifica Segnalazione non sono raccolti o, se ricevuti o raccolti accidentalmente, devono essere prontamente cancellati da parte dei Gestori della Segnalazione competenti rispetto alla Violazione.

Allo stesso modo, saranno cancellati i dati personali eventualmente segnalati e riferiti a comportamenti non compresi nell'ambito di applicazione della legge e/o della Procedura Whistleblowing del Titolare.

Se le informazioni ricevute contengono dati personali particolari di cui all'art. 9 del GDPR, saranno cancellate immediatamente, senza essere registrate ed elaborate.

Se si stabilisce che le informazioni fornite o parte di esse non sono veritiere, devono essere immediatamente cancellate non appena tale circostanza emerge, a meno che la mancanza di veridicità possa costituire un reato, nel quale caso le informazioni saranno conservate per il tempo necessario durante il procedimento legale.

I dati di segnalazione e la relativa documentazione saranno conservati per il tempo necessario al trattamento della segnalazione e comunque al più tardi non oltre 5 (cinque) anni (in Italia) dalla data della comunicazione dell'esito finale della procedura di segnalazione (nel rispetto degli obblighi di riservatezza delle informazioni nonché di limitazione della conservazione, previsti dalle normative applicabili in materia). Successivamente a tale termine, le segnalazioni verranno eliminate dal sistema, oppure conservate in forma anonimizzata, fatta salva l'eventuale esigenza di conservazione per tutto l'ulteriore tempo necessario all'espletamento di un procedimento amministrativo o giudiziario già avviato o per procedimenti investigativi ai sensi del Codice di Procedura Penale.

Diritti degli interessati

L'interessato, nelle persone del Segnalante o del Facilitatore, ha diritto di accedere in ogni momento ai dati che lo riguardano e di esercitare i diritti previsti dagli articoli da 15 al 22 del GDPR, per quanto applicabili (diritto di accesso ai dati personali, diritto a rettificarli, diritto di ottenerne la cancellazione o cd. diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali o quello di opposizione al trattamento), inviando una e-mail all'indirizzo: whistleblowing@omniatechnologiesgroup.com.

I suddetti diritti non sono esercitabili dalla persona coinvolta o dalla persona menzionata nella segnalazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, ai sensi dell'art. 2undecies del Codice Privacy in quanto dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante.

Dicembre 2025

OMNIA TECHNOLOGIES SPA