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.

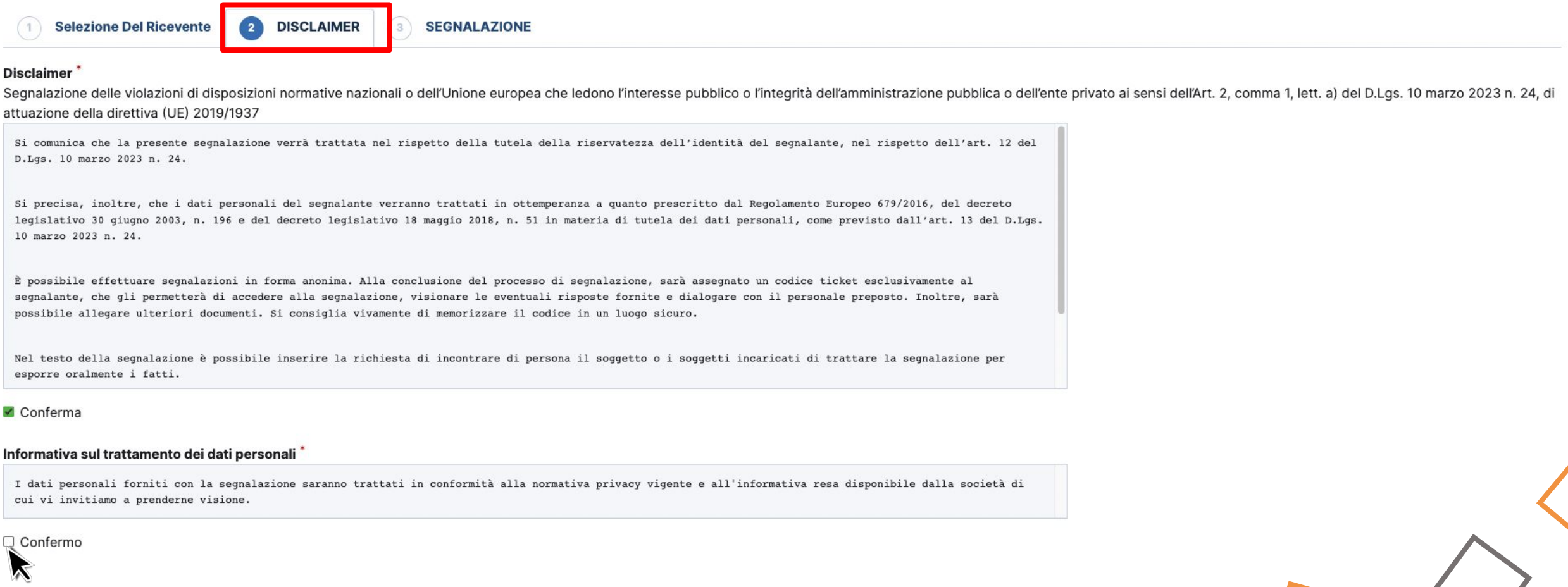
La prima azione che può essere richiesta dalla piattaforma, nella sezione **“Selezione del Ricevente”** è quella di (eventualmente) escludere quei soggetti ai quali non si intende far pervenire la segnalazione.

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

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.

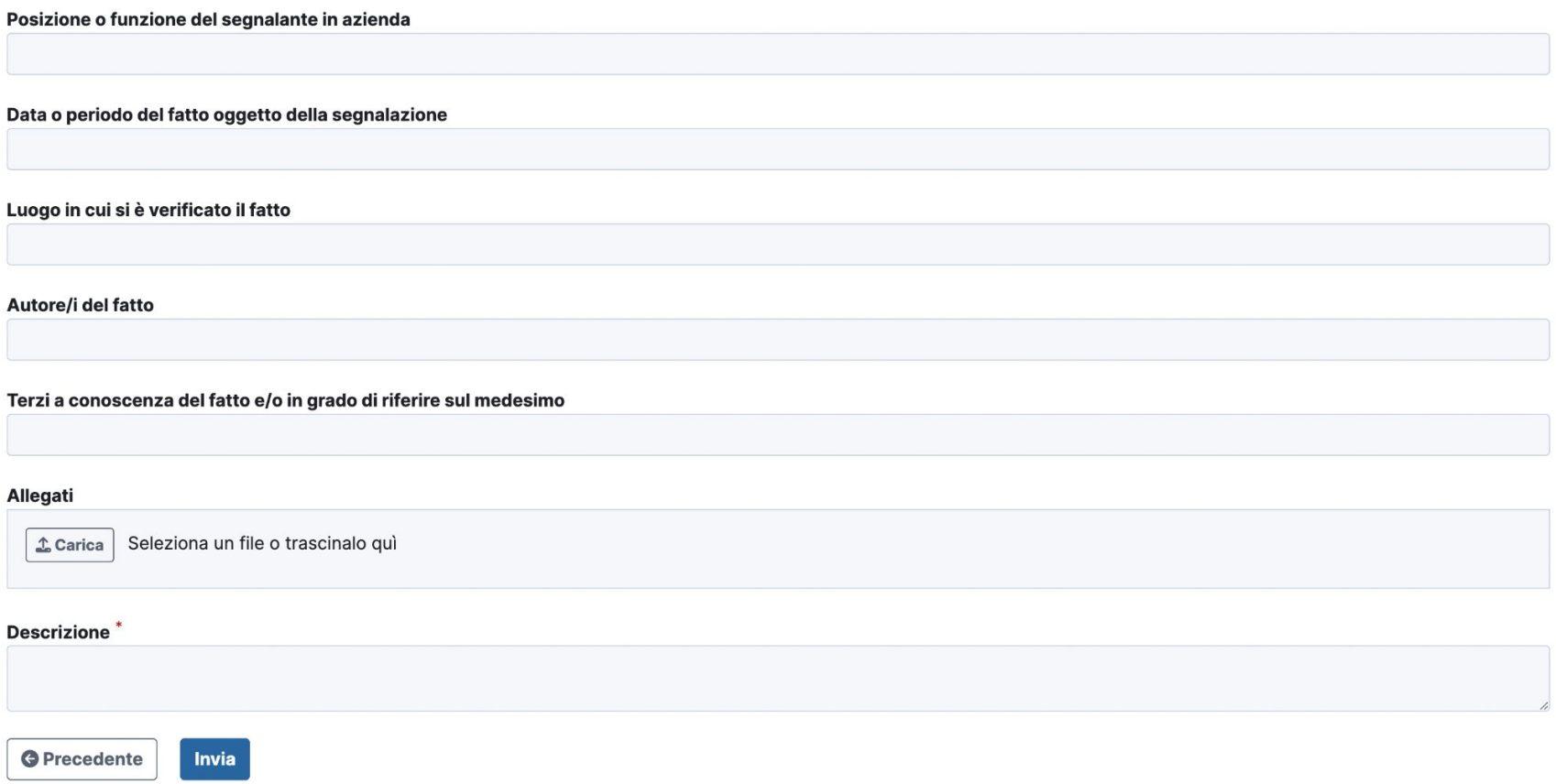
Per proseguire con la segnalazione cliccare su **“Conferma”** su entrambe e poi sul tasto **“Successivo”.**



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.

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.

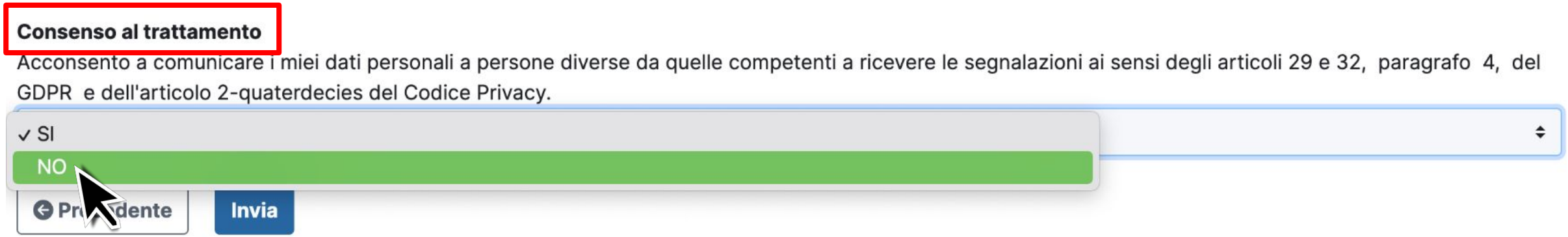


Un ultimo campo obbligatorio richiede di fornire una breve **descrizione** della violazione individuata.

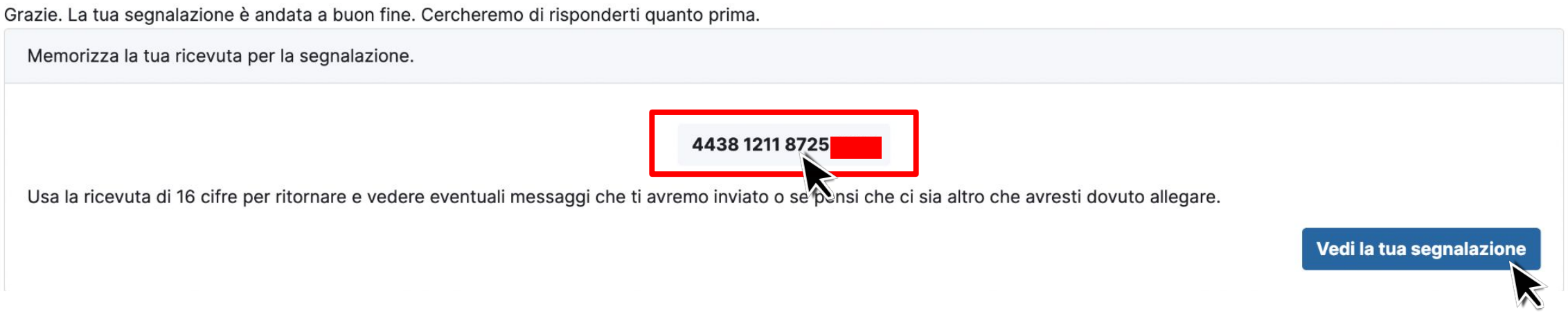
Nel caso in cui il segnalante abbia fornito i propri dati identificativi, la piattaforma chiede se questi intenda fornire o meno il **consenso** a condividere tali dati a soggetti diversi dal gestore delle segnalazioni.

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.

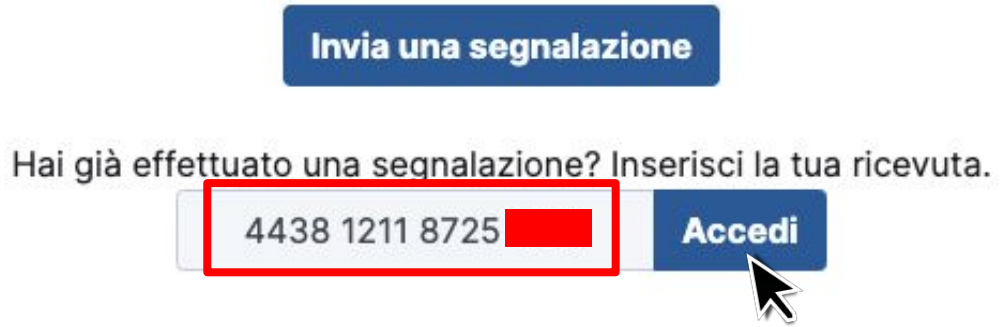


Dopo aver premuto “Invia” la segnalazione è stata inoltrata al gestore. La piattaforma a questo punto rilascerà il **codice numerico** che il segnalante dovrà annotarsi, conservare e non divulgare a terzi. Sarà l’unico modo attraverso cui potrà **ri-accedere a questa segnalazione** per monitorarne l'andamento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

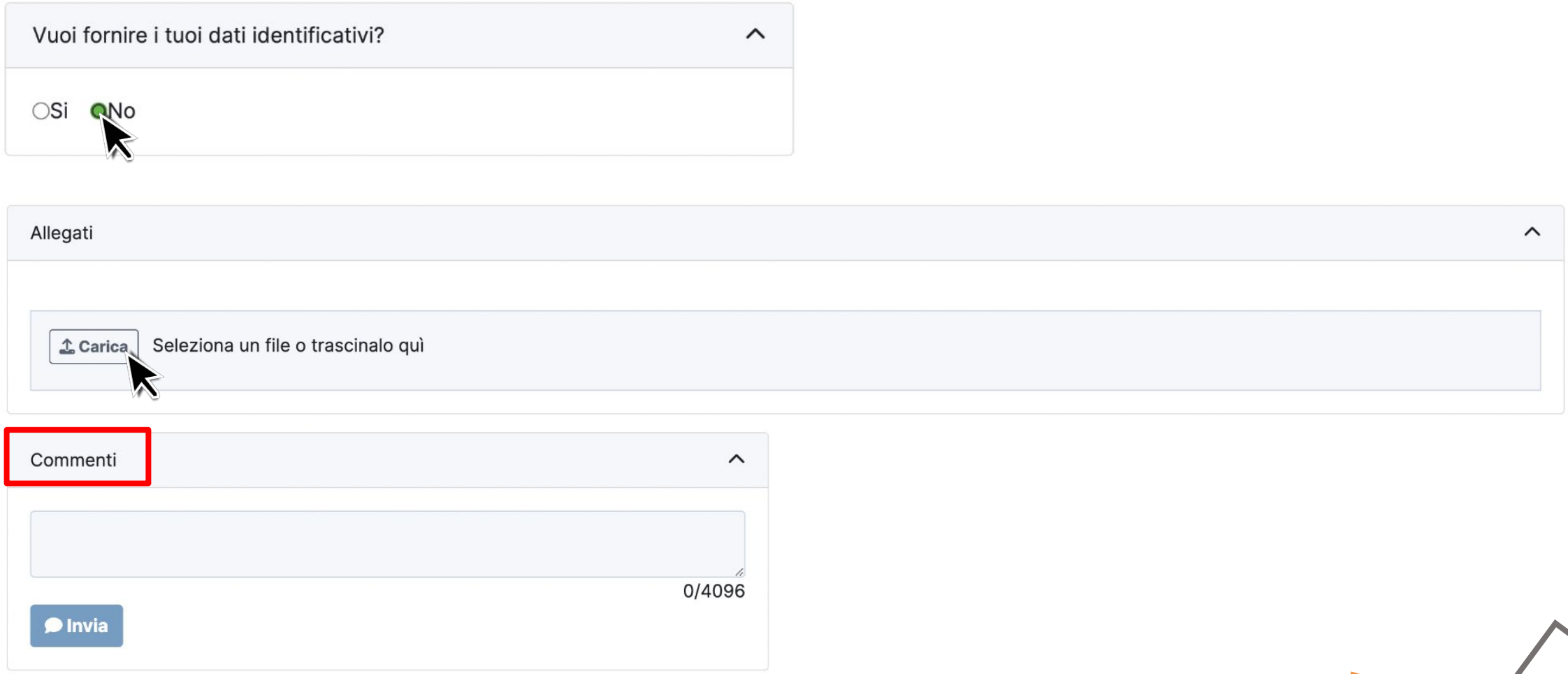


Il pulsante **“Vedi la tua segnalazione”** consente di visualizzare immediatamente lo stato della segnalazione per controllarne gli estremi.

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



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”.**



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.

TESEO

DEMO PIATTAFORMA

CLICCARE QUI PER EFFETTUARE UNA SEGNALAZIONE DI PROVA


TESEO