# PROCEDURA PER LA SEGNALAZIONE DI VIOLAZIONI ("WHISTLEBLOWING")

## PARTE 1 - INTRODUZIONE

Foppa Fustelle Group Srl  invita tutti propri dipendenti, collaboratori, business partner e stakeholders più in generale a fare sentire la propria voce nel caso di situazioni di illiceità cui dovessero assistere o di cui possano essere venuti a conoscenza.

In tal senso ha istituito una serie di canali di segnalazione per permettere ai Segnalanti di esprimersi nei modi ritenuti più tutelanti o efficaci: Foppa Fustelle Group Srl ascolterà e risponderà in modo appropriato, indipendentemente dal canale scelto.

Potrete:

- parlare con il vostro supervisore o manager

In aggiunta, Foppa Fustelle Group Srl ha predisposto una piattaforma dedicata per l'invio di Segnalazioni, idonea a garantire la riservatezza e – ove ritenuto utile – l'anonimato del Segnalante.

Tale piattaforma è raggiungibile dall'indirizzo foppagroup.go-tell.it e permette di inviare segnalazioni puntuali senza necessità di creare account.

La Segnalazione sarà gestita da:

- Macchi Rossana, impiegata, indirizzo mail rmacchi@foppagroup.com
- Pirazzoli Giovanni, impiegato, indirizzo mail gpirazzoli@foppagroup.com

in qualità di Gestori delle Segnalazioni.

Al termine della Segnalazione, il sistema genererà un codice di 16 cifre che il Segnalante può utilizzare per verificare eventuali successive risposte ricevute da parte del gestore in merito alla Segnalazione effettuata o integrare quanto inizialmente dichiarato.

## 1. Cosa è il whistleblowing?

Il **whistleblowing** è un modo per segnalare comportamenti scorretti o illegali che potrebbero danneggiare la nostra azienda. Questi comportamenti potrebbero includere violazioni delle nostre procedure interne o di qualsiasi altra norma applicabile.

Le segnalazioni devono essere basate su fatti concreti o irregolarità. Per irregolarità si intendono quegli elementi sintomatici di potenziali violazioni che, pur non costituendo ancora un illecito conclamato, rappresentano indici ragionevoli del fatto che una violazione potrebbe essere commessa. Non è necessario disporre di prove definitive al momento dell'invio, ma di informazioni sufficientemente circostanziate.

Le segnalazioni, inoltre, devono essere inviate in buona fede: qualora tu non disponga di tutte le informazioni per una Segnalazione basata su fatti concreti, ti invitiamo ad essere chiaro nella formulazione del suo contenuto

### 1.1. Whistleblowing interno

Se sei un dipendente e segnali un comportamento scorretto o illegale all'interno dell'azienda, questo è chiamato whistleblowing interno.

### 1.2. Whistleblowing esterno

Se segnali un comportamento scorretto o illegale a una figura esterna, come un ente giudiziario o i media, questo è chiamato whistleblowing esterno.

## 2. Cosa si può segnalare e cosa regolamenta questa procedura?

Questa procedura regolamenta le Segnalazioni di violazioni delle norme o comportamenti irregolari che hai riscontrato nella nostra azienda. La procedura regola, inoltre, come riceviamo, analizziamo e gestiamo le segnalazioni, che sono tutte gestite rispettando la confidenzialità del segnalante.

Puoi anche effettuare segnalazioni anonime, anche se preferiremmo tu dicessi chi sei. Questo ci permetterebbe di meglio verificare quanto segnali e di tutelarti con più efficacia.

## 3. Definizioni

| | |
|---|---|
| Contesto lavorativo | Le attività lavorative o professionali, presenti o passate, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle Violazioni e nel cui ambito potrebbe rischiare di subire Ritorsioni in caso di Segnalazione o di divulgazione pubblica o di denuncia all'Autorità giudiziaria o contabile |
| Facilitatore | La persona che assiste un Segnalante nel processo di Segnalazione, la cui identità è tutelata come quella del Segnalante stesso |
| Gestore delle Segnalazioni | La persona o il team di persone, interne o esterne, individuate per la gestione delle Segnalazioni |
| Informazioni sulle violazioni | Informazioni, compresi i sospetti fondati, riguardanti Violazioni commesse o che, sulla base di elementi concreti (indici sintomatici), potrebbero essere commesse nell'organizzazione, nonché gli elementi riguardanti condotte volte ad occultare tali Violazioni |
| Persona coinvolta | La persona menzionata nella Segnalazione, o nella divulgazione pubblica, come persona alla quale la violazione è attribuita o la persona comunque implicata nella Violazione segnalata o divulgata pubblicamente |
| Riscontro | Comunicazione al Segnalante su come la segnalazione è stata o sarà gestita |
| Ritorsione | 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, che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto |
| Segnalante | La persona che effettua la Segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio Contesto lavorativo |
| Segnalazione | La comunicazione scritta od orale di informazioni sulle Violazioni |
| Soggetti del settore privato | Soggetti, diversi da quelli rientranti nella definizione di soggetti del settore pubblico, i quali: (i) hanno impiegato, nell'ultimo anno, la media di almeno 50 (cinquanta) lavoratori subordinati con contratti di lavoro a tempo determinato o indeterminato; (ii) rientrano nell'ambito di applicazione degli atti dell'Unione europea, anche se nell'ultimo anno non hanno raggiunto la media di 50 (cinquanta) lavoratori subordinati; (iii) adottano Modelli di Organizzazione, Gestione e Controllo previsti dal D. Lgs. 231/2001 |
| Soggetti del settore pubblico | Le amministrazioni pubbliche di cui all'art. 1, co. 2, del D. Lgs. 165/2001, le autorità amministrative indipendenti di garanzia, vigilanza o regolazione, gli enti pubblici economici, gli organismi di diritto pubblico, i concessionari di pubblico servizio, le società a controllo pubblico e le società *inhouse* |
| Violazioni | Azioni o comportamenti contrari alle nostre politiche interne e alla legge, come meglio individuate al punto 4 che segue |

## PARTE 2 – AMBITO DI APPLICAZIONE

### 4. Violazioni

Sono definite "Violazioni" tutti i comportamenti, atti od omissioni che danneggiano l'interesse pubblico o l'integrità di Foppa Fustelle Group Srl, e che consistono in:

- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori:
  a. appalti pubblici,
  b. servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento al terrorismo,
  c. sicurezza e conformità dei prodotti,
  d. sicurezza dei trasporti,
  e. tutela dell'ambiente,
  f. radioprotezione e sicurezza nucleare,
  g. sicurezza degli alimenti e dei mangimi e salute e benessere degli animali,
  h. salute pubblica, protezione dei consumatori, tutela della vita privata e protezione dei dati personali, sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione europea;
- atti od omissioni riguardanti il mercato interno, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato;
- altri illeciti amministrativi, contabili, civili o penali che non rientrino già nelle categorie specifiche sopra elencate.

### 4.1. Violazioni che non sono oggetto di segnalazione

Non possono essere oggetto di Segnalazioni, divulgazione pubblica o denuncia:

- le situazioni **legate ad un interesse di carattere personale**, cioè che attengono esclusivamente al tuo rapporto individuale di lavoro o di impiego pubblico, oppure ai rapporti con le figure gerarchicamente sovraordinate

Sono escluse, ad esempio, le segnalazioni riguardanti vertenze di lavoro, discriminazioni tra colleghi, conflitti interpersonali tra la persona segnalante e un altro lavoratore

- le segnalazioni di violazioni **che siano già disciplinate dagli atti dell'Unione europea o nazionali**, oppure da quelli nazionali indicati nella parte II dell'allegato alla Direttiva (UE) 2019/1937
- le segnalazioni di violazioni in materia di sicurezza nazionale, di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato dell'Unione europea.

### 5. Tabella riassuntiva dell'ambito di applicazione

| | Violazione | Ambito di applicazione |
|---|---|---|
| 1. | illeciti amministrativi, contabili, civili o penali | settore **pubblico** |
| 2. | condotte illecite rilevanti ai sensi del D. Lgs. 231/2001 | nel settore privato, si possono effettuare Segnalazioni agli Enti che (i) adottano modelli 231 o, in alternativa, (ii) hanno raggiunto nell'ultimo anno la media di almeno 50 lavoratori subordinati con contratti a tempo determinato o indeterminato |
| 3. | illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori:<br>• appalti pubblici, | nel settore privato, si possono effettuare Segnalazioni agli Enti che: (i) **hanno impiegato**, nell'ultimo anno, la media di **almeno cinquanta lavoratori subordinati** con contratti di lavoro a tempo indeterminato o |

| | | |
|---|---|---|
| | • servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento al terrorismo,<br>• sicurezza e conformità dei prodotti,<br>• sicurezza dei trasporti,<br>• tutela dell'ambiente,<br>• radioprotezione e sicurezza nucleare,<br>• sicurezza degli alimenti e dei mangimi e salute e benessere degli animali,<br>• salute pubblica, protezione dei consumatori, tutela della vita privata e protezione dei dati personali, sicurezza delle reti e dei sistemi informativi. | determinato; (ii) **rientrano nell'ambito di applicazione degli atti dell'Unione**, anche se nell'ultimo anno non hanno raggiunto la media di 50 (cinquanta) lavoratori subordinati |
| 4. | atti od omissioni che ledono gli interessi finanziari dell'Unione europea | nel settore privato, si possono effettuare Segnalazioni agli Enti che: (i) **hanno impiegato**, nell'ultimo anno, la media di **almeno cinquanta lavoratori subordinati** con contratti di lavoro a tempo indeterminato o determinato; (ii) **rientrano nell'ambito di applicazione degli atti dell'Unione**, anche se nell'ultimo anno non hanno raggiunto la media di 50 (cinquanta) lavoratori subordinati |
| 5. | atti od omissioni riguardanti il mercato interno, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato | nel settore privato, si possono effettuare Segnalazioni agli Enti che: (i) **hanno impiegato**, nell'ultimo anno, la media di **almeno cinquanta lavoratori subordinati** con contratti di lavoro a tempo indeterminato o determinato; (ii) **rientrano nell'ambito di applicazione degli atti dell'Unione**, anche se nell'ultimo anno non hanno raggiunto la media di 50 (cinquanta) lavoratori subordinati |
| 6. | atti o comportamenti che rendono vana la tutela delle materie di cui ai precedenti punti 3, 4 e 5. | nel settore privato, si possono effettuare Segnalazioni agli Enti che: (i) **hanno impiegato**, nell'ultimo anno, la media di **almeno cinquanta lavoratori subordinati** con contratti di lavoro a tempo indeterminato o determinato; (ii) **rientrano nell'ambito di applicazione degli atti dell'Unione**, anche se nell'ultimo anno non hanno raggiunto la media di 50 (cinquanta) lavoratori subordinati |

## 6. Segnalante

Il Segnalante è la persona fisica che effettua la Segnalazione o la divulgazione pubblica di informazioni sulle Violazioni acquisite nell'ambito del proprio contesto lavorativo.

La Segnalazione può essere effettuata da tutti i seguenti soggetti:

- personale con un rapporto di lavoro dipendente
- lavoratori autonomi
- liberi professionisti e consulenti, fornitori
- volontari e tirocinanti
- azionisti o proprietari di quote societarie
- persone con funzione di amministrazione, direzione, controllo, vigilanza o rappresentanza.

Tutti questi soggetti sono coperti dalla tutela legale contro atti ritorsivi.

A tutti i soggetti sopra elencati, la tutela si applica non solo se la Segnalazione, la denuncia o la divulgazione pubblica avviene durante l'esistenza del rapporto di lavoro, ma anche durante il periodo di prova e anteriormente, o dopo la cessazione del rapporto lavorativo.

Sono esempi di Ritorsioni (vedi definizione di cui sopra) vietate:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- 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;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- 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'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;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

La protezione dalle Ritorsioni è garantita anche:

- al facilitatore (persona fisica che assiste il segnalante nel processo di segnalazione e operante all'interno del medesimo contesto lavorativo);
- alle persone del medesimo contesto lavorativo del Segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del Segnalante o della persona che ha sporto una denuncia o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno il Segnalante un rapporto abituale e corrente;
- agli enti di proprietà del Segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo di tali persone.

La protezione si estende anche al mantenimento della riservatezza di tali soggetti.

Sono previste misure di sostegno che consistono in informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni offerta dalle disposizioni normative nazionali e da quelle dell'Unione europea, sui diritti della persona coinvolta, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato. Maggiori informazioni sono disponibili all'indirizzo https://www.anticorruzione.it/-/whistleblowing .

## PARTE 3 - SEGNALAZIONI

## 7. Segnalazione

### 7.1. Caratteristiche del canale di gestione delle Segnalazioni

Il canale di gestione è configurato per garantire la specificità e l'indipendenza dalle ordinarie linee di reporting.

I sistemi di segnalazione prevedono canali alternativi a tua disposizione, così da assicurare che:

- il soggetto preposto alla ricezione, all'esame e alla valutazione della segnalazione non sia gerarchicamente e/o funzionalmente subordinato al soggetto segnalato,
- non sia esso stesso il presunto responsabile della violazione e
- non abbia un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio.

I soggetti preposti alla ricezione, all'esame e alla valutazione delle segnalazioni non partecipano all'adozione degli eventuali provvedimenti decisionali, che sono rimessi alle funzioni o agli organi aziendali competenti.

### 7.2. Elementi della segnalazione

Devi fornire tutti gli elementi utili e necessari per consentire al Gestore delle Segnalazioni che riceverà la Segnalazione di condurre un'istruttoria, di procedere alle verifiche e agli accertamenti del caso, e valutare la ricevibilità e la fondatezza della Segnalazione.

Per effettuare la Segnalazione, non è necessario che tu disponga di prove della violazione; tuttavia, devi disporre di informazioni sufficientemente circostanziate che ne facciano ritenere ragionevole l'invio.

La Segnalazione deve contenere i seguenti elementi:

- le tue generalità, con indicazione della qualifica ricoperta e/o della funzione/attività svolta nell'ambito della Società (generalità che saranno tenute riservate). Puoi anche scegliere di comunicare la tua identità in un secondo momento, sebbene possa essere più facile la gestione della Segnalazione con la tua immediata identificazione;
- una chiara e completa descrizione di fatti, il più possibile precisi e concordanti, oggetto di Segnalazione, che costituiscano o possano costituire una Violazione rilevante
- se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi i fatti oggetto della Segnalazione;
- se conosciute, le generalità o altri elementi che consentano di identificare il soggetto e/o i soggetti che hanno realizzato i fatti segnalati (ad esempio qualifica ricoperta e area in cui svolge l'attività)
- l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di Segnalazione
- l'indicazione di eventuali documenti che possono confermare la fondatezza dei fatti oggetto di Segnalazione
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti oggetto di Segnalazione ed in genere ogni altra informazione o documento che possa essere utile a comprendere i fatti segnalati.

### 7.3. Tipi di segnalazione

**Segnalazioni incomplete**

Se la Segnalazione non è circostanziata, e non consente di individuare elementi sufficienti per avviare un'istruttoria (ad esempio, in mancanza dell'illecito commesso, del periodo di riferimento, di cause e finalità dell'illecito, persone/funzioni coinvolte, etc.), il Gestore delle Segnalazioni competente per la ricezione della Segnalazione, provvederà a chiederti integrazioni, al fine di dare seguito alla Segnalazione stessa.

**Segnalazione non rilevante**

La Segnalazione non è pertinente al campo di applicazione della presente procedura, perché si riferisce a soggetti esterni oppure a fatti, azioni o comportamenti che non sono oggetto di segnalazione ai sensi della normativa applicabile.

Il Gestore delle Segnalazioni qualora ritenesse fondata e circostanziata tale Segnalazione, seppur non rilevante ai suoi fini, può procedere a sottoporre la segnalazione all'attenzione della funzione interna competente, avendo sempre cura di mantenere la riservatezza sull'identità del segnalante.

Qualora non possa essere garantita la tua tutela, la Segnalazione sarà trasmessa solo a seguito di tuo espresso consenso.

**Segnalazione rilevante ma non trattabile**

La Segnalazione è pertinente al campo di applicazione della presente procedura, ma, a conclusione della fase di esame preliminare e di eventuale richiesta di ulteriori informazioni, non è stato possibile raccogliere sufficienti informazioni ed elementi in merito all'oggetto della Segnalazione, al fine di poter procedere con ulteriori indagini.

**Segnalazione vietata**

Il Gestore delle Segnalazioni comunicherà tale circostanza alla funzione competente per l'eventuale avvio del procedimento disciplinare e la valutazione dell'eventuale comunicazione della Segnalazione al Segnalato, per consentirgli l'esercizio dei diritti di difesa.

Nel caso in cui la funzione compente dovesse decidere di non coinvolgere il Segnalato, si procederà all'archiviazione della Segnalazione ricevuta.

Il coinvolgimento di altre funzioni potrebbe essere richiesto anche successivamente, laddove la natura diffamatoria, calunniosa o discriminatoria dovesse emergere solo durante la successiva fase di indagine.

È vietato, in ogni caso:

- 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.

Tali condotte, insieme all'invio di Segnalazioni vietate o comunque effettuate con dolo o colpa grave o ritenibili palesemente infondate, saranno sanzionabili in conformità al sistema disciplinare adottato.

Sono previste possibili sanzioni nel caso di Segnalazioni effettuate con dolo o colpa grave, o che si dovessero rivelare false, infondate, con contenuto diffamatorio o comunque effettuate al solo scopo di danneggiare la Società, il segnalato o altri soggetti interessati dalla segnalazione.

Si specifica che nei casi di invio di Segnalazioni vietate, la riservatezza dell'identità del segnalante nonché le altre misure di tutela del segnalante previste dalla Società non saranno garantite

### 7.4. Segnalazione inviata a un canale diverso da quello competente a riceverla

La tua riservatezza in quanto Segnalante è tutelata anche se la Segnalazione viene effettuata attraverso modalità diverse da quelle istituite in conformità al decreto, o perviene a personale diverso da quello autorizzato e competente a gestire le Segnalazioni, al quale, comunque, le stesse vanno trasmesse senza ritardo.

Qualora la Segnalazione interna sia presentata ad un soggetto diverso da quello individuato e autorizzato, la Segnalazione deve essere trasmessa, **entro 7 (sette) giorni** dal suo ricevimento, al soggetto competente.

Ti verrà data contestuale notizia della trasmissione della Segnalazione.

La Segnalazione può essere presentata al superiore gerarchico, ma tale Segnalazione non può essere considerata di whistleblowing, e quindi, in tal caso, non potrai beneficiare delle tutele previste.

### 7.5. Segnalazione effettuata di persona

Qualora venga effettuata una Segnalazione di persona, direttamente al Gestore delle Segnalazioni, il gestore della Segnalazione potrà aprire il form di Segnalazione per conto tuo, inserendo tutte le informazioni necessarie a dare corso alla Segnalazione stessa.

### 7.6. Segnalazione interna ed esterna

**Segnalazione interna**

Nell'ambito della gestione del canale di Segnalazione interna, il Gestore delle Segnalazioni a cui è affidata la gestione del canale di Segnalazione interna, svolge le seguenti attività:

- comunica al Segnalante un avviso di ricevimento della Segnalazione entro 7 (sette) giorni dalla data di ricezione
- mantiene le interlocuzioni con il Segnalante e chiede, se necessario, integrazioni
- dà seguito alle Segnalazioni ricevute
- fornisce riscontro al Segnalante, in merito alla Segnalazione, entro 3 (tre) mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro 3 (tre) mesi dalla scadenza del termine di 7 (sette) giorni dalla presentazione della Segnalazione

**Segnalazione esterna**

Oltre alla segnalazione interna, tu – in qualità di Segnalante – puoi effettuare una segnalazione esterna all'ANAC se ricorrono i seguenti presupposti:

- hai già effettuato una Segnalazione interna, che non abbia ricevuto riscontro
- hai fondati motivi di ritenere che, se effettuassi una Segnalazione interna, alla stessa non sarebbe dato efficace seguito o che la stessa segnalazione potrebbe determinare il rischio di ritorsione
- hai fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per l'interesse pubblico

L'ANAC, avendo fornito a qualsiasi persona interessata informazioni sull'uso del Canale di Segnalazione esterna:

- procede a darti avviso del ricevimento della Segnalazione esterna entro 7 (sette) giorni dalla data del suo ricevimento, salvo esplicita richiesta contraria, o salvo il caso in cui l'ANAC ritenga che l'avviso pregiudicherebbe la protezione della riservatezza della tua identità
- mantiene le interlocuzioni con te e può richiederti, se necessario, integrazioni
- dà diligente seguito alle Segnalazioni ricevute
- svolge l'istruttoria necessaria a dare seguito alla Segnalazione, anche mediante audizioni e acquisizione di documenti
- ti dà riscontro entro 3 (tre) mesi o, se ricorrono giustificate e motivate ragioni, 6 (sei) mesi dalla data di avviso di ricevimento della segnalazione esterna, o, in mancanza di detto avviso, dalla scadenza dei 7 (sette) giorni dal ricevimento
- ti comunica l'esito finale, che può consistere nell'archiviazione, nella trasmissione alle autorità competenti, in una raccomandazione o in una sanzione amministrativa

## 8. Gestione della segnalazione

### 8.1. Ricezione della segnalazione

All'atto della ricezione di una Segnalazione, indipendentemente dal canale utilizzato, il Gestore delle Segnalazioni provvederà ad attribuire un numero identificativo progressivo che ne consentirà l'identificazione univoca.

### 8.2. Analisi e valutazione preliminare

Il Gestore delle Segnalazioni provvede tempestivamente alla presa in carico e all'analisi della Segnalazione ricevuta, al fine della sua valutazione preliminare.

A seguito di questa analisi, il Gestore delle Segnalazioni provvederà a classificare la Segnalazione in una delle categorie indicate al punto 7.3 che precede, che implicheranno un diverso e specifico flusso.

### 8.3. Indagini

Al termine della fase di valutazione preliminare, se la Segnalazione ricevuta viene classificata come "rilevante e trattabile", il Gestore delle Segnalazioni procederà con l'avvio delle verifiche e indagini interne al fine di raccogliere ulteriori informazioni di dettaglio per verificare la fondatezza dei fatti segnalati e raccoglierne adeguata evidenza.

Nell'ambito dell'attività istruttoria, il Gestore delle Segnalazioni potrà avvalersi del supporto di strutture e/o funzioni aziendali interne adeguatamente qualificate e/o attraverso il ricorso a consulenti esterni.

In tali circostanze i soggetti coinvolti nell'attività di istruttoria diventano anch'essi destinatari della presente procedura e sono di conseguenza chiamati al rispetto, tra gli altri, degli obblighi di riservatezza.

In caso di violazioni da parte di tali soggetti dei principi definiti dalla presente procedura, la Società potrà applicare le misure indicate nel sistema sanzionatorio del Modello 231.

### 8.4. Report dell'attività di verifica

La fase di verifica si conclude con la stesura di un report per formalizzare il contesto di riferimento della Segnalazione, delle attività di verifica svolte, delle modalità seguite e dei relativi risultati ottenuti.

Il report proporrà, inoltre, le azioni da intraprendere in relazione a ciascun rilievo emerso.

### 8.5. Conclusioni

All'esito delle indagini, qualora il Gestore delle Segnalazioni non ravvisi la fondatezza dei comportamenti illeciti descritti nella Segnalazione o comunque che tali comportamenti non integrino una Violazione come definita in questa procedura, provvede ad archiviare la Segnalazione.

Qualora invece ne ravvisi la fondatezza e la Segnalazione riguardi dipendenti della Società, invierà tempestivamente il report conclusivo delle indagini alla funzione Risorse Umane per la valutazione degli eventuali provvedimenti disciplinari da intraprendere e/o per le eventuali comunicazioni alle Autorità competenti.

Contemporaneamente, il Gestore delle Segnalazioni valuterà l'eventualità di informare il Consiglio di Amministrazione

## PARTE 4 – TUTELA DEL SEGNALANTE

### 9. Riservatezza e divieto di ritorsione

Nessuna ritorsione o discriminazione, diretta o indiretta, può derivare se hai effettuato una Segnalazione in buona fede.

Inoltre, sono previste sanzioni nei confronti di chi viola le misure a tutela di te quale Segnalante.

La riservatezza viene garantita anche:

- a qualsiasi altra informazione o elemento della segnalazione dal cui disvelamento si possa dedurre direttamente o indirettamente la tua identità di Segnalante.
- nel caso di segnalazioni - interne o esterne - effettuate oralmente attraverso telefonate, messaggi vocali, o mediante un incontro diretto con chi tratta la segnalazione.

La Società potrà inoltre intraprendere le opportune iniziative anche in sede giudiziale.

#### 9.1. Tutela giurisdizionale del segnalante

La tua riservatezza quale Segnalante è garantita anche nell'ambito giurisdizionale, e in particolare:

- nell'ambito del **procedimento penale**, l'identità del Segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p.
- nell'ambito del **procedimento dinanzi alla Corte dei conti**, l'identità del Segnalante non può essere rivelata fino alla chiusura della fase istruttoria.
- nell'ambito del **procedimento disciplinare**, l'identità del Segnalante non può essere rivelata, se la contestazione dell'addebito disciplinare è fondata su accertamenti diversi rispetto alla Segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla Segnalazione, e risulti indispensabile per la difesa dell'incolpato conoscere l'identità del Segnalante, la Segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del Segnalante stesso.

#### 9.2. Consenso espresso del Segnalante

Come sopra indicato, per rivelare la tua identità quale Segnalante devono sussistere:

- la comunicazione scritta delle ragioni alla base della necessità di rivelare l'identità del Segnalante, e
- il consenso espresso del Segnalante.

La **prima ipotesi** ricorre quando, nell'ambito di un procedimento disciplinare avviato nei confronti del presunto autore della condotta segnalata, la tua identità quale Segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare.

In tal caso, oltre al previo tuo consenso, la normativa chiede anche di comunicarti, previamente e in forma scritta, le motivazioni che giustificano il disvelamento della tua identità.

La **seconda ipotesi** ricorre, invece, nel caso in cui la rivelazione della tua identità quale Segnalante sia indispensabile anche ai fini della difesa della persona coinvolta.

Anche in questo caso per disvelare la tua identità quale Segnalante è necessario acquisire previamente il tuo consenso e notificarti in forma scritta le motivazioni alla base della necessità di disvelarne l'identità.

## PARTE 5 – SANZIONI

### 10. Provvedimenti disciplinari

Foppa Fustelle Group Srl sanziona le violazioni della presente procedura in conformità alle normative locali.

Il mancato rispetto della presente procedura può comportare l'applicazione di provvedimenti disciplinari nei confronti dei dipendenti in conformità alla normativa locale applicabile, con ogni conseguenza di legge anche con riguardo alla conservazione del rapporto di lavoro e all'eventuale risarcimento dei danni derivanti dalla violazione medesima.

Il rispetto di quanto previsto dalla presente procedura deve considerarsi parte essenziale delle obbligazioni contrattuali assunte da ogni soggetto che abbia rapporti di affari con Foppa Fustelle Group srl. Pertanto, ogni violazione della procedura potrà costituire inadempimento contrattuale, con ogni conseguenza di legge in ordine alla risoluzione del contratto e al conseguente risarcimento dei danni derivanti.

**Egr. Sig. Giovanni Pirazzoli**

**Re: Impegno alla riservatezza e autorizzazione al trattamento di dati personali nell'ambito della gestione del canale interno di segnalazione – Addendum alla nomina a Persona Autorizzata**

Alla luce dei compiti a Lei affidati da Foppa Fustelle Group Srl, con riferimento al Suo ruolo di Gestore designato per la piattaforma di gestione delle segnalazioni ("whistleblowing") adottata ai sensi del D. Lgs. 24/2023,

**PREMESSO CHE**

-Foppa Fustelle Group Srl ha assunto, sia in sede di conformità al GDPR che sotto il dettato di cui al D. Lgs. 24/2023, tutti i necessari impegni per la sicurezza della piattaforma anche nel trattamento dei dati personali;

-Lei è stato in precedenza già individuato come Persona Autorizzata al trattamento dei dati personali di Foppa Fustelle Group Srl, come da autorizzazione in precedenza sottoscritta;

-Lei avrà accesso alla piattaforma di gestione delle segnalazioni ("whistleblowing") adottata ai sensi del D. Lgs. 24/2023, pertanto disponendo di informazioni riservate e personali riguardanti i soggetti segnalatori (se non anonimi), gli eventuali facilitatori e i soggetti segnalati.

Tutto ciò premesso, con la presente Lei viene autorizzato all'accesso alla menzionata piattaforma secondo le seguenti

**ISTRUZIONI**

-mantenere il più ampio riserbo sui trattamenti svolti a mezzo della piattaforma, nonché più in generale su qualsiasi informazione e dato personale di cui venga a conoscenza nel corso dello svolgimento delle Sue mansioni;

-assicurarsi che nessun altro soggetto acceda alla piattaforma, salvo che in qualità di ulteriori persone espressamente autorizzate;

-adottare tutte le misure di sicurezza ed osservare le disposizioni che Le verranno eventualmente impartite;

-operare in ossequio e nel rispetto delle caratteristiche della piattaforma di cui è appositamente informato;

-informare immediatamente e per iscritto la direzione aziendale e, in ogni caso, il *Data Protection Officer* nominato nella persona di Andrea Pivi in merito a qualsiasi anomalia o malfunzionamento relativo al sistema;

-non accedere ai dati contenuti nella piattaforma per estrarne copia, né direttamente attraverso il sistema fornito, né con l'ausilio di mezzi diversi (es. fotografie tramite smartphone, tablet, ecc.), salvo che in esecuzione degli specifici compiti previsti a Suo carico dalla normativa applicabile;

-non effettuare sui dati contenuti nella piattaforma operazioni di alterazione e/o duplicazione e/o cancellazione, salvo sulla base di precise istruzioni ricevute per iscritto;

-evitare ogni diffusione dei dati e di tutti gli ulteriori contenuti oggetto del trattamento;

-conformarsi ad ogni ulteriore istruzione che Le sarà impartita.

Caravaggio 08/05/2026

Firma per presa visione e accettazione

*(segue informativa in merito alla diffusione dei Suoi dati personali – nome, cognome e contatto – ai segnalanti)*

## INFORMATIVA "GESTORE DEL CANALE DI SEGNALAZIONE"

**Titolare del trattamento**
Il Titolare del trattamento è **Foppa Fustelle Group Srl**

**Categorie di dati trattati**
I dati trattati sono:
- dati personali identificativi e di contatto del gestore del canale di segnalazione*.

I dati contrassegnati con l'asterisco (*) sono obbligatori per consentire di effettuare il relativo trattamento.

**Finalità, basi giuridiche e tempo di conservazione**
Il trattamento dei dati personali è necessario al fine di:
- diffondere, ai sensi della normativa vigente, i dati identificativi e di contatto del gestore del canale di segnalazione a tutti i potenziali segnalanti, con i mezzi ritenuti opportuni dal Titolare;

In relazione alla finalità appena descritta:
- la base giuridica è l'art. 6 (1) lett. c), in quanto il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- i dati personali saranno trattati per il tempo pari all'attribuzione della carica e comunque non oltre 5 anni a decorrere dal termine della carica.

**Categorie di soggetti che possono trattare dati personali, ambito di comunicazione o diffusione**

Nei limiti degli obblighi, dei compiti o delle finalità sopra indicati:
- i dati personali saranno trattati esclusivamente da dipendenti e collaboratori del Titolare, nonché da soggetti terzi nominati Responsabili ai sensi dell'art. 28 GDPR, nel rispetto di quanto previsto dalla legge anche con riguardo alle misure di sicurezza a protezione e salvaguardia dei dati stessi;
- i dati saranno diffusi esclusivamente con le modalità indicate, salvo ulteriore consenso dell'interessato.

L'elenco dei Responsabili può essere richiesto al Titolare.
Il Titolare potrà comunicare i dati personali a terzi, autonomi titolari, al solo fine di dare esecuzione ad obblighi di legge.

**Diritti dell'interessato**
L'interessato potrà, in qualsiasi momento, esercitare i diritti previsti dal Reg. UE n. 2016/679, ed in particolare il diritto:
- di accedere ai suoi dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
- di proporre reclamo all'autorità di controllo. Per l'Italia, l'autorità di controllo è l'Autorità Garante per la protezione dei dati personali (www.gpdp.it).

L'esercizio dei diritti sopra richiamati potrà avvenire attraverso l'invio di una richiesta e-mail ai riferimenti noti.

**Egr. Sig.ra Rossana Macchi**

**Re: Impegno alla riservatezza e autorizzazione al trattamento di dati personali nell'ambito della gestione del canale interno di segnalazione – Addendum alla nomina a Persona Autorizzata**

Alla luce dei compiti a Lei affidati da Foppa Fustelle Group Srl, con riferimento al Suo ruolo di Gestore designato per la piattaforma di gestione delle segnalazioni ("whistleblowing") adottata ai sensi del D. Lgs. 24/2023,

**PREMESSO CHE**

-Foppa Fustelle Group Srl ha assunto, sia in sede di conformità al GDPR che sotto il dettato di cui al D. Lgs. 24/2023, tutti i necessari impegni per la sicurezza della piattaforma anche nel trattamento dei dati personali;

-Lei è stato in precedenza già individuato come Persona Autorizzata al trattamento dei dati personali di Foppa Fustelle Group Srl, come da autorizzazione in precedenza sottoscritta;

-Lei avrà accesso alla piattaforma di gestione delle segnalazioni ("whistleblowing") adottata ai sensi del D. Lgs. 24/2023, pertanto disponendo di informazioni riservate e personali riguardanti i soggetti segnalatori (se non anonimi), gli eventuali facilitatori e i soggetti segnalati.

Tutto ciò premesso, con la presente Lei viene autorizzato all'accesso alla menzionata piattaforma secondo le seguenti

**ISTRUZIONI**

-mantenere il più ampio riserbo sui trattamenti svolti a mezzo della piattaforma, nonché più in generale su qualsiasi informazione e dato personale di cui venga a conoscenza nel corso dello svolgimento delle Sue mansioni;

-assicurarsi che nessun altro soggetto acceda alla piattaforma, salvo che in qualità di ulteriori persone espressamente autorizzate;

-adottare tutte le misure di sicurezza ed osservare le disposizioni che Le verranno eventualmente impartite;

-operare in ossequio e nel rispetto delle caratteristiche della piattaforma di cui è appositamente informato;

-informare immediatamente e per iscritto la direzione aziendale e, in ogni caso, il *Data Protection Officer* nominato nella persona di Andrea Pivi in merito a qualsiasi anomalia o malfunzionamento relativo al sistema;

-non accedere ai dati contenuti nella piattaforma per estrarne copia, né direttamente attraverso il sistema fornito, né con l'ausilio di mezzi diversi (es. fotografie tramite smartphone, tablet, ecc.), salvo che in esecuzione degli specifici compiti previsti a Suo carico dalla normativa applicabile;

-non effettuare sui dati contenuti nella piattaforma operazioni di alterazione e/o duplicazione e/o cancellazione, salvo sulla base di precise istruzioni ricevute per iscritto;

-evitare ogni diffusione dei dati e di tutti gli ulteriori contenuti oggetto del trattamento;

-conformarsi ad ogni ulteriore istruzione che Le sarà impartita.

Caravaggio 08/05/2026

Firma per presa visione e accettazione

Macchi Rossana

*(segue informativa in merito alla diffusione dei Suoi dati personali – nome, cognome e contatto – ai segnalanti)*

## INFORMATIVA "GESTORE DEL CANALE DI SEGNALAZIONE"

**Titolare del trattamento**
Il Titolare del trattamento è **Foppa Fustelle Group Srl**

**Categorie di dati trattati**
I dati trattati sono:
- dati personali identificativi e di contatto del gestore del canale di segnalazione*.

I dati contrassegnati con l'asterisco (*) sono obbligatori per consentire di effettuare il relativo trattamento.

**Finalità, basi giuridiche e tempo di conservazione**
Il trattamento dei dati personali è necessario al fine di:
- diffondere, ai sensi della normativa vigente, i dati identificativi e di contatto del gestore del canale di segnalazione a tutti i potenziali segnalanti, con i mezzi ritenuti opportuni dal Titolare;

In relazione alla finalità appena descritta:
- la base giuridica è l'art. 6 (1) lett. c), in quanto il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- i dati personali saranno trattati per il tempo pari all'attribuzione della carica e comunque non oltre 5 anni a decorrere dal termine della carica.

**Categorie di soggetti che possono trattare dati personali, ambito di comunicazione o diffusione**

Nei limiti degli obblighi, dei compiti o delle finalità sopra indicati:
- i dati personali saranno trattati esclusivamente da dipendenti e collaboratori del Titolare, nonché da soggetti terzi nominati Responsabili ai sensi dell'art. 28 GDPR, nel rispetto di quanto previsto dalla legge anche con riguardo alle misure di sicurezza a protezione e salvaguardia dei dati stessi;
- i dati saranno diffusi esclusivamente con le modalità indicate, salvo ulteriore consenso dell'interessato.

L'elenco dei Responsabili può essere richiesto al Titolare.
Il Titolare potrà comunicare i dati personali a terzi, autonomi titolari, al solo fine di dare esecuzione ad obblighi di legge.

**Diritti dell'interessato**
L'interessato potrà, in qualsiasi momento, esercitare i diritti previsti dal Reg. UE n. 2016/679, ed in particolare il diritto:
- di accedere ai suoi dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
- di proporre reclamo all'autorità di controllo. Per l'Italia, l'autorità di controllo è l'Autorità Garante per la protezione dei dati personali (www.gpdp.it).

L'esercizio dei diritti sopra richiamati potrà avvenire attraverso l'invio di una richiesta e-mail ai riferimenti noti.

**INFORMATIVA "SEGNALANTI E FACILITATORI"**

**Titolare del trattamento**
Il Titolare del trattamento è Foppa Fustelle Group Srl, con sede in Caravaggio (BG) 24047, viale Europa Unita 37, C.F. e P. IVA 02502560168, contattabile ai seguenti recapiti:
- scrivendo una e-mail a amministrazione@foppagroup.com
- per posta ordinaria all'indirizzo della sede indicata.

Il Titolare ha nominato un DPO-Designato Privacy contattabile alla e-mail indicata.

**Categorie di dati trattati**
Le categorie di dati trattati relative al segnalante e, ove presente, al facilitatore, sono le seguenti:
- dati personali identificativi;
- dati personali di contatto ;
- dati comuni o particolari condivisi liberamente nella segnalazione.

I dati contrassegnati con l'asterisco (*) sono obbligatori per consentire di effettuare il relativo trattamento.

**Finalità, basi giuridiche e tempo di conservazione**
Il trattamento dei dati personali è necessario al fine di:
1. consentire al segnalante di effettuare una segnalazione relativa ad uno degli illeciti previsti dal D. Lgs. n.24/2023;
2. dar seguito alla segnalazione, e in particolare valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate;
3. informare il segnalante del seguito che è stato dato o che si intende dare alla segnalazione;
4. informare il segnalante delle ragioni per cui risulta necessario rivelare dati riservati e/o delle ragioni per cui risulta indispensabile, anche ai fini della difesa della persona coinvolta, rivelare l'identità del segnalante.
5. diffondere, dietro consenso del segnalante, i suoi dati personali ai fini della corretta gestione della segnalazione

In relazione alle finalità appena descritte:
- la base giuridica per le finalità da 1 a 4 è l'art. 6 (1) lett. c), in quanto il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- la base giuridica per la finalità n. 5 è l'art. 6 (1) lett. a), in quanto il trattamento è basato sul consenso dell'interessato;

I dati personali saranno conservati per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

**Conseguenze del mancato conferimento dei dati**
Il conferimento dei dati personali indicati come obbligatori è necessario per perseguire le finalità indicate: non fornire tali dati comporta l'impossibilità di effettuare il trattamento. Il conferimento degli altri dati personali è facoltativo.

**Categorie di soggetti che possono trattare dati personali, ambito di comunicazione o diffusione**
Nei limiti degli obblighi, dei compiti o delle finalità sopra indicati:
- i dati personali saranno trattati esclusivamente da dipendenti e collaboratori del Titolare, nonché da soggetti terzi nominati Responsabili ai sensi dell'art. 28 GDPR, nel rispetto di quanto previsto dalla legge anche con riguardo alle misure di sicurezza a protezione e salvaguardia dei dati stessi;
- i dati non saranno in alcun modo diffusi, salvo consenso dell'interessato.

L'elenco dei Responsabili può essere richiesto al Titolare.
Il Titolare potrà comunicare i dati personali a terzi, autonomi titolari, al solo fine di dare esecuzione ad obblighi di legge.

**Diritti dell'interessato**

L'interessato potrà, in qualsiasi momento, esercitare i diritti previsti dal Reg. UE n. 2016/679, ed in particolare il diritto:

- di accedere ai suoi dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
- di opporsi al trattamento, nel caso in cui il Titolare eserciti un proprio legittimo interesse;
- di ottenere la portabilità dei dati, ove prevista;
- di revocare il consenso, ove previsto: la revoca non pregiudica la liceità del precedente trattamento;
- di proporre reclamo all'autorità di controllo. Per l'Italia, l'autorità di controllo è l'Autorità Garante per la protezione dei dati personali (www.gpdp.it).

L'esercizio dei diritti sopra richiamati potrà avvenire attraverso l'invio di una richiesta e-mail all'indirizzo indicato sopra.

**INFORMATIVA "PERSONE COINVOLTE"**

**Titolare del trattamento**
Il Titolare del trattamento è Foppa Fustelle Group Srl, con sede in Caravaggio (BG) 24043, Viale Europa Untia 37, C.F. e P. IVA 02502560168, contattabile ai seguenti recapiti:
- scrivendo una e-mail a amministrazione@foppagroup.com
- per posta ordinaria all'indirizzo della sede indicata.

Il Titolare ha nominato un DPO-Designato Privacy contattabile alla e-mail indicata.

**Categorie di dati trattati**
Le categorie di dati trattati sono le seguenti:
- dati personali identificativi e di contatto della persona coinvolta*;
- dati personali, comuni, particolari o relativi a condanne della persona coinvolta emersi nel corso della segnalazione;
- ulteriori dati personali, comuni, particolari o relativi a condanne condivisi dalla persona coinvolta.

I dati contrassegnati con l'asterisco (*) sono obbligatori per consentire di effettuare il relativo trattamento.

**Finalità, basi giuridiche e tempo di conservazione**
Il trattamento dei dati personali è necessario al fine di:
- dar seguito alla segnalazione, e in particolare valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate;
- sentire, anche su sua richiesta, la persona coinvolta, eventualmente anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

In relazione a ciascuna delle finalità appena descritte:
- la base giuridica è l'art. 6 (1) lett. c) GDPR, in quanto il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- i dati personali saranno conservati per il tempo necessario al trattemento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

**Conseguenze del mancato conferimento dei dati**

Il conferimento dei dati personali forniti direttamente dalla persona coinvolta è facoltativo. Non fornire tali ulteriori dati non comporta l'impossibilità di procedere con l'esame della segnalazione.

**Categorie di soggetti che possono trattare dati personali, ambito di comunicazione o diffusione**
Nei limiti degli obblighi, dei compiti o delle finalità sopra indicati:
- i dati personali saranno trattati esclusivamente da dipendenti e collaboratori del Titolare, nonché da soggetti terzi nominati Responsabili ai sensi dell'art. 28 GDPR, nel rispetto di quanto previsto dalla legge anche con riguardo alle misure di sicurezza a protezione e salvaguardia dei dati stessi;
- i dati non saranno in alcun modo diffusi, salvo consenso dell'interessato.

L'elenco dei Responsabili può essere richiesto al Titolare.
Il Titolare potrà comunicare i dati personali a terzi, autonomi titolari, al solo fine di dare esecuzione ad obblighi di legge.

**Diritti dell'interessato**
L'interessato potrà, in qualsiasi momento, esercitare i diritti previsti dal Reg. UE n. 2016/679, ed in particolare il diritto:
- di accedere ai suoi dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
- di opporsi al trattamento, nel caso in cui il Titolare eserciti un proprio legittimo interesse;
- di ottenere la portabilità dei dati, ove prevista;
- di revocare il consenso, ove previsto: la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito in precedenza;
- di proporre reclamo all'autorità di controllo. Per l'Italia, l'autorità di controllo è l'Autorità Garante per la protezione dei dati personali (www.gpdp.it).

L'esercizio dei diritti sopra richiamati potrà avvenire attraverso l'invio di una richiesta e-mail all'indirizzo indicato sopra.

Gentili tutti,

comunichiamo che è stata attivata, a partire da oggi, la piattaforma di segnalazione interna (o "whistleblowing"), tramite cui qualunque soggetto che ritenga di aver rilevato un illecito commesso nell'ambito delle operazioni aziendali può segnalarlo, anche in via anonima, ad un referente individuato dalla nostra società, che gestirà la segnalazione con attenzione e riservatezza.

La piattaforma è raggiungibile al seguente indirizzo web: foppagroup.go-tell.it

A breve sarà disponibile anche tramite link diretto nel nostro sito web ufficiale.

La piattaforma, basata sul software Globaleaks, conforme allo standard ISO 37002:2021 "Whistleblowing management systems", garantisce elevati standard di sicurezza e resilienza secondo le best practices di settore, conformi alle linee guida ANAC e al Reg. UE 2016/679 ("GDPR").

I referenti designati sono la Sig.ra Rossana Macchi e il Sig. Giovanni Pirazzoli.

**Cosa è il whistleblowing?**

Il whistleblowing è un modo per segnalare comportamenti scorretti o illegali che potrebbero danneggiare la nostra azienda: questi comportamenti potrebbero includere violazioni delle nostre procedure interne o di qualsiasi altra norma applicabile, e devono essere basate su fatti concreti e devono essere inviate in buona fede.

La creazione di una piattaforma di segnalazione interna è un obbligo di legge derivante dal D. Lgs. 24/2023, che entra pienamente in vigore per tutte le società con almeno 50 dipendenti dal **17 dicembre 2023**.

**Come si effettuano le segnalazioni?**

Ricordiamo a tutti che è quindi possibile avviare le segnalazioni nei seguenti modi:

- digitale via piattaforma web (in modalità anche totalmente anonima)

Sconsigliamo di utilizzare strumenti come la e-mail semplice o la PEC per le segnalazioni, in quanto non sicuri.

Buon lavoro a tutti,

La Direzione

Go-Tell

# Piattaforma Whistleblowing Go-Tell

# Documentazione a supporto del Titolare per la valutazione di impatto sulla protezione dei dati

## CONTESTO: Panoramica del trattamento

**Quale è il trattamento in considerazione?**

La Valutazione d'Impatto sulla Protezione dei Dati (o "DPIA") è un processo che il titolare del trattamento deve effettuare ogni volta che un trattamento di dati personali, specialmente quando coinvolge nuove tecnologie, potrebbe rappresentare un rischio significativo per i diritti e le libertà delle persone, considerando la natura, l'ambito, il contesto e gli obiettivi del trattamento.

Con riferimento alla presente valutazione, inoltre, si evidenzia come il Legislatore italiano abbia previsto per legge la necessità di effettuare una DPIA in relazione alla gestione dei sistemi di whistleblowing (art. 13, co. 6, D.Lgs. 24/2023).

La DPIA è considerata uno degli elementi più importanti nel nuovo quadro normativo stabilito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), poiché cristallizza le responsabilità dei soggetti che trattano i dati.

Il titolare del trattamento, infatti, deve non solo assicurare il rispetto delle norme, ma anche dimostrare in modo adeguato come garantisce tale rispetto.

Gate2Digital S.r.l., fornitrice della piattaforma "Go-Tell", nel suo ruolo di responsabile del trattamento per la gestione del sistema di whistleblowing, con questo documento intende fornire tutte le informazioni necessarie al titolare del trattamento per effettuare compiutamente la valutazione d'impatto come previsto dall'art. 35 del Regolamento.

Ambito di analisi, pertanto, sarà la piattaforma Go-Tell e i connessi trattamenti di dati personali effettuati:

- invio di segnalazioni ai sensi del citato D.Lgs. 24/2023, in applicazione della Direttiva (UE) n. 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali;
- gestione delle segnalazioni all'interno di Go-Tell;
- archiviazione delle segnalazioni processate e loro cancellazione al termine del periodo di conservazione dei dati stabilito dal titolare del trattamento.

In relazione ai trattamenti analizzati, si segnala come Go-Tell sia una piattaforma basata sul software Globaleaks, conforme allo standard ISO 37002:2021 "Whistleblowing management systems". Go-Tell, inoltre, è istanziato all'interno di un provider europeo certificato ai sensi della normativa ISO/IEC 27001:2013 (certificato scaricabile all'indirizzo https://www.hetzner.com/assets/downloads/FOX-Certificate.pdf)

**Quali sono le responsabilità connesse al trattamento?**

Il Cliente che sceglie di utilizzare Go-Tell come piattaforma per la gestione informatica delle segnalazioni ai sensi del D.Lgs. 24/2023 opera in qualità di Titolare del trattamento.

Nel suo ruolo di Titolare del trattamento, infatti, determina finalità e modalità del trattamento (la gestione delle segnalazioni, ossia il cosiddetto "whistleblowing"), scegliendo i soggetti autorizzati alla gestione dei dati personali trattati, individuando i responsabili del trattamento da coinvolgere e, in definitiva, valutando il complesso delle operazioni di trattamento dei dati personali correlati al corretto esercizio del diritto di whistleblowing da parte dei soggetti destinatari.

Gate2Digital S.r.l., società fornitrice della piattaforma Go-Tell, opera in qualità di Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing, nel rispetto delle indicazioni fornite dal Titolare in conformità all'art. 28 del GDPR.

Gate2Digital S.r.l. ha sede in Via Alessandro Stradella n. 13 - 20129 Milano (MI). Per ogni necessità inerente al servizio è possibile scrivere a support@go-tell.it.

Per l'esecuzione del servizio SaaS Go-Tell, Gate2Digital S.r.l. ha individuato quale fornitore tecnologico Hetzner Online GmbH, società di diritto tedesco, operante per quanto qui analizzato, in qualità di Sub-Responsabile del trattamento, nominato da Gate2Digital S.r.l. per la fornitura dell'infrastruttura informatica. Per i datacenter europei, Hetzner Online GmbH non fa ricorso ad ulteriori Sub-Responsabili del trattamento. Hetzner, avente sede in Industriestrasse n. 25 - 91710 Gunzenhausen (Germany), è contattabili all'indirizzo info@hetzner.com. Hetzner Online GmbH ha, inoltre, nominato un proprio Responsabile per la Protezione dei Dati contattabile all'indirizzo data-protection@hetzner.com

**Ci sono standard applicabili al trattamento?**

In relazione al servizio analizzato, si segnala come l'infrastruttura informatica sia certificata secondo la norma ISO 27001, che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI). Il certificato può essere visionato all'indirizzo https://www.hetzner.com/pdf/en/FOX_Certificate.pdf

La piattaforma Go-Tell, basata sul software rilasciato con licenza AGPLv3 GlobalLeaks, è invece conforme allo standard ISO 37002 inerente i sistemi di gestione di whistleblowing.

L'intera piattaforma, come meglio dettagliato nel prosieguo, nasce per tutelare l'identità dei segnalanti, aventi come principio guida la minimizzazione dei dati personali trattati nel rispetto della privacy by design e privacy by default.

* * *

## CONTESTO: Dati, processi e risorse utilizzate

**Quali sono i dati trattati?**

La piattaforma Go-Tell raccoglie le seguenti tipologie di dati personali:

1. dati identificativi degli utenti registrati (nome, username, indirizzo e-mail). Le tipologie di utente registrato sono:
    - utente amministratore
    - utente custode dell'identità (figura eventuale)
    - utente gestore delle segnalazioni

2. dati personali identificativi del soggetto segnalante, nel caso in cui si sia qualificato, unitamente all'informazione di contatto ulteriore da questi indicata in fase di segnalazione (ad esempio indirizzo mail personale, numero telefonico, etc)
3. dati personali, anche particolari o inerenti condanne penali o reati, eventualmente contenute nelle segnalazioni inviate mediante la piattaforma Go-Tell, non aprioristicamente determinabili
4. dati personali identificativi e di contatto dei soggetti coinvolti nella gestione della piattaforma (referente di progetto sia lato Titolare che lato Responsabile)
5. ulteriori dati informatici tecnici necessari all'esecuzione della piattaforma informatica

I dati sopra indicati sono trattati da personale appositamente autorizzato ai sensi dell'art. 29 GDPR e da responsabili del trattamento in forza di idonea nomina ai sensi dell'art. 28 GDPR. Nello specifico:

- i dati di cui ai punti 1 e 4 saranno trattati dal Titolare del trattamento e dal Responsabile del trattamento Gate2Digital per la corretta esecuzione del contratto e del servizio da questo regolato;
- i dati di cui ai punti 2 e 3 saranno trattati unicamente dal soggetto incaricato di gestire le segnalazioni. L'utente amministratore della piattaforma può tecnicamente trattare tali dati (per finalità di conservazione degli stessi e manutenzione della piattaforma), ma tali dati sono crittografati e inintelligibili ai terzi;
- i dati di cui al punto 5 sono trattati per il solo fine di garantire la fruizione del servizio e non sono memorizzati oltre il tempo strettamente necessario (non è ad esempio salvato l'indirizzo IP del segnalante, informazioni sul device utilizzato o altre informazioni che possano identificare indirettamente il segnalante).

I dati sopra indicati sono conservati per il tempo necessario, nel rispetto del limite indicato dal D.Lgs. 24/2023 che stabilisce in 5 anni la data retention delle segnalazioni ricevute. I dati di cui ai punti 1 e 4 sono conservati per il tempo necessario a garantire l'esecuzione del contratto. I dati di cui al punto 5, come sopra specificato, non sono conservati oltre il tempo strettamente necessario per garantire la comunicazione elettronica.

**Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?**

Il ciclo di vita del trattamento è strutturato in diversi step:

1. il primo passaggio consiste nell'attivazione della piattaforma, in cui dati sopra indicati al punto 4 sono trattati per la contrattualizzazione e successiva attivazione dell'istanza di Go-Tell.
2. il secondo passaggio consiste nella configurazione della piattaforme, creando il canale di segnalazione, gli utenti registrati e associando il canale di segnalazione creato al questionario per la raccolta delle segnalazioni. Le ulteriori configurazioni effettuate non prevedono trattamento di dati personali.
3. il terzo passaggio prevede la messa in produzione del servizio Go-Tell con la condivisione del canale con i soggetti che potranno effettuare le segnalazioni. All'interno di tale step è possibile individuare i seguenti momenti:
    - invio di una segnalazione da parte di un segnalante utilizzando la piattaforma, che genera un codice di 16 cifre che il segnalante può utilizzare per rientrare nella piattaforma e vedere la propria segnalazione nonché interagire con il soggetto gestore delle segnalazioni;

- notifica a mezzo mail in merito all'avvenuta raccolta di una segnalazione (nessuna informazione specifica sulla segnalazione è presente nella notifica a mezzo mail);
- analisi della segnalazione da parte del soggetto autorizzato individuato dal Titolare del trattamento. Tale fase può essere più o meno strutturata, a seconda della tipologia e del contenuto della segnalazione ricevuta. Sostanzialmente prevede (i) una fase di riscontro al segnalante, (ii) una fase di analisi seguita ad (iii) una eventuale fase di indagini;
- la segnalazione viene quindi archiviata o viene dato seguito al contenuto della segnalazione e di tale conclusione viene dato riscontro al segnalante. Qualora fosse necessario condividere l'identità del Segnalante, nei soli casi previsti dal D.Lgs. 24/2023, tale richiesta motivata può essere condivisa con il segnalante sempre all'interno della piattaforma Go-Tell;
- la segnalazione, trascorso il periodo di data retention previsto dalla normativa, viene cancellata in modo sicuro dalla piattaforma, le eventuali copie documentali cartacee create dal gestore delle segnalazioni devono essere distrutte manualmente secondo le procedure condivise con il Titolare.

4. al termine del contratto il database crittografato contenente le segnalazioni viene condiviso con il Titolare o cancellato in modo sicuro, a seconda delle indicazioni fornite dal Titolare stesso. L'istanza di Go-Tell viene terminata e i dati personali di cui ai punti 1 e 4 sono conservati secondo gli obblighi di legge per finalità amministrative e contabili.

**Quali sono le risorse di supporto ai dati?**

L'istanza opera su sistema operativo Linux mantenuto aggiornato in relazione alle patch e agli aggiornamenti di sicurezza.

L'istanza di Go-Tell è avviata e mantenuta attiva all'interno di un docker container rootless, al fine di ulteriormente mitigare il rischio in caso di attacco, contrastando la possibilità di escalation dei privilegi.

Il sistema operativo Linux è ospitato su Virtual Private Machine fornite dal Sub-fornitore Hetzner Online GmbH all'interno dello spazio economico europeo.

Il backup è effettuato su altra Virtual Private Machine dislocata in una diversa località, così da mitigare il rischio in caso di eventi naturali disastrosi.

Le comunicazioni dirette tra le Virtual Private Machine e tra dette Virtual Private Machine e gli utenti in caso di manutenzione/aggiornamento sono effettuate mediante canali sicuri crittografati.

Non sono previste copie cartacee di documenti per l'uso della piattaforma. In ogni caso il gestore delle segnalazioni può esportare le segnalazioni (mediante creazione automatica di file di testo contenenti il contenuto delle segnalazioni e copia degli eventuali allegati presenti) o stampare tali segnalazioni. In questi casi devono essere seguite le istruzioni in tema di gestione dei dati personali contenuti in documenti cartacei indicate dal Titolare del trattamento.

* * *

## PRINCIPI FONDAMENTALI: Proporzionalità e necessità

**Gli scopi del trattamento sono specifici, espliciti e legittimi?**

Le finalità del trattamento sono specifiche e consistono nel contrasto ai fenomeni illeciti individuati dal Legislatore europeo, come declinate dal Legislatore italiano, all'interno della

realtà del Titolare del trattamento. Tale finalità è resa nota agli interessati mediante idonea informativa e attività di comunicazione interna e sensibilizzazione sul tema.

Le informazioni raccolta possono essere usate al solo fine di dar corso alle indagini su fatti oggetto di segnalazioni e per proteggere da atti ritorsivi il segnalante. In caso di manifeste segnalazioni in mala fede, il segnalante stesso può essere oggetto di sanzioni.

La legittimità di tali trattamenti emerge direttamente dal testo normativo già richiamato, il D.Lgs. 24/2023.

**Quali sono le basi legali che rendono lecito il trattamento?**

La base legale per l'esecuzione dei trattamenti già analizzati consiste nel rispetto dell'obbligo di legge cui è soggetto il Titolare del trattamento per quanto riguarda la gestione delle segnalazioni.

La base legale del consenso è applicata all'eventuale condivisione dell'identità del segnalante con soggetti terzi, nei soli casi previsti dalla normativa e quando tale condivisione sia necessaria, a seguito di specifico ed espresso consenso da parte del segnalante.

Il trattamento dei dati personali per la contrattualizzazione tra il Titolare del trattamento e Gate2Digital è basata sulla necessità di processare tali informazioni per eseguire il contratto di fornitura della piattaforma Go-Tell, mentre la successiva archiviazioni per finalità contabili e amministrative è basata sull'obbligo di legge imposto alle parti.

**I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?**

Per la creazione degli utenti registrati sono richiesti unicamente i dati identificativi quali nome, username e indirizzo di posta elettronica.

Il Titolare predispone il questionario di segnalazione al fine di raccogliere tutte e solo le informazioni ritenute rilevanti dal segnalatore per descrivere eventuali violazioni della normativa vigente, secondo i limite di cui al D.Lgs. 24/2023.

Come prima descritto, Go-Tell rispetta il principio della privacy by design: log di sistema, applicativi e firewall sono configurati per non registrate nei propri registri informazioni personali o possano portare all'individuazione dell'identità del segnalante (quali ad esempio indirizzi IP User Agents e altri metadati relativi al segnalante).

Il Titolare del trattamento può, inoltre, attivare l'uso di TOR Browser per ulteriormente proteggere l'anonimato del segnalante.

Gli ulteriori dati raccolti all'interno della segnalazione non sono aprioristicamente individuabile, come detto.

I metadati degli eventuali allegati alla segnalazione eventualmente condivisi dal segnalante non sono eliminati automaticamente dalla piattaforma Go-Tell, in quanto potrebbero contenere informazioni utili per finalità di indagine, anche in ottica di digital forensic.

**I dati sono esatti e aggiornati?**

Gli utenti registrati hanno l'onere di mantenere aggiornati i propri dati personali. Qualsiasi cambio effettuato dagli utenti registrati è applicato in tempo reale dall'intero applicativo Go-Tell.

**Qual è il periodo di conservazione dei dati?**

Il tempo di conservazione dei dati è di 5 anni nel rispetto delle indicazioni fornite dal Legislatore italiano. Eventuali segnalazioni non inerenti possono essere cancellate prima e di tale

cancellazione resta traccia nel log di audit applicativo, senza salvataggio di informazioni circa il contenuto della segnalazione eliminata.

A fronte del termine del contratto i dati sono cancellati al più tardi entro 30 giorni dal termine del rapporto con Gate2Digital.

## PRINCIPI FONDAMENTALI: Misure a tutela dei diritti degli interessati

**Come sono informati del trattamento gli interessati?**

Il Titolare ha predisposto un'informativa *ex* art. 13 da fornitore al segnalante e al facilitatore che mette a disposizione degli interessati. Tale informativa è presente anche nel questionario di segnalazione.

Il Titolare ha predisposto anche un'informativa *ex* artt. 13 e 14 per il soggetto segnalato e per il soggetto individuato a seguito delle indagini effettuate. Tale informativa viene fornita dal gestore delle segnalazioni al più presto, sempre che fornire tale informativa non vanifichi le finalità di indagine eventualmente in corso.

**Ove applicabile: come si ottiene il consenso degli interessati?**

A seconda della modalità di segnalazione scelta, il consenso potrà essere fornito nell'ambito del colloquio diretto con il gestore delle segnalazioni che dovrà formalizzare tale fase o all'interno della piattaforma Go-Tell, che permette la comunicazione biunivoca tra segnalante e gestore delle segnalazioni.

**Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?**

Gli interessati possono esercitare tali diritti direttamente all'interno della piattaforma mediante richiesta al gestore delle segnalazioni o di persona, una volta che si siano correttamente identificati.

Come specificato, la piattaforma permette la stampa o l'esportazione della singola segnalazione.

**Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?**

Gli interessati possono esercitare tali diritti direttamente all'interno della piattaforma mediante richiesta al gestore delle segnalazioni o di persona, una volta che si siano correttamente identificati. L'eventuale rettifica o cancellazione dovrà essere valutata nel rispetto dei requisiti di cui al D.Lgs. 24/2023.

**Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?**

Gli interessati possono esercitare tali diritti direttamente all'interno della piattaforma mediante richiesta al gestore delle segnalazioni o di persona, una volta che si siano correttamente identificati. L'eventuale opposizione dovrà essere valutata nel rispetto dei requisiti di cui al D.Lgs. 24/2023.

**Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?**

Il rapporto con Gate2Digital è formalizzato mediante idoneo atto giuridico ai sensi dell'art. 28 GDPR, nel quale è specificato l'ambito di trattamento legittimo (fornitura della piattaforma relativa al canale di segnalazione interno).

L'ulteriore rapporto tra Gate2Digital e Hetnzer Online GmbH è ulteriormente disciplinato mediante data processing agreement ai sensi dell'art. 28 GDPR che regolamenta il

trattamento di dati personali correlato alla fornitura della piattaforma tecnologica che ospita le istanze di Go-Tell.

**In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?**

Per l'utilizzo della piattaforma Go-Tell non viene effettuato alcun trasferimento di dati al di fuori dell'Unione Europea.

* * *

## ELENCO DI MISURE DI SICUREZZA ADOTTATE

**Crittografia**

Go-Tell implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.
Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2
Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.
Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento.
Per maggiori informazioni, si fa riferimento a quanto indicato su https://go-tell.it/specs/

**Controllo degli accessi logici**

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.
Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.
Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.
Gli accessi privilegiati alle risorse amministrative sono protetti tramite canali sicuri di comunicazioni protetti da crittografia.

**Controllo degli accessi fisici**

Gli accessi al datacenter sono regolamentati e controllati, come meglio specificati nel documento pubblicato su https://www.hetzner.com/assets/Uploads/downloads/Sicherheit-en.pdf

**Tracciabilità**

Go-Tell implementa un sistema di audit log sicuro e rispetto della privacy che registra le attività effettuate dagli utenti e dal sistema in compatibilità con la massima riservatezza richiesta dal processo di whistleblowing.
I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.
I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog.

**Archiviazione sicura**

Il backend di Go-Tell implementa un database locale SQLite protetto a cui si accede tramite l'ORM SQLAlchemy. Questa scelta progettuale è stata fatta per garantire all'applicazione il pieno controllo della sua configurazione, implementando un'ampia serie di misure di sicurezza in linea con le raccomandazioni di sicurezza di SQLite (quali cancellazione sicura, auto-vacuum, livelli di trust del database limitati, disattivazione di funzionalità non strettamente necessarie).

**Gestione delle vulnerabilità tecniche**

La piattaforma su cui si basa Go-Tell è soggetta a periodici controlli di sicurezza indipendenti per verificare e migliorare la sicurezza del sistema.
Inoltre, è attivo un progetto di bug bounty, ospitato su HackerOne.
A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.
Per maggiori informazioni, si fa riferimento a quanto indicato su https://go-tell.it/specs/

**Backup**

I backup vengono effettuati su base giornaliera con le seguenti retention:

- 7 giorni per i backup completi del sistema virtuale
- 30 giorni per i backup completi dei dati utili al ripristino completo dell'istanza

**Manutenzione**

È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.
Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale di Gate2Digital, attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.
Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale di Gate2Digital e del relativo fornitore Hetzner Online GmbH attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

**Sicurezza hardware**

I datacenter del fornitore Hetzner Online GmbH dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7, maggiori informazioni su https://www.hetzner.com/assets/Uploads/downloads/Sicherheit-en.pdf
I datacenter del fornitore sono certificati ISO 27001, certificato visionabile su https://www.hetzner.com/assets/downloads/FOX-Certificate.pdf

**Gestione dei data breach**

Gate2Digital, nel rispetto della nomina ricevuta dal Titolare del trattamento, si è dotata di una procedura per la gestione dei data breach, così da segnalare senza ritardo eventuali data breach e assistere il Titolare nelle successive fasi di indagine e comunicazione con l'autorità competente.

**Lotta contro i malware**

Tutti i computer del personale di Gate2Digital e dei sub-responsabili nominati eseguono firewall e antivirus.

**Contrasto degli attacchi che prevedano escalation dei privilegi**

Ogni istanza di Go-Tell è gestita in container docker dedicati, creati e mantenuti in modalità rootless, al fine di ulteriormente limitare le possibilità di successo di eventuali tentativi di attacco, impedendo l'escalation dei privilegi dal container al server

**Contrasto agli accessi di BOT**

Il sistema implementa una prova di lavoro automatica su ogni login che impone a ogni client di richiedere un token e di risolvere un problema computazionale prima di poter eseguire un login o presentare una segnalazione. Inoltre, il sistema implementa una limitazione della velocità delle sessioni dei whistleblower impedendo l'esecuzione di più di 5 richieste al secondo

**Sicurezza delle password**

Accedendo all'interfaccia web di login, gli amministratori e i gestori delle segnalazioni devono inserire i rispettivi nome utente e password. Se la password inserita è valida, il sistema consente l'accesso alle funzionalità disponibili per quell'utente. Il sistema implementa le seguenti misure di sicurezza per le password:

- le password non vengono mai memorizzate in chiaro ma il sistema ne mantiene a riposo solo un hash. Questo vale per ogni parola segreta, password o equivalente informazione di autenticazione, comprese le ricevute dei segnalanti;
- la piattaforma memorizza le password degli utenti con un hash casuale a 128 bit, unico per ogni utente. Le password vengono sottoposte a hash utilizzando Argon2. L'hash prevede un seme generato su base utente specifico per ciascun utente e un seme generato a partire dall'istanza della singola piattaforma;
- il sistema impone l'uso di password complesse implementando un algoritmo personalizzato necessario per garantire un'entropia ragionevole di ogni segreto di autenticazione
- il sistema implementa l'autenticazione a due fattori (2FA) basata su TOTP, con algoritmo RFC 6238 e segreti a 160 bit. Gli utenti possono attivare la 2FA tramite le proprie preferenze;
- il sistema impone agli utenti di cambiare la propria password al primo accesso. Per impostazione predefinita, il sistema impone agli utenti di cambiare la propria password con cadenza prefissata.

**Sicurezza applicativa**

La sicurezza delle applicazioni Web è implementata in conformità con le linee guida di sicurezza OWASP Session Management Cheat Sheet. I cookie non vengono utilizzati intenzionalmente per ridurre al minimo gli attacchi XSRF e ogni possibile attacco basato su di essi. Invece di utilizzare i cookie, l'autenticazione si basa su un'intestazione di sessione HTTP personalizzata inviata dal client sulle richieste autenticate.

**Sandbox intra-applicativo**

Il backend di Go-Tell integra AppArmor per impostazione predefinita e implementi un profilo di sandboxing rigoroso che consente all'applicazione di accedere solo ai file strettamente necessari. Inoltre, l'applicazione viene eseguita sotto un utente dedicato e un gruppo con privilegi ridotti.

| |
|---|
| Versione aggiornata al 10 giugno 2025 |