



**WHISTLEBLOWING  
SEGNALAZIONI TESEO ERM**

La piattaforma **WHISTLEBLOWING SEGNALAZIONI TESEO ERM** consente il dialogo tra il gestore della segnalazione ed il segnalante, attraverso modalità che garantiscono anche l'anonimato, in conformità con la normativa italiana ed europea.

Segnalazioni Teseo erm è basata sulla piattaforma GlobaLeaks ed è conforme alla legge sulla tutela dei segnalanti.

La versione che incorpora l'ambiente TESEO è facile, intuitiva e personalizzabile.

La piattaforma è stata aggiornata a seguito del recepimento della Direttiva UE 2019/1937.



# FUNZIONALITÀ

- Gestione delle segnalazioni, anche anonime, in conformità alla direttiva UE 1937/19 e D.Lgs. 24/2023;
- Compliance al Regolamento Europeo 679/16 (GDPR);
- Opzione multilingue;
- Configurazione personalizzata del form di segnalazione;
- Comunicazione diretta tra segnalante e gestore della segnalazione;
- Categorizzazione dell'illecito oggetto della segnalazione;
- Gestione delle scadenze tramite reminder (alert via mail);
- Gestione Whistleblowing per gruppi nazionali e internazionali;
- Gestione archivio documentale e conservazione delle segnalazioni.



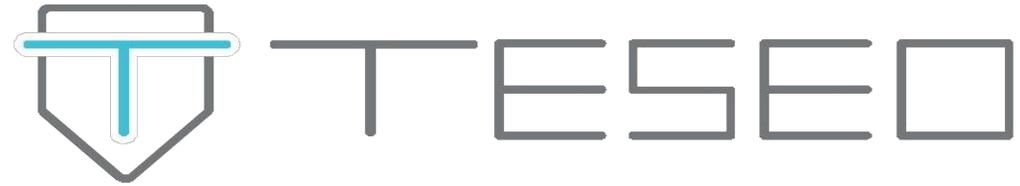
# GESTIONE IN OUTSOURCING

Laddove richiesto e se compatibile con le dimensioni dell'azienda il servizio può essere implementato anche in outsourcing attraverso un Team Esterno qualificato e indipendente.

Il canale di segnalazione in questo caso viene gestito da soggetti esterni incaricati.

La gestione in outsourcing prevede la presa in carico della segnalazione, la presa di contatti con il soggetto segnalante tramite la piattaforma, la raccolta di evidenze e la conseguente valutazione circa la pertinenza della segnalazione. Verrà poi trasmesso un report al referente aziendale interno.





# ISTRUZIONI OPERATIVE

WHISTLEBLOWING SEGNALAZIONI TESEO ERM

Il soggetto che abbia individuato una violazione rientrante nel perimetro della normativa Whistleblowing dovrà semplicemente cliccare sul link condiviso dall'azienda.

Non è richiesto alcun accesso tramite credenziali, sarà sufficiente cliccare sul tasto **“Invia una segnalazione”**



Il campo sottostante **“Hai già effettuato una segnalazione?”** consente di visualizzare lo stato di una segnalazione precedentemente effettuata per monitorarne l'andamento e le eventuali risposte del gestore, semplicemente inserendo il codice numerico rilasciato dalla piattaforma.



La piattaforma consente di selezionare, se la Società lo ha previsto, a quale azienda/dipartimento/area fa riferimento la segnalazione. Sarà sufficiente cliccarvi sopra con il cursore.



## Demo Teseo Whistleblowing

Scegli un canale di segnalazione:

**AZIENDA / DIVISIONE / AREA 1**



**AZIENDA / DIVISIONE / AREA 2**



La prima azione che può essere richiesta dalla piattaforma, nella sezione “**Selezione del Ricevente**” è quella di (eventualmente) escludere quei soggetti ai quali non si intende far pervenire la segnalazione.

La segnalazione potrebbe infatti riguardare le azioni proprio di uno dei componenti del comitato di gestione.

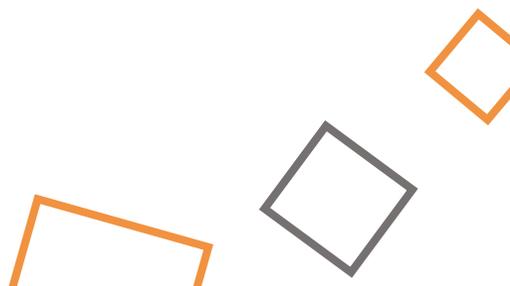
1 **Selezione Del Ricevente** 2 **DISCLAIMER** 3 **SEGNALAZIONE**

Seleziona i destinatari della tua segnalazione:

<input checked="" type="checkbox"/> <b>Gestore della Segnalazione</b>	<input type="checkbox"/> <b>Sindaco Gestore</b>
--	--

Successivo →

Per escludere (o ri-comprendere) uno o più di questi soggetti basterà spuntare la casella posta sopra al loro nome o funzione.



Alla sezione “Disclaimer” la piattaforma mostrerà una breve informativa riferita alla normativa Whistleblowing e un’informativa privacy sul trattamento dei dati personali.

Per proseguire con la segnalazione cliccare su “**Conferma**” su entrambe e poi sul tasto “**Successivo**”.

1 Selezione Del Ricevente 2 **DISCLAIMER** 3 SEGNALAZIONE

#### Disclaimer \*

Segnalazione delle violazioni di disposizioni normative nazionali o dell’Unione europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica o dell’ente privato ai sensi dell’Art. 2, comma 1, lett. a) del D.Lgs. 10 marzo 2023 n. 24, di attuazione della direttiva (UE) 2019/1937

Si comunica che la presente segnalazione verrà trattata nel rispetto della tutela della riservatezza dell’identità del segnalante, nel rispetto dell’art. 12 del D.Lgs. 10 marzo 2023 n. 24.

Si precisa, inoltre, che i dati personali del segnalante verranno trattati in ottemperanza a quanto prescritto dal Regolamento Europeo 679/2016, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51 in materia di tutela dei dati personali, come previsto dall’art. 13 del D.Lgs. 10 marzo 2023 n. 24.

È possibile effettuare segnalazioni in forma anonima. Alla conclusione del processo di segnalazione, sarà assegnato un codice ticket esclusivamente al segnalante, che gli permetterà di accedere alla segnalazione, visionare le eventuali risposte fornite e dialogare con il personale preposto. Inoltre, sarà possibile allegare ulteriori documenti. Si consiglia vivamente di memorizzare il codice in un luogo sicuro.

Nel testo della segnalazione è possibile inserire la richiesta di incontrare di persona il soggetto o i soggetti incaricati di trattare la segnalazione per esporre oralmente i fatti.

Conferma

#### Informativa sul trattamento dei dati personali \*

I dati personali forniti con la segnalazione saranno trattati in conformità alla normativa privacy vigente e all’informativa resa disponibile dalla società di cui vi invitiamo a prenderne visione.

Confermo



La sezione “**Segnalazione**” è dedicata al vero e proprio form compilabile nel quale inserire gli estremi della violazione individuata. Il form prevede campi da compilare obbligatoriamente, contrassegnati con un asterisco (\*), e campi facoltativi. È richiesto obbligatoriamente l’inserimento di un breve **titolo** che sintetizzi la problematica individuata, il suo inquadramento all’interno di una **tipologia di problema**, individuabile attraverso un menù a tendina, e di esprimere la propria volontà a fornire o meno il **consenso** a rilasciare i propri dati identificativi.

1 Selezione Del Ricevente    2 DISCLAIMER    **3 SEGNALAZIONE**

**Oggetto della segnalazione \***  
Un titolo che sintetizzi l'oggetto e la natura della segnalazione

**Tipologia di problema \***

**Anonimato \***  
Sei disposto a fornire, con la garanzia del pieno rispetto del principio di riservatezza, i tuoi dati identificativi o preferisci inoltrare la segnalazione in modo completamente anonimo?

**Vuoi fornire i tuoi dati identificativi? \***

**Nome \***  **Cognome \***

**Metodo di contatto alternativo \***

Se il consenso viene fornito, la piattaforma richiederà nome, cognome e se si desidera indicare un metodo di contatto alternativo per monitorare l’andamento della segnalazione (oltre alla piattaforma stessa).

I campi seguenti, che riguardano l'identità del segnalante e alcune specifiche informazioni inerenti la violazione individuata, non sono obbligatori. È data anche la possibilità di **allegare** documenti, immagini e altre tipologie di file.

Posizione o funzione del segnalante in azienda

Data o periodo del fatto oggetto della segnalazione

Luogo in cui si è verificato il fatto

Autore/i del fatto

Terzi a conoscenza del fatto e/o in grado di riferire sul medesimo

Allegati



Seleziona un file o trascinalo qui

Descrizione \*

← Precedente

Invia

Un ultimo campo obbligatorio richiede di fornire una breve **descrizione** della violazione individuata.



Nel caso in cui il segnalante abbia fornito i propri dati identificativi, la piattaforma chiede se questi intenda fornire o meno il **consenso** a condividere tali dati a soggetti diversi dal gestore delle segnalazioni.

Il gestore ha infatti la possibilità di coinvolgere ulteriori funzioni aziendali per la risoluzione delle problematiche segnalate, nel caso in cui lo ritenga necessario.

Se il segnalante nega tale consenso, l'unico soggetto a conoscenza della sua identità (ove dichiarata) sarà il gestore, il quale non potrà condividere tale informazione a quelle ulteriori funzioni aziendali coinvolte.

#### Consenso al trattamento

Acconsento a comunicare i miei dati personali a persone diverse da quelle competenti a ricevere le segnalazioni ai sensi degli articoli 29 e 32, paragrafo 4, del GDPR e dell'articolo 2-quaterdecies del Codice Privacy.

✓ SI

NO

← Precedente

Invia



Dopo aver premuto “Invia” la segnalazione è stata inoltrata al gestore. La piattaforma a questo punto rilascerà il **codice numerico** che il segnalante dovrà annotarsi, conservare e non divulgare a terzi. Sarà l’unico modo attraverso cui potrà **ri-accedere a questa segnalazione** per monitorarne l'andamento e le risposte del gestore, a meno che non si sia indicato un metodo alternativo di contatto.

Grazie. La tua segnalazione è andata a buon fine. Cercheremo di risponderti quanto prima.

Memorizza la tua ricevuta per la segnalazione.

4438 1211 8725 

Usa la ricevuta di 16 cifre per ritornare e vedere eventuali messaggi che ti avremo inviato o se pensi che ci sia altro che avresti dovuto allegare.

[Vedi la tua segnalazione](#)

Il pulsante “**Vedi la tua segnalazione**” consente di visualizzare immediatamente lo stato della segnalazione per controllarne gli estremi.

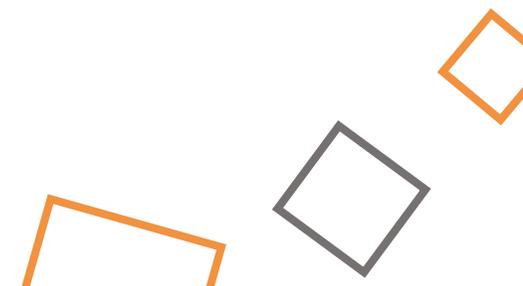
Per accedere successivamente e monitorare lo stato della segnalazione, inserire il codice numerico nella schermata iniziale e premere **“Accedi”**.

Invia una segnalazione

Hai già effettuato una segnalazione? Inserisci la tua ricevuta.

4438 1211 8725

Accedi



Ogni volta che si ri-accede alla propria segnalazione è possibile fornire (ove omessi) i propri dati identificativi, allegare nuovo materiale e inviare messaggi di testo tramite la sezione **“Commenti”**.

Vuoi fornire i tuoi dati identificativi? 

Si  No

Allegati 

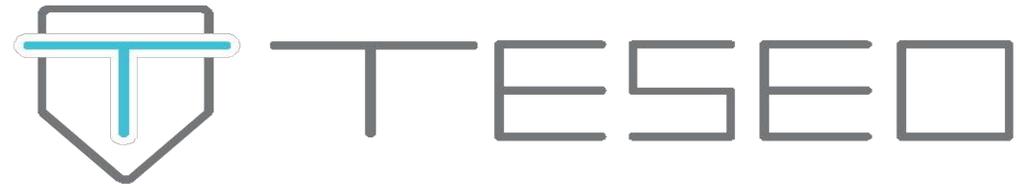
 Carica Seleziona un file o trascinalo qui

Commenti 

0/4096

 Invia





# MISURE IT

WHISTLEBLOWING SEGNALAZIONI TESEO ERM

### ❑ **Crittografia**

Implementata secondo le policies GlobaLeaks

<https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html>

### ❑ **Controllo degli accessi logici**

Log accessi da parte dei soggetti interessati

Log ricezione delle segnalazioni (non viene tenuta traccia)

I riceventi accedono tramite apposito account personale.

Credenziali di accesso vengono generate dell'utente e devono essere generate credenziali di accesso (minimo dieci caratteri, di cui 7 caratteri diversi e almeno 3 con diversi caratteri, maiuscole, minuscola, numeri, simbolo).

### ❑ **Tracciabilità**

Log di audit che identificano le attività che avvengono sulla piattaforma,

Log Utenti, Log Segnalazioni, Log Attività pianificate

### ❑ **Archiviazione**

Datacenter situato in Italia di Aruba con elevati standard di sicurezza

Data Center Rating 4 (Former Tier 4)

<https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx>

### ❑ **Gestione delle vulnerabilità tecniche**

<https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx>

### ❑ **Backup**

La macchina virtuale è già ridondata (in caso di danno fisico a un disco o a una macchina, ne esiste una sua copia che subentra automaticamente.)

### ❑ **Manutenzione**

In caso di manutenzione viene spenta la macchina che viene archiviata e poi si procede alla manutenzione (backup che poi può essere ripristinato)

### ❑ **Sicurezza dei canali informatici**

Piattaforma accessibile tramite protocollo https oppure tramite connettività onion routing browser (tor).

### ❑ **Sicurezza dell'hardware**

<https://www.datacenter.it/data-center-aruba/italia-bergamo-dc-it3.aspx>

### ❑ **Lotta contro il malware**

Accessibile solo e esclusivamente tramite https.

### ❑ **Gestire gli incidenti di sicurezza e le violazioni dei dati personali**

Gli incidenti di sicurezza e le violazioni dei dati personali vengono gestiti secondo la "Procedura Data Breach" adottata dalla Società in conformità a quanto prescritto dagli artt. 33-34 del GDPR.



# DEMO PIATTAFORMA



[CLICCARE QUI PER EFFETTUARE UNA  
SEGNALAZIONE DI PROVA](#)

