Regolamento per la gestione delle segnalazioni di illeciti (Whistleblowing) e per la tutela del Segnalante (Whistleblower)

ai sensi del D.lgs. 24/2023

CRONOLOGIA DELLE REVISIONI

09/12/2023	Versione 1 – Prima stesura

Sommario

1 – Premessa, scopo del documento e riferimenti normativi

Il Decreto Legislativo n. 24 del 10 marzo 2023, recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali" (di seguito il "Decreto"), ha esteso in maniera significativa il perimetro di applicazione della disciplina in materia di segnalazioni, in precedenza limitata, per il settore privato, ai soli enti dotati di Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001. In particolare, il Decreto individua e disciplina i soggetti segnalanti, l'oggetto delle segnalazioni di violazione, i canali da istituire e prevedere, gli adempimenti e le tutele che le società sono tenute a implementare e garantire, definendone inoltre i criteri e le tempistiche di adeguamento.

Nell'impostazione di tale sistema di segnalazioni, si è inoltre tenuto in debita considerazione quanto riportato dalle "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali" approvate da ANAC con Delibera n° 311 del 12 luglio 2023 (di seguito anche "Linee Guida ANAC")

La Fior di Grano Snc di Apis Mariano con sede legale in Osimo (AN), Via Po n. 9, P.IVA 01325540423 (di seguito "Fior di Grano") con il presente regolamento intende dare attuazione al Decreto sopra menzionato al fine rimuovere i fattori che possono disincentivare o ostacolare il ricorso all'istituto, come ad esempio dubbi e incertezze circa le modalità da seguire e timori di ritorsioni o discriminazioni. L'obiettivo perseguito è quello di fornire al whistleblower chiare indicazioni operative in merito all'oggetto, ai contenuti, ai destinatari e alle modalità di trasmissione delle segnalazioni, nonché circa le forme di tutela che gli vengono offerte nel nostro ordinamento.

In particolare il regolamento intende:

- chiarire i principi ispiratori dell'istituto, evidenziando le regole che la Fior di Grano deve osservare;
- precisare le modalità di gestione delle segnalazioni;
- dettagliare le modalità seguite per tutelare la riservatezza dell'identità del Segnalante, del contenuto della segnalazione e dell'identità di eventuali altri soggetti indicati.

2 – Ambito di applicazione

L'ambito di applicazione del Regolamento riguarda tutti i comportamenti, gli atti o le omissioni che ledono l'interesse o l'integrità della Fior di Grano e che consistono in:

1. illeciti amministrativi, contabili, civili o penali che non rientrano nei numeri 3), 4), 5) e 6);

2. condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6);
3. illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al d.lgs. 23 marzo 2023 n. 24 ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato citato in precedenza, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
4. atti o omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;
5. atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
6. atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5);

Le disposizioni regolamentari non si applicano:

a) alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona Segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate;
b) alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al d.lgs. 23 marzo 2023 n. 24 ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato citato in precedenza;
c) alle segnalazioni di violazioni in materia di sicurezza nazionale.

3 – Soggetti tutelati

Nel caso di segnalazioni, denunce all'Autorità giudiziaria o contabile, divulgazioni pubbliche di informazioni sulle violazioni conosciute nell'ambito del proprio contesto lavorativo, le disposizioni del presente Regolamento si applicano, in particolare:

a) ai dipendenti della Fior di Grano;

b) ai titolari di un rapporto di collaborazione, ai sensi dell'articolo 2 del decreto legislativo n. 81 del 2015, che svolgono la propria attività lavorativa presso la società;
c) ai lavoratori o i collaboratori che svolgono la propria attività lavorativa presso soggetti che forniscono beni o servizi o che realizzano opere in favore della società;
d) ai liberi professionisti ed ai consulenti che prestano la propria attività presso la società;
e) ai volontari ed ai tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Fior di Grano;
f) all'azionista ed alle persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

La tutela delle persone segnalanti si applica anche qualora la segnalazione, la denuncia all'autorità giudiziaria o contabile o la divulgazione pubblica di informazioni avvenga nei seguenti casi:

a) quando il rapporto giuridico, nei casi indicai nel paragrafo precedente, non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
b) durante il periodo di prova;
c) successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

Fermo quanto previsto nell'articolo 17, co. 2 e co. 3, del d.lgs. 24/2023, le misure di protezione di cui al capo III, si applicano anche:

a) ai facilitatori;
b) alle persone del medesimo contesto lavorativo della persona Segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile 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;
c) ai colleghi di lavoro della persona Segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
d) agli enti di proprietà della persona Segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle già menzionate persone.

4 – La segnalazione interna e il suo contenuto

La Fior di Grano ha istituito un canale di segnalazione interna che garantisce la riservatezza dell'identità della persona Segnalante, della persona coinvolta e della persona comunque

menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

In armonia all'art. 4, co. 5, del d.lgs. 24/2023, la gestione del canale di segnalazione interna è affidata all'Ufficio Amministrativo della Società Fior di Grano snc di Mariano Apis (nel seguito "Gestore delle Segnalazioni").

A tal fine, le segnalazioni possono essere effettuate mediante il canale criptato messo a disposizione dalla Società Team System e raggiungibile al seguente indirizzo internet **https://fiordigrano.smartleaks.cloud**, il cui portale è liberamente accessibile dalla Sezione Società trasparente quale sezione del sito istituzione della Fior di Grano al seguente indirizzo Internet: **http//www.fiordigrano.com**.

Si rinvia all'allegato A quale parte integrante e sostanziale del presente regolamento per la spiegazione di tutte le fasi che il Segnalante deve seguire per inoltrare la segnalazione tramite il portale di cui sopra.

I dati della segnalazione sono scorporati dai dati identificativi del Segnalante ed automaticamente inoltrati, per l'avvio tempestivo dell'istruttoria al Gestore delle Segnalazioni, il quale riceve una comunicazione di avvenuta presentazione, con il codice identificativo della stessa (senza ulteriori elementi di dettaglio).

I dati identificativi del Segnalante sono custoditi, in forma crittografata e sono accessibili solamente al Gestore delle Segnalazioni.

Il Gestore delle Segnalazioni accede alla propria area riservata e alle informazioni di dettaglio delle varie segnalazioni ricevute.

Di norma, la segnalazione deve contenere almeno i seguenti elementi:

- l'identità del soggetto che effettua la segnalazione;
- la descrizione chiara e completa dei fatti oggetto di segnalazione
- le circostanze di tempo e di luogo in cui i fatti sono stati commessi;
- le generalità o gli altri elementi che consentano di identificare il soggetto/i che ha/hanno posto/i in essere i fatti segnalati;
- l'indicazione di eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione;
- l'indicazione di eventuali documenti che possano confermare la fondatezza di tali fatti;
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

Il whistleblower deve fornire tutti gli elementi utili affinché si possa procedere alle verifiche ed agli accertamenti a riscontro della fondatezza dei fatti segnalati.

La tutela dell'anonimato non è sinonimo di accettazione di comunicazioni anonime, considerato che la tutela del whistleblower si riferisce a segnalazioni provenienti da soggetti individuabili e riconoscibili.

Fermo quanto stabilito dal paragrafo precedente, la Fior di Grano si riserva di prendere in considerazione le segnalazioni anonime, ove queste si presentino adeguatamente circostanziate e rese con dovizia di particolari, siano tali cioè da far emergere fatti di particolare gravità e con un contenuto che risulti adeguatamente dettagliato, circostanziato e relazionato a contesti determinati (es.: indicazione di nominativi o qualifiche particolari, menzione di uffici specifici, procedimenti o eventi particolari, ecc.).

Il canale informatico di segnalazione interna adottato dalla Fior di Grano rappresenta la principale forma di segnalazione attraverso la quale i segnalatori possono effettuare le segnalazioni.

Non si possono escludere segnalazioni in forma scritta o orale così come previste dal Decreto. In ogni caso tali forme devono avere natura residuale in quanto non possono garantire, per lora natura, quelle forme di riservatezza che un canale informatico criptato riesce a garantire.

In particolare, la segnalazione scritta può essere effettuata secondo le seguenti modalità:

- con posta ordinaria (in busta sigillata apponendo la dicitura esterna “NON APRIRE Riservata personale”) inviandolo al seguente indirizzo: Fior di Grano – Via Po 9 – 60027 Osimo (AN)
- con posta interna (inserendolo in busta sigillata apponendo la dicitura esterna “NON APRIRE - Riservata personale”);
- con posta elettronica certificata (PEC) al seguente indirizzo istituito in modo specifico per le segnalazioni di cui al presente regolamento: **trasparenzafdgwh@pec.it.**

Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona Segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

Se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, la segnalazione, previo consenso della persona Segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all’ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona Segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del personale addetto. La persona Segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Quando, su richiesta della persona Segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, essa, previo consenso della persona Segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all’ascolto oppure mediante verbale. In caso di verbale, la persona Segnalante può verificare, rettificare e confermare il verbale dell’incontro mediante la propria sottoscrizione.

5 – La gestione delle segnalazioni interne

Nell'ambito della gestione del canale di segnalazione interna, il Gestore delle Segnalazioni, sia nell'ambito del canale informatizzato sia nel caso di segnalazioni scritte, orali o con incontro diretto, attua le seguenti fasi:

a) fase di PRESA IN CARICO della segnalazione:

- Entro 7 giorni dalla ricezione, rilascia al Segnalante conferma del ricevimento della segnalazione;
- Mantiene le interlocuzioni con la persona Segnalante, a cui possono essere richieste, se necessario, integrazioni alla segnalazione;

b) fase di VALUTAZIONE DI AMMISSIBILITA':

il Gestore della segnalazione provvede a dare diligente seguito alle segnalazioni ricevute, avviando tempestivamente l'analisi preliminare della Segnalazione al fine di verificare la conformità della stessa alle norme applicabili e al presente Regolamento, in particolare valutando l'ammissibilità e la fondatezza dell'esposto.

Questa fase si potrà concludere alternativamente:

- con l'archiviazione motivata della segnalazione che non rientri nell'ambito oggettivo del presente Regolamento;
- con l'apertura della successiva fase finalizzata ad intraprendere ogni opportuna azione per valutare la sussistenza dei fatti segnalati.

b) fase di ISTRUTTORIA DI MERITO della Segnalazione qualora non archiviata in quanto ritenuta non ammissibile:

questa fase rappresenta l'insieme delle attività finalizzate a verificare nel merito il contenuto delle segnalazioni, in cui va garantita la massima riservatezza circa l'identità del Segnalante e l'oggetto della segnalazione.

Tale fase ha lo scopo principale di verificare nel merito la veridicità delle informazioni sottoposte ad indagine e di formalizzare i fatti accertati, attraverso attività di verifica interna con l'utilizzo di tecniche investigative obiettive ed il supporto delle strutture aziendali competenti ed interessate rispetto al contenuto della Segnalazione.

Qualora siano necessarie audizioni del Segnalante (o di altri soggetti interessati, testimoni o periti), le informazioni raccolte e/o i documenti consegnati devono essere debitamente archiviati.

Questa fase si dovrà concludere con un giudizio circa la fondatezza della segnalazione che consiste:

- con l'archiviazione della segnalazione che risultino prive di fondamento o non sia stato possibile accertare i fatti o per altri motivi;
- con la comunicazione ai Titolari dell'Azienda dell'esito dell'istruttoria interna,

mediante trasmissione di un Report riepilogativo delle azioni svolte e delle informazioni assunte, nel caso in cui la segnalazione risulti fondata e i fatti in essa segnalati siano accertati.

In tale Report, verrà dato atto:

- delle evidenze raccolte;
- delle informazioni assunte;
- dei fatti accertati;
- delle azioni intraprese per l'istruttoria;
- delle eventuali azioni mitigative e/o correttive.

A seguito della trasmissione del Report, potranno essere definite ed intraprese dalla Società azioni mitigative e/o correttive, oltre a quelle volte a comminare, se del caso, sanzioni disciplinari in linea con quanto previsto dalla normativa applicabile, dai contratti collettivi di lavoro di riferimento e dalle procedure applicabili a tutela degli interessi della Società (ad es. provvedimenti disciplinari, azioni giudiziarie, interruzione del rapporto in essere).

Durante questa fase, il Gestore delle Segnalazioni continuerà a mantenere rapporti con il Segnalante, informandolo sullo stato di avanzamento dell'istruttoria, almeno con riferimento ai principali snodi decisionali. Al fine di garantire la massima trasparenza nella gestione della segnalazione, il Whistleblower potrà sempre accedere alla Piattaforma e conoscere lo status di lavorazione della segnalazione, utilizzando il codice numerico che viene generato dalla Piattaforma al termine dell'inserimento della segnalazione, nel caso di utilizzo del canale informatico riportato nel presente regolamento.

Entro tre mesi dalla data dell’avviso di ricevimento, il Gestore delle Segnalazioni dovrà fornire un riscontro al Segnalante, informandolo del seguito che viene dato o che si intende dare alla segnalazione.

In ogni caso, terminata l'istruttoria, il Gestore delle Segnalazioni comunicherà al Segnalante l’esito finale della procedura di segnalazione, che consentirà di chiudere la segnalazione.

Si rinvia all’allegato B quale parte integrante del presente regolamento per quanto attiene alle specifiche tecniche di gestione delle Segnalazioni sul portale informatico scelto dalla Società.

6 – Le Segnalazioni esterne

È possibile effettuare una Segnalazione esterna qualora, al momento della presentazione, ricorra una delle seguenti condizioni:

a. il canale di segnalazione interna di cui al precedente capitolo 4 non è attivo;
b. la persona Segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto alcun seguito;

c. il whistleblower ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
d. il Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Il ricorso alla segnalazione esterna è, pertanto, residuale, rispetto alla segnalazione interna.

È onere della persona Segnalante valutare la ricorrenza di una delle situazioni elencate sopra prima di procedere ad effettuare una segnalazione esterna.

Le segnalazioni esterne sono effettuate dal Segnalante direttamente all'Autorità Nazionale Anti Corruzione (ANAC), mediante i canali appositamente predisposti. Si tratta di:

- Piattaforma informatica, accessibile al seguente al seguente url: **https://servizi.anticorruzione.it/segnalazioni/#/**
- Segnalazioni orali;
- Incontri diretti fissati entro un termine ragionevole.

Nel sito istituzionale di ANAC, cliccando il link alla pagina dedicata, si accede al servizio dedicato al "whistleblowing" (**https://www.anticorruzione.it/-/whistleblowing**), ove si trovano indicazioni chiare e facilmente accessibili relative al canale, ai soggetti competenti cui è affidata la gestione delle segnalazioni, nonché alle procedure.

Per tutto quanto non previsto nel presente capitolo si rimanda al sito istituzionale dell'ANAC.

7 – Obbligo di riservatezza

Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

L'identità della persona Segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona Segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

Nell'ambito del procedimento disciplinare, l'identità della persona Segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona Segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione è utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona Segnalante alla rivelazione della propria identità. È dato avviso alla persona Segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati, qualora la rivelazione dell'identità della persona Segnalante e delle informazioni connesse sia indispensabile anche ai fini della difesa della persona coinvolta.

Fermo quanto previsto dall'art. 12 del d.lgs. 24/2023, nei procedimenti avviati in ragione di una segnalazione, la persona coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

8 – Divulgazioni pubbliche

La persona Segnalante che effettua una divulgazione pubblica beneficia della protezione prevista dal presente decreto se, al momento della divulgazione pubblica, ricorre una delle seguenti condizioni:

a. la persona Segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna, alle condizioni e con le modalità previste dai capitoli 4 e 5 e non è stato dato tempestivo riscontro in merito alle misure previste o adottate per dare seguito alle segnalazioni;
b. la persona Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
c. la persona Segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

Restano ferme le norme sul segreto professionale degli esercenti la professione giornalistica, con riferimento alla fonte della notizia.

9 – Condizioni per la protezione della persona Segnalante

Le misure di protezione previste dal Capo III del d.lgs. 24/2023 si applicano alle persone di cui all'art. 3 quando ricorrono le seguenti condizioni:

a. al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica, la persona Segnalante o denunciante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate fossero vere e rientrassero nell'ambito oggettivo di cui all'art. 1 del presente regolamento;
b. la segnalazione o divulgazione pubblica è stata effettuata sulla base di quanto previsto dal capitolo 8 del presente regolamento e, in generale, dal Capo II del d.lgs. 24/2023.

I motivi che hanno indotto la persona a segnalare o denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

È impregiudicata la responsabilità penale e disciplinare del whistleblower nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi degli artt. 368 e 595 del Codice Penale e dell'articolo 2043 del Codice Civile.

Quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona Segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, non sono garantite le tutele stabilite dal Capo III del d.lgs. 24/2013 e, alla persona Segnalante o denunciante, è altresì irrogata una sanzione disciplinare.

Le medesime misure sono applicate anche ai casi di segnalazione o denuncia all'autorità giudiziaria o contabile o divulgazione pubblica anonime, se la persona Segnalante è stata successivamente identificata e ha subito ritorsioni.

10 – Divieto di ritorsione

Gli enti e le persone indicate del capitolo 3 non possono subire alcuna ritorsione.

Nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento di comportamenti, atti o omissioni vietati ai sensi del presente articolo nei confronti delle persone di cui al capitolo 3, si presume che gli stessi siano stati posti in essere a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia è a carico di colui che li ha posti in essere.

In caso di domanda risarcitoria presentata all'autorità giudiziaria dalle persone indicate dal capitolo 3, se tali persone dimostrano di aver effettuato, ai sensi del d.lgs. 24/2023, una segnalazione, una divulgazione pubblica o una denuncia all'autorità giudiziaria o contabile e di aver subito un danno, si presume, salvo prova contraria, che il danno sia conseguenza di tale segnalazione, divulgazione pubblica o denuncia all'autorità giudiziaria o contabile.

Costituiscono ritorsioni le fattispecie elencate dall'art. 17, comma 4, del d.lgs. 24/2023 e, in particolare:

a. il licenziamento, la sospensione o misure equivalenti;
b. la retrocessione di grado o la mancata promozione;
c. il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
d. la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
e. le note di merito negative o le referenze negative;

f. l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
g. la coercizione, l'intimidazione, le molestie o l'ostracismo;
h. la discriminazione o comunque il trattamento sfavorevole;
i. la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
j. il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
k. 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. la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
m. l'annullamento di una licenza o di un permesso;
n. la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Sono nulli gli atti assunti in violazione del presente articolo e, in generale, dell'art. 17 del d.lgs. 24/2023. Le persone di cui al capitolo 3 che siano state licenziate a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile hanno diritto a essere reintegrate nel posto di lavoro, in ragione della specifica disciplina applicabile al lavoratore.

Gli enti e le persone di cui al capitolo 3 possono comunicare all'ANAC le ritorsioni che ritengono di avere subito.

Il Segnalante che ritiene di aver subito una discriminazione o una ritorsione può, altresì, dare notizia circostanziata dell'avvenuta discriminazione al Gestore delle Segnalazioni che, valutata tempestivamente la sussistenza degli elementi, segnala l'ipotesi di discriminazione alle autorità competenti.

Resta fermo ed impregiudicato la facoltà del Segnalante di dare notizia dell'accaduto alle organizzazioni sindacali o all'Autorità Giudiziaria competente.

11 – Limitazione della responsabilità

Non è punibile l'ente o la persona di cui al capitolo 3 che riveli o diffonda informazioni sulle violazioni coperte dall'obbligo di segreto o relative alla tutela del diritto d'autore o alla protezione dei dati personali ovvero riveli o diffonda informazioni sulle violazioni che offendono la reputazione della persona coinvolta o denunciata, quando, al momento della rivelazione o diffusione, vi fossero fondati motivi per ritenere che la rivelazione o diffusione delle stesse informazioni fosse necessaria per svelare la violazione e la segnalazione, la divulgazione pubblica o la denuncia all'autorità giudiziaria o contabile è stata effettuata ai sensi del presente Regolamento.

Quando ricorrono le ipotesi di cui al precedente paragrafo, è esclusa altresì ogni ulteriore responsabilità, anche di natura civile o amministrativa.

Salvo che il fatto costituisca reato, l'ente o la persona di cui al capitolo 3 non incorre in alcuna responsabilità, anche di natura civile o amministrativa, per l'acquisizione delle informazioni sulle violazioni o per l'accesso alle stesse.

In ogni caso, la responsabilità penale e ogni altra responsabilità, anche di natura civile o amministrativa, non è esclusa per i comportamenti, gli atti o le omissioni non collegati alla segnalazione, alla denuncia all'autorità giudiziaria o contabile o alla divulgazione pubblica o che non sono strettamente necessari a rivelare la violazione.

12 – Formazione e condivisione delle informazioni

Affinché possa essere garantita adeguata visibilità nei luoghi di lavoro ed accessibilità alle persone che, pur non frequentando tali luoghi, intrattengano un rapporto giuridico con la Fior di Grano, il Regolamento è pubblicato nel sito internet istituzionale della Società nella sezione "Società trasparente".

Nella medesima sezione del sito internet saranno pubblicati i seguenti documenti:

- le specifiche tecniche e informatiche rilasciate, sotto la propria responsabilità, dalla Società Team System che ha realizzato per conto della Fior di Grano il canale informatico dedicato per le segnalazioni riportate nel presente regolamento;
- Il manuale utente del Segnalante che accede alla piattaforma informatica per effettuare le segnalazioni;
- Il manuale utente del ricevente le segnalazioni sempre nell'ambito della piattaforma informatica.

Inoltre, per il personale interno la Fior di Grano prevede la definizione di una formazione dedicata alla divulgazione del contenuto del presente Regolamento al fine di assicurare a tutto il personale di conoscere le modalità tecniche e operative per agevolare la possibilità di effettuare le Segnalazioni di illeciti o irregolarità di cui vengono a conoscenza nell'ambito della propria attività lavorativa.

Il canale preferenziale scelto dalla Fior di Grano per dare massima diffusione alle disposizioni del presente regolamento è il canale INTRANET dell'Azienda.

Tale formazione sarà nuovamente erogata laddove si dovesse rendere necessaria (ad esempio, su richiesta espressa del personale o in caso di variazione dei soggetti che sono coinvolti nella gestione delle segnalazioni).

E' previsto inoltre un percorso formativo specifico per il personale dell'Ufficio Amministrativo di Fior di Grano addetto alla gestione delle segnalazioni con preferenza per la formazione a distanza su piattaforme FAD che rilasciano attestati di frequenza e valutazione a fine corso.

Si precisa inoltre che, in conformità a quanto previsto dall'art. 18 del d.lgs. 24/2023, presso ANAC è istituito l'elenco degli enti del Terzo settore che forniscono misure di sostegno alle persone segnalanti.

Si rinvia al d.lgs. 24/2023 per quanto non espressamente previsto nel presente regolamento.

13 – Privacy e sicurezza

Nell'ambito della gestione delle segnalazioni, la Fior di Grano tratta i dati personali dei soggetti Segnalanti ed eventualmente di altre categorie di soggetti interessati indicati da questi negli esposti presentati.

La Società si configura come autonomo Titolare del trattamento ed assicura il rispetto dei principi fondamentali e degli obblighi derivanti dal Regolamento (UE) 2016/679 (GDPR):

- alla luce del principio di «liceità, correttezza e trasparenza», al Segnalante viene resa specifica Informativa sul trattamento dei dati personali, in cui vengono presentate le informazioni principali relative al trattamento (ad es. la finalità, i tempi di conservazione dei dati personali, le basi di liceità del trattamento, le categorie di dati personali trattati ed i soggetti coinvolti nel trattamento), nonché vengono illustrati i diritti del Segnalante e le relative modalità di esercizio;
- alla luce del principio di «minimizzazione», vengono raccolti esclusivamente i dati personali necessari per il perseguimento delle finalità. In caso di raccolta accidentale di dati non necessari, questi vengono immediatamente cancellati;
- alla luce del principio della «limitazione della conservazione», le segnalazioni e tutta la documentazione che costituisce la pratica non possono essere utilizzate oltre i termini di conservazione il termine di conservazione è fissato in anni 5 (cinque) dalla comunicazione al Segnalante dell'esito finale della procedura di segnalazione.

La Società Team System, quale fornitore di servizi coinvolti nel processo di gestione delle segnalazioni, è designata quale responsabile del trattamento dei dati (ai sensi dell'art. 28 GDPR), sulla base delle specifiche tecniche di cui all'allegato C parte integrante e sostanziale del presente regolamento.

14 – Adozione del regolamento e successivi aggiornamenti

Il presente Regolamento è stato approvato con apposito atto dal legale rappresentate della Fior di Grano e sarà oggetto di successivi aggiornamenti sempre approvati con le medesime modalità nel caso si rendessero necessari cambiamenti significati nell'ambito della sua applicazione.

15 – Allegati

Costituiscono parte integrante e sostanziale del presente regolamento i seguenti allegati:

ALLEGATO A – Manuale del Segnalante

ALLEGATO B – Manuale del Gestore delle segnalazioni

ALLEGATO C - Documentazione a supporto del titolare per la valutazione di impatto sulla protezione dei dati e sulla sicurezza

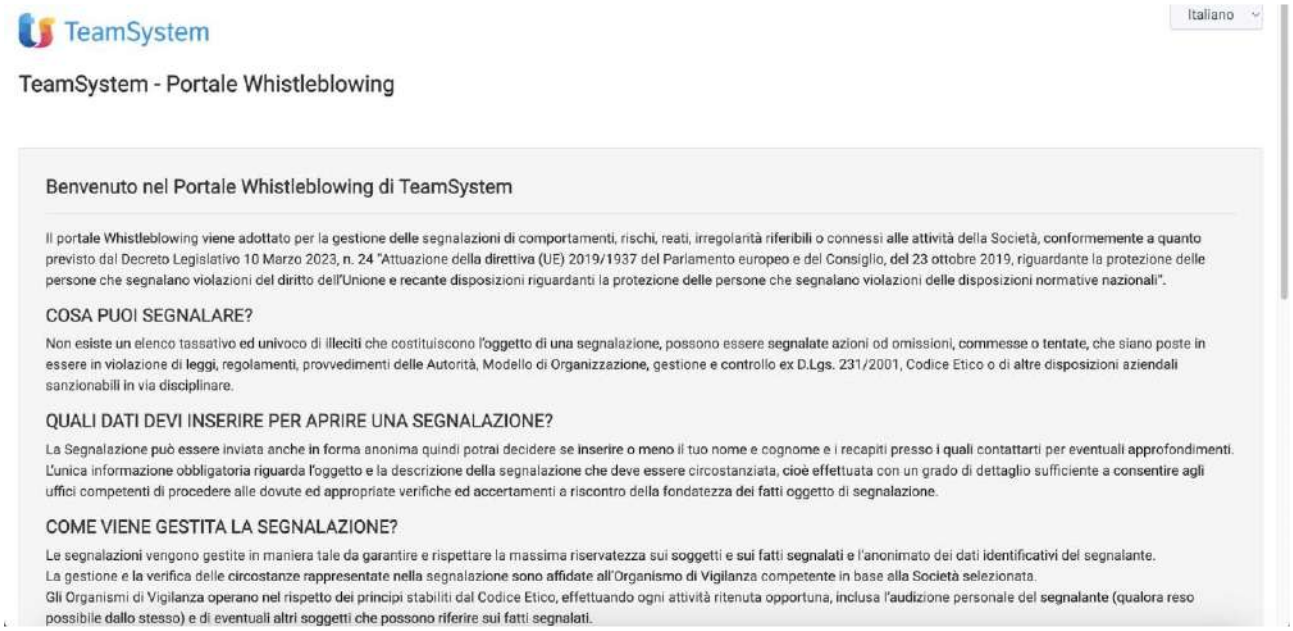
ALLEGATO A

MANUALE DEL SEGNALANTE

PROCEDURE PER LE SEGNALAZIONI INTERNE TRAMITE L'UTILIZZO DEL CANALE INFORMATICO

Accesso al portale

È possibile accedere alla piattaforma di Whistleblowing cliccando sul seguente link: **https://fiordigrano.smartleaks.cloud.**

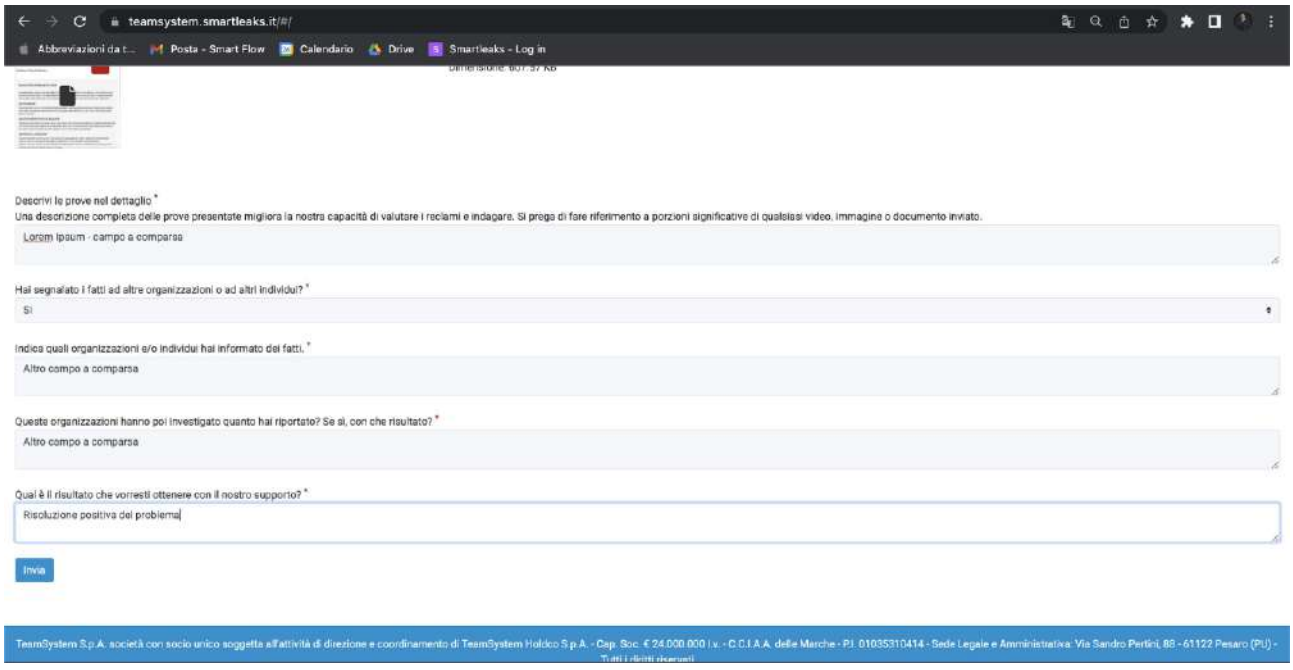


Effettuare una segnalazione

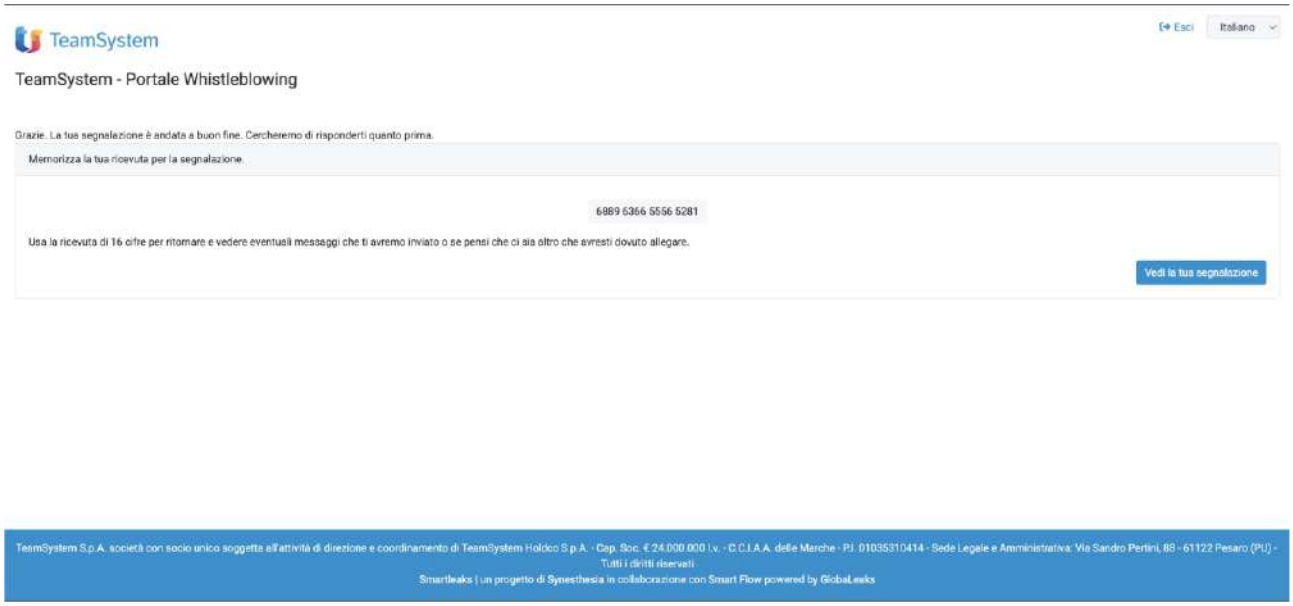
a) Per inviare una segnalazione il Segnalante dovrà cliccare sul pulsante «Invia una segnalazione», disponibile in fondo alla pagina principale della piattaforma.

b) La piattaforma potrebbe contenere più canali: scegliere il canale dell'azienda collegata alla segnalazione. Sarà presentato un questionario a cui rispondere. Notare bene: le domande contrassegnate con asterisco (*) sono obbligatorie

c) Con un click sul pulsante «Invia» che si trova al fondo del questionario, il Segnalante invia la segnalazione.



d) Il sistema tutela la riservatezza della comunicazione e l'anonimato del Segnalante, è necessario quindi conservare con cura il codice fornito nel momento dell'invio della segnalazione. In caso di smarrimento dell'identificativo sarà necessario effettuare una nuova segnalazione al sistema.



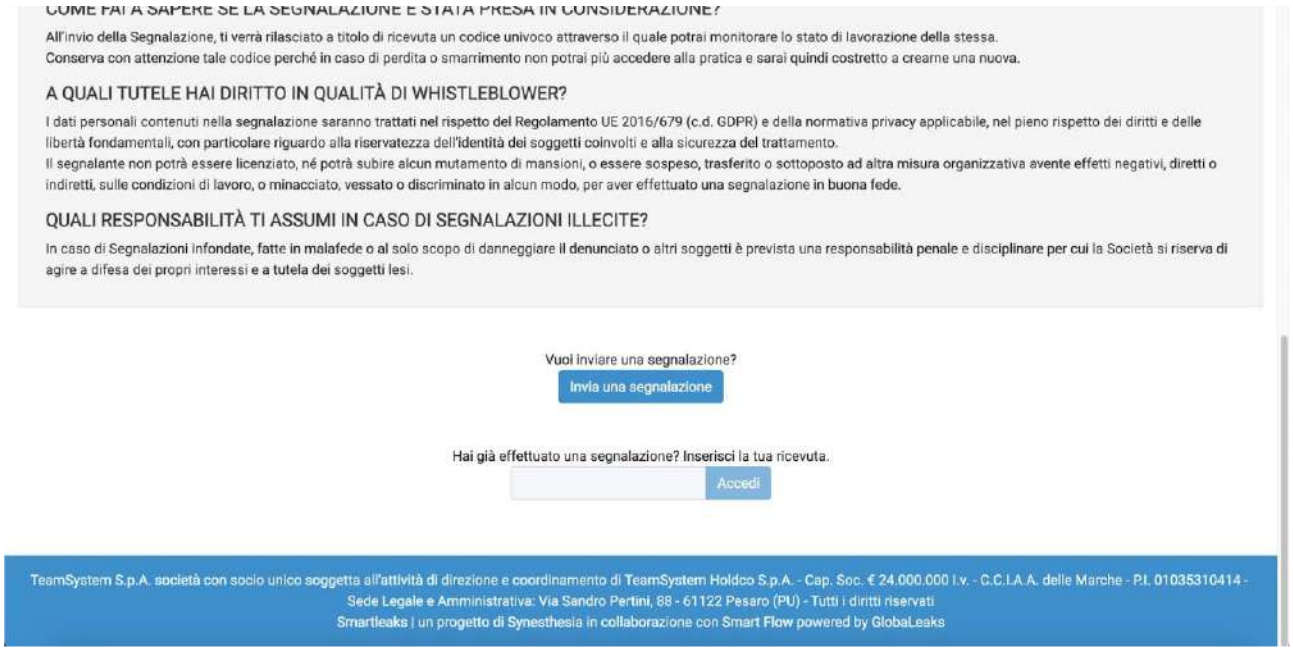
L'identificativo della segnalazione (il codice) consente all'utente di monitorare lo stato di avanzamento della segnalazione, integrare la segnalazione effettuata con eventuali informazioni aggiuntive, scambiare messaggi privati con l'incaricato della gestione delle segnalazioni mantenendo la massima riservatezza.

3649 5250 4669 0573

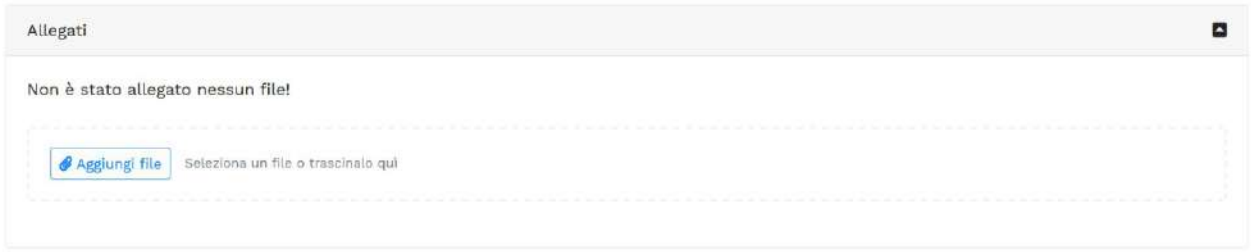
CODICE DI ESEMPIO

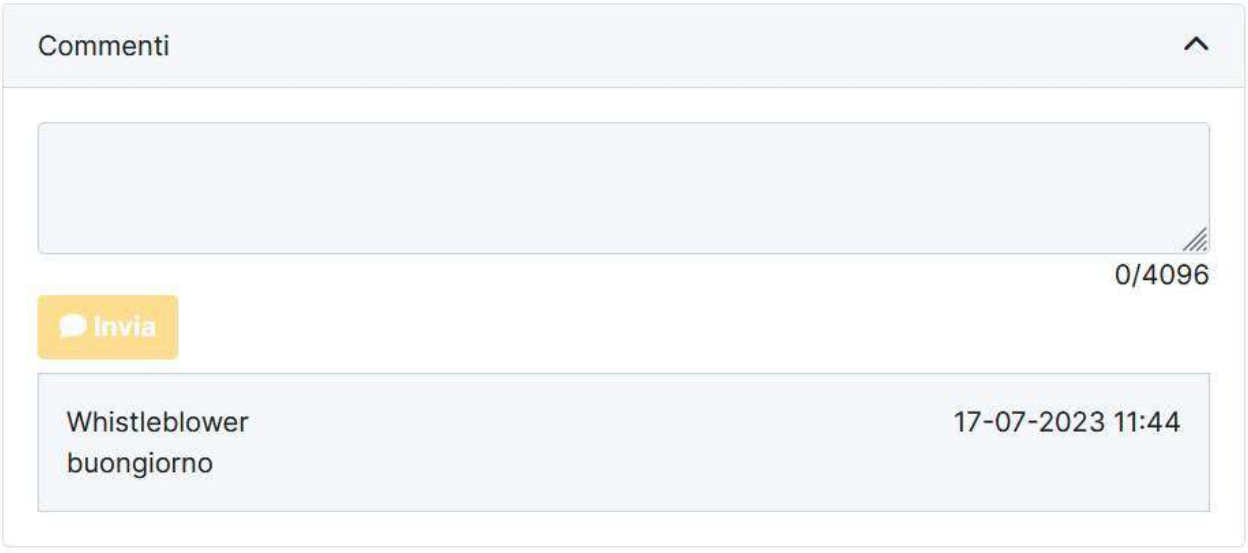
Monitorare una segnalazione già effettuata

Quando l'utente volesse verificare lo stato della segnalazione da lui inserita è sufficiente che esso si connetta al sito principale ed inserisca l'identificativo della segnalazione (ricevuta), fornito al primo inserimento della segnalazione, all'interno dell'apposito spazio evidenziato.



È possibile, in questo modo, controllare lo stato di avanzamento della propria segnalazione, aggiungere altri file e tenere aperto il canale di comunicazione con il ricevente della segnalazione con il ricevente attraverso l'apposito box.





ALLEGATO B

MANUALE DEL GESTORE DELLE SEGNALAZIONI

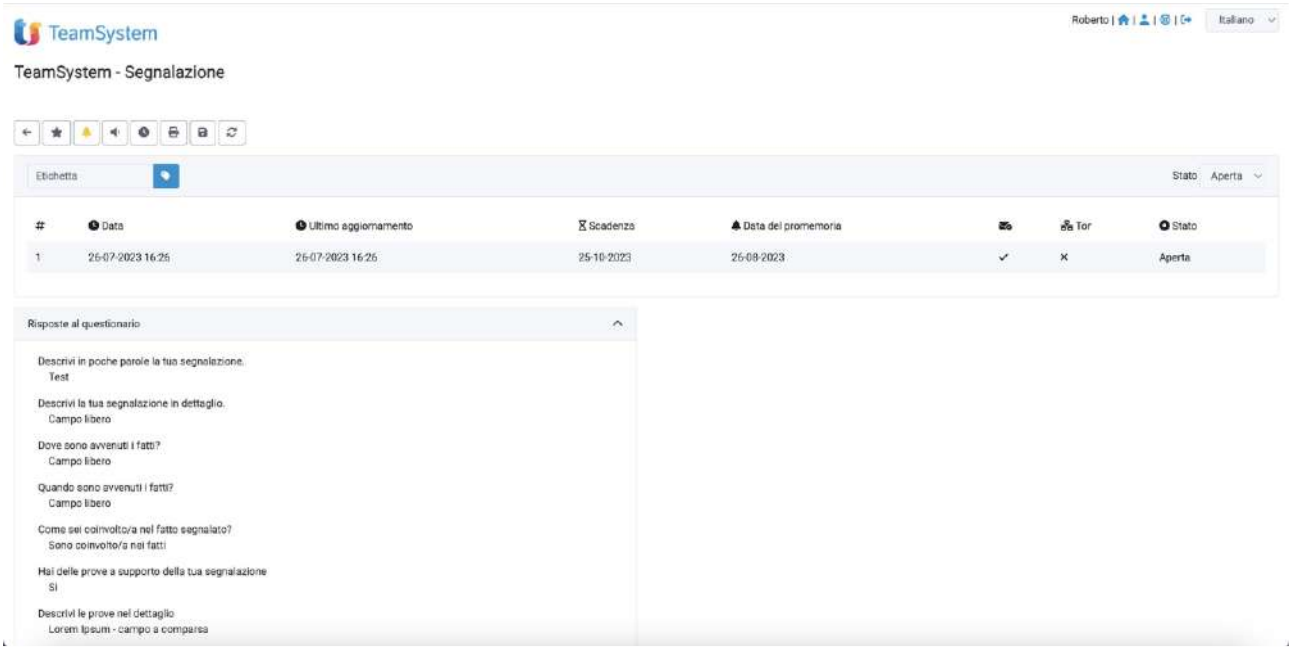
PROCEDURE PER LA GESTIONE DELLE SEGNALAZIONI TRAMITE L'UTILIZZO DEL CANALE INFORMATICO

Accesso al portale

Il Ricevente può accedere al portale anche tramite il link che è contenuto in una notifica di segnalazione avvenuta.

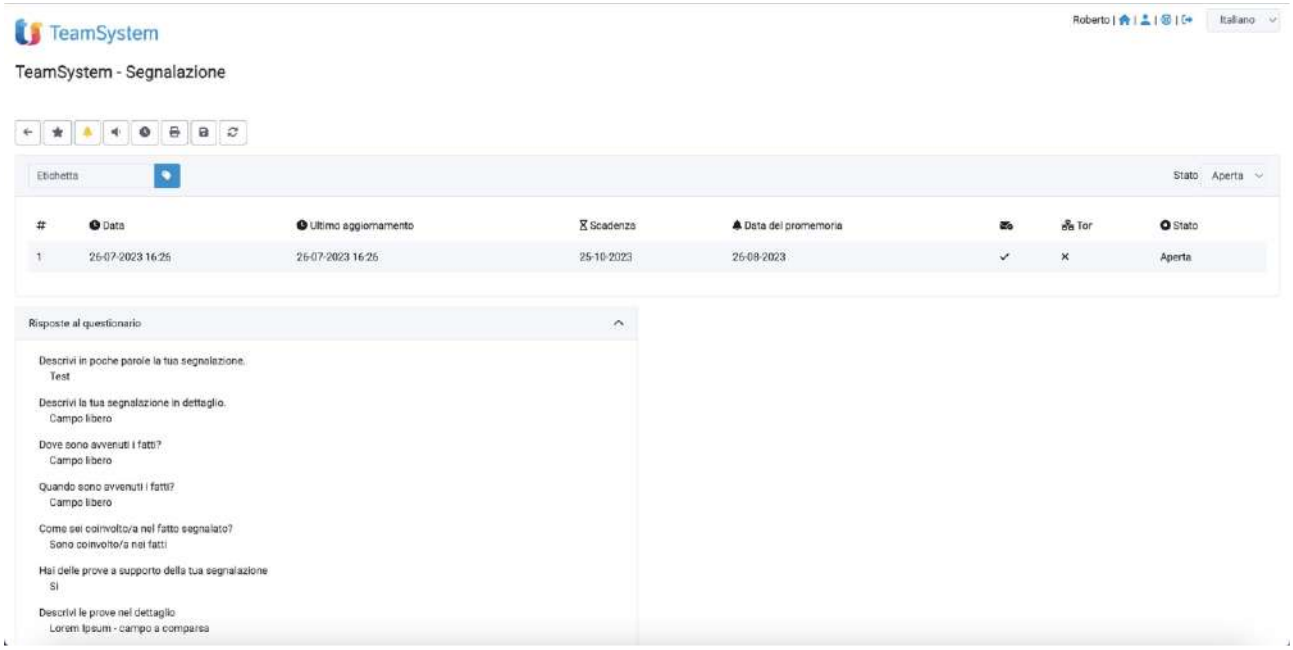
Gestione della segnalazione

Il Gestore delle Segnalazioni vede le risposte al questionario compilato dal Segnalante.



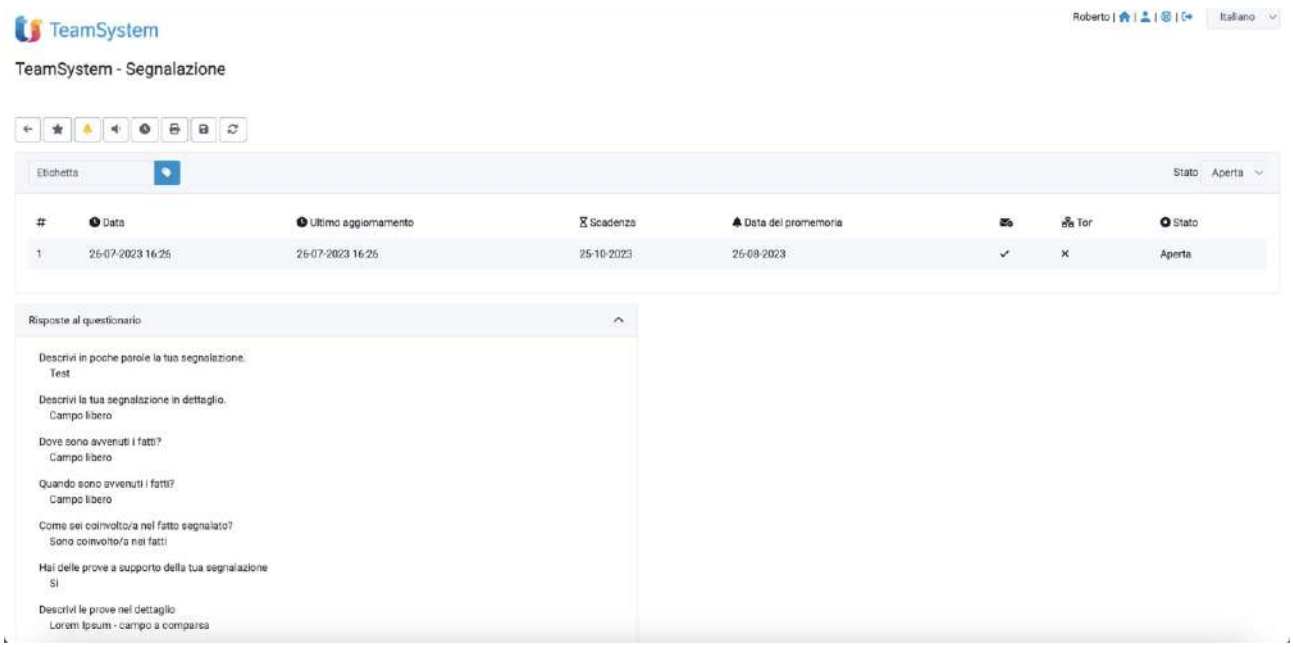
Nella sezione evidenziata, il Gestore delle Segnalazioni vede:

1. Il pulsante per tornare al menu principale;
2. La stellina, per contrassegnare la Segnalazione come importante;
3. La campanella, per impostare una notifica email di promemoria;
4. Il tasto per abilitare e disabilitare le notifiche da questa Segnalazione;



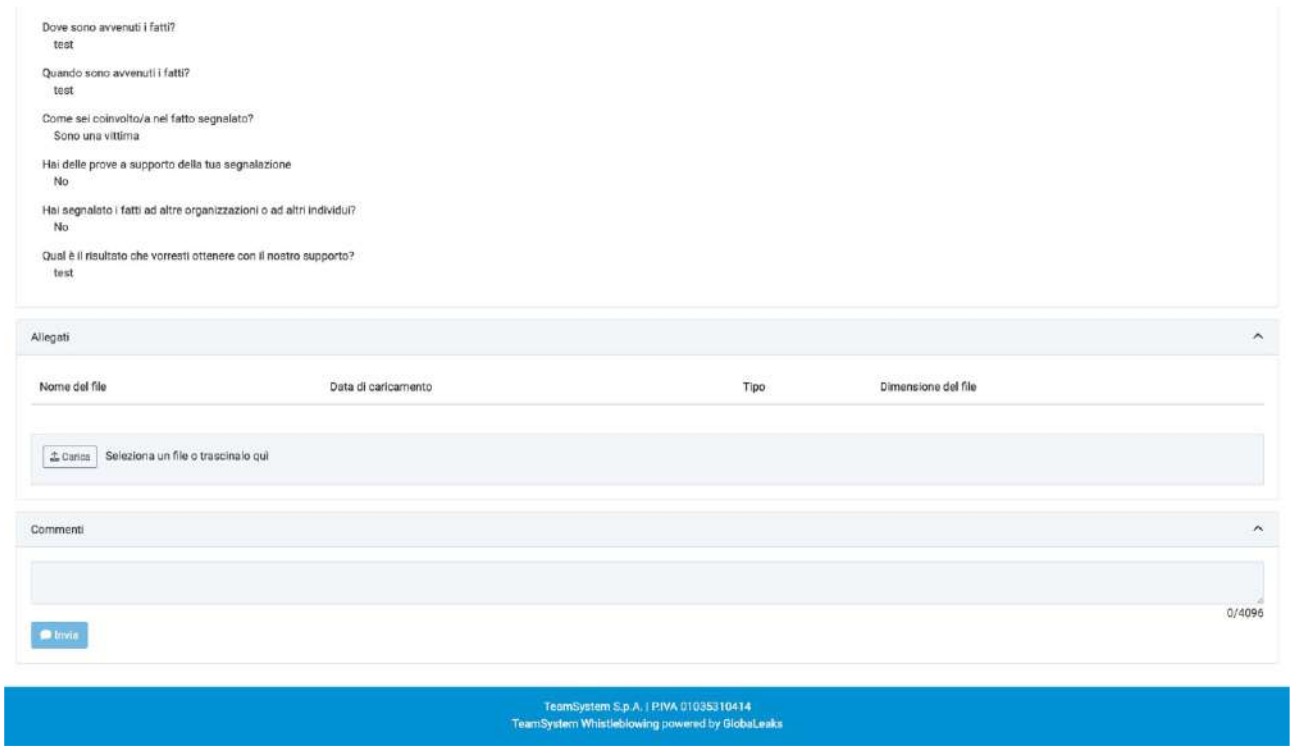
Nella sezione evidenziata, il Gestore delle Segnalazioni vede:

1. Il numero della segnalazione;
2. Il canale di segnalazione;
3. La data in cui la segnalazione è stata effettuata;
4. L'ultimo aggiornamento sulla segnalazione: quando il Segnalante o il Ricevente effettuano un aggiornamento (un commento o il caricamento di un allegato), la data si aggiorna;
5. La scadenza, ovvero fino a quando la segnalazione deve essere conservata;
6. La data del promemoria;
7. Se il Ricevente ha letto la versione più recente della Segnalazione;
8. Se la segnalazione è stata effettuata tramite Tor browser;
9. Lo stato della Segnalazione.



In calce alla segnalazione, il Gestore delle Segnalazioni vede e ha la possibilità di scaricare gli eventuali allegati del Segnalante.

Inoltre, può scrivere un messaggio per il Segnalante e caricare egli stesso degli allegati.



ALLEGATO C

DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI E SULLA SICUREZZA

TeamSystem, in qualità di responsabile del trattamento, si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

Accordi per la protezione dei dati personali: https://www.teamsystem.com/dpa/

La piattaforma informatica di segnalazione è basata sul software TeamSystem Whistleblowing powered by GlobaLeaks.

MISURE DI SICUREZZA

CRITTOGRAFIA

L'applicativo implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. 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.

Protocollo crittografico:
https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

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 supporta protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

TRACCIABILITÀ

L'applicativo implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità 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 e registri remoti centralizzati.

ARCHIVIAZIONE

L'applicativo implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

GESTIONE DELLE VULNERABILITÀ TECNICHE

Globaleaks è periodicamente soggetto ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. 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.

Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

BACKUP

I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

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 e per quelli che compongono l'infrastruttura fisica e di backup è prevista una modalità di manutenzione accessibile al personale TeamSystem e ai relativi fornitori, Smart Flow e Synesthesia, attraverso cui svolgere le modifiche al sistema e installare gli aggiornamenti.

SICUREZZA DEI CANALI INFORMATICI

Tutte le connessioni sono protette tramite protocollo TLS 1.2+ e connessioni con protocollo SSH.

SICUREZZA DELL'HARDWARE

I datacenter del fornitore dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24.

Il fornitore di hosting è certificato ISO 9001:2015 e ISO 27001:2013.

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

TeamSystem ha definito una procedura per la gestione delle violazioni dei dati personali.

Privacy Policy: https://www.teamsystem.com/privacy-policy/

LOTTA CONTRO IL MALWARE

I computer del personale di TeamSystem e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale e il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti

le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

SUB - RESPONSABILI

- **Smart Flow Srl SB**
  P.IVA: 11592420019
  Corso Giuseppe Siccardi, 11 bis - 10122
  Torino (TO) Sito web: https://smart-flow.it
  Configurazione dei portali Whistleblowing, assistenza clienti
- **Synesthesia Srl SB**
  P. IVA 10502360018
  Corso Dante, 118 - 10126
  Torino (TO) Sito web:
  https://www.synesthesia.it
  Sviluppo e manutenzione software e hardware
- **Host.it**
  P.IVA 08505460017
  Corso Svizzera 185, 10149
  Torino (TO) Sito web:
  https://host.it
  Servizio di hosting

TRASFERIMENTO DI DATI PERSONALI

Non viene effettuato alcun trasferimento di dati personali. In particolare i dati rimangono sul territorio italiano.

RIEPILOGO DELLE MISURA DI SICUREZZA FISICHE ADOTTATE

- Credenziali di autenticazione, assegnate individualmente ad ogni addetto.
  - Autenticazione mediante user-id e password.
  - Parola chiave di almeno 12 caratteri.
  - Disattivazione delle vecchie credenziali.
  - Disposizioni scritte per la disponibilità dei dati.
- Cifratura dei dati memorizzati.
- Cifratura dei dati trasmessi.
  - Cifratura con protocollo PGP.
- Sospensione automatica delle sessioni di lavoro.
- Sospensione manuale delle sessioni di Lavoro.
- Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia

adeguate contromisure che garantiscano un rischio residuale basso.

- Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda
- Verifica ed eventuale nomina degli amministratori di sistema se presenti
- Pseudonimizzazione.
- Trattamento dei dati con protocolli criptati.
- Profili di autorizzazione di ambito diverso per diversi incaricati.
    - È utilizzato un sistema di autorizzazione.
    - I profili di autorizzazione vengono specificati prima di ogni trattamento.
    - Verifica periodica del profilo di autorizzazione.