FIRSTANCE
PRIVATE INSURANCE PLATFORM

Policy* in materia di *Whistleblowing

Versione	1
Approvato da	Consiglio di Amministrazione del 6.12.2023
Funzione Responsabile	Legal & Compliance

SOMMARIO

1. PREMESSA

Firstance S.r.l. (di seguito la "Firstance" o la "Società") si impegna costantemente a condurre la propria attività con onestà e integrità. Tuttavia, va riconosciuto il fatto che ogni azienda è soggetta al rischio di azioni scorrette o comportamenti illeciti.

È quindi dovere della Società adottare le misure adeguate a identificare tali situazioni al fine di porvi rimedio. Incoraggiando a livello aziendale una cultura aperta e responsabile, è possibile inoltre contribuire a prevenire le stesse situazioni.

Tutto il personale della Società è tenuto ad osservare le procedure e le *policy* adottate d Firstance e a segnalare qualsiasi comportamento che non rispetti i principi fondamentali in esso contenuti.

Ogni singolo soggetto ha la responsabilità di esprimere eventuali timori su possibili condotte illecite nell'ambito del contesto lavorativo.

2. QUADRO NORMATIVO DI RIFERIMENTO

Nell'ambito delle disposizioni che disciplinano l'attività svolta dagli intermediari assicurativi, l'articolo 35 della Direttiva 2016/97 (IDD) sulla distribuzione assicurativa (recepita dal d.lgs. n. 68/2018) prevede che le Autorità pongano in atto meccanismi efficaci per consentire e incoraggiare le segnalazioni di violazioni attinenti allo svolgimento di attività assicurativa o di distribuzione assicurativa.

I meccanismi individuati dalla Direttiva prevedono:

- procedure specifiche per il ricevimento delle segnalazioni e per il relativo seguito;
- protezione adeguata dei dipendenti, dei collaboratori di imprese e di intermediari e, ove possibile, di altri soggetti che riferiscono di violazioni commesse all'interno dell'impresa o dell'intermediario contro ritorsioni, discriminazioni e altri tipi di trattamento iniqui;
- la protezione dell'identità sia della persona che segnala le violazioni sia della persona sospettata di essere responsabile della violazione, in tutte le fasi della procedura.

La nuova disciplina sul whistleblowing è stata recepita negli articoli 10-quater e 10-quinquies del CAP (in vigore dal 1°ottobre 2018) al fine di prevenire o far emergere illeciti o irregolarità all'interno delle organizzazioni aziendali operanti nel mercato assicurativo e, più in generale, favorire una cultura della legalità e della trasparenza.

Con riferimento alle disposizioni in materia di "Antiriciclaggio", il 4 luglio 2017 è entrato in vigore il Decreto Legislativo del 25 maggio 2017, n. 90 che ha modificato e riscritto integralmente, anziché emendarlo, il contenuto del Decreto Legislativo del 21 novembre 2007, n. 231 (di seguito anche "D.Lgs. n. 231/2007"). L'articolo 48 del Capo VII ("segnalazioni di violazioni") del D.Lgs. n. 231/2007 prevede l'introduzione del sistema di segnalazione di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo (c.d. whistleblowing).

Da ultimo, il legislatore italiano ha provveduto a recepire – per il tramite del Decreto Legislativo n. 24 del 10 marzo 2023 (di seguito anche "d*ecreto whistleblowing*") – la direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio riguardante "*la protezione delle persone che segnalano violazioni del diritto dell'Unione Europea*". In particolare, il decreto *whistleblowing* ha abrogato la disciplina nazionale previgente in materia di *whistleblowing* e, nello specifico, l'art. 6, comma 2-*bis*, lett. a) del Decreto Legislativo 8 giugno 2001, n. 231, come successivamente modificato e integrato (il "Decreto 231/01"), regolamentando in toto la disciplina in materia di segnalazione *whistleblowing*[1].

Tali disposizioni normative mirano a definire i requisiti minimi necessari per la predisposizione di sistemi di *whistleblowing*, volti a consentire al personale di segnalare atti e fatti che possano costituire una violazione delle norme che regolano il contrasto al riciclaggio e al finanziamento del terrorismo, garantendo al contempo la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto segnalato.

3. AMBITO DI APPLICAZIONE

La presente Policy si pone l'obiettivo di individuare idonee e comuni soluzioni organizzative in materia di *whistleblowing*, in conformità con quanto previsto dalle diverse citate disposizioni normative e proporzionalmente al profilo dimensionale e alla complessità operativa della Società.

Come sopra riportato, la normativa primaria applicabile alla Società circoscrive il "perimetro oggettivo" del *whistleblowing*:

- agli "*atti o fatti che possano costituire violazione delle norne disciplinanti l'attività assicurativa e distributiva svolta";*
- alle "*violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo*";
- alle violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato, previste dal decreto whistleblowing. Sono escluse dall'applicazione di tale decreto le fattispecie indicate all'art. 1, comma 2 del decreto stesso.

Infine, la Società si è dotata di un Organismo di Vigilanza, come previsto dal Decreto 231/01. Il Decreto 231/01 contribuisce all'individuazione del perimetro oggettivo di applicazione del *whistleblowing,* prevedendo che siano oggetto di segnalazione all'Organismo di Vigilanza – ai sensi della presente Policy – anche eventuali violazione del Modello adottato dalla Società ai sensi di detto Decreto 231/01.

Le segnalazioni possono essere effettuate (in linea con l'ambito di applicazione soggettivo definito dall'art. 3 del decreto *whistleblowing*):

- da tutto il personale della Società, così come definito dall'articolo 1, comma 2, lettera cc) del D.Lgs. n. 231/2007 (oltreché dall'art. 1, comma 1, lett. i-*ter*) del TUF), ovvero "*i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione del soggetto obbligato, anche in forma diversa dal rapporto di lavoro subordinato, ivi compresi i consulenti finanziari abilitati all'offerta fuori sede di cui all'articolo 31, comma 2, del TUF nonché i produttori diretti e i soggetti*

[1] Con riferimento a tale ultima normativa la Società rientra nel perimetro soggettivo in quanto ricompresa nella definizione di "enti che operano in specifici settori" e "enti che hanno adottato il Modello organizzativo e di gestione ai sensi del D. Lgs. n. 231/2001", indipendentemente dalla media del numero di lavoratori dell'ultimo anno.

addetti all'intermediazione di cui all'articolo 109, comma 2, lettere c) ed e), CAP";

- da tutti coloro che vengono a conoscenza di violazioni nell'ambito del proprio contesto lavorativo, in qualità di dipendenti o collaboratori, lavoratori subordinati e autonomi, liberi professionisti ed altre categorie come volontari e tirocinanti, anche non retribuiti, gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;
- da soggetti terzi (ad esempio, fornitori), che abbiano conoscenza di violazioni nell'ambito dei rapporti con la Società.

Inoltre, le misure di protezione definite nella presente *Policy* si applicano anche:

- ai facilitatori (persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve rimanere);
- 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;
- 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;
- 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 predette persone.

La Società aggiorna almeno annualmente (ovvero ogniqualvolta si renda necessario) il perimetro dei soggetti che possono effettuare le segnalazioni. Qualora un nuovo soggetto rientri nel suddetto perimetro, la Società è tenuta a trasmettere allo stesso la presente Policy.

La presente Policy, ai sensi dell'art. 5 del Decreto whistleblowing, è pubblicata sul sito internet della Società https://firstance.com/it/ nella sezione dedicata.

Il Consiglio di Amministrazione approva i sistemi interni di segnalazione delle violazioni. È prevista la possibilità, nei casi indicati al successivo paragrafo "7. CANALE DI SEGNALAZIONE ESTERNO", di effettuare segnalazioni esterne, utilizzando il canale di segnalazione attivato dall'Autorità nazionale anticorruzione (di seguito anche "ANAC"), nonché, in ultima istanza, di effettuare una divulgazione pubblica.

4. NOMINA DEL RESPONSABILE DEI SISTEMI INTERNI DI SEGNALAZIONE

Conformemente con quanto previsto dalle disposizioni normative, la Società designa un Responsabile dei Sistemi Interni di Segnalazione (di seguito anche "*RSIS*"), con il compito di:

- assicurare il corretto funzionamento delle procedure;
- esaminare e valutare le segnalazioni ricevute;
- riferire direttamente e senza indugio al Collegio Sindacale le informazioni oggetto di segnalazione, ove rilevanti;
- riferire direttamente e senza indugio all'Organismo di Vigilanza le segnalazioni ricevute;

- redigere – nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali – una relazione annuale sul corretto funzionamento del sistema interno di segnalazione, contenente informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute. Tale relazione è sottoposta annualmente all'attenzione del Consiglio di Amministrazione;
- tenere un apposito registro delle segnalazioni.

Il Consiglio di Amministrazione del 6.12.2023 ha nominato la Dott.ssa Roberta Pulicati – Responsabile della Funzione Legale & Compliance – quale soggetto RSIS. Coerentemente con le previsioni normative e con il proprio modello organizzativo e operativo – alla luce del principio di proporzionalità – la Società ha ritenuto di attribuire al RSIS anche le attività di ricezione, nonché quelle di esame e valutazione delle segnalazioni. Tale attività di esame e di valutazione può essere effettuata da parte del RSIS anche con il supporto, se necessario, di personale qualificato anche esterno.

Qualora il RSIS sia il presunto responsabile della violazione o abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità di giudizio, le attività di ricezione, esame e valutazione delle segnalazioni saranno svolte dal Vice Responsabile dei Sistemi Interni di Segnalazione, Titolare della "*Funzione di riserva*", individuata dal Consiglio di Amministrazione nella medesima riunione del 6.12.2023 nella persona del Dott. Maurizio Fantoni, responsabile Funzione HR.

5. CONTENUTO E MODALITÀ DI SEGNALAZIONE

5.1. SEGNALAZIONI INTERNE DELLE VIOLAZIONI

Il segnalante (come meglio precisato nel precedente Paragrafo 3) deve fornire, fin ove possibile, gli elementi utili alla ricostruzione del fatto e ad accertare la fondatezza di quanto segnalato. La segnalazione deve contenere i seguenti elementi:

- generalità del soggetto segnalante, con indicazione dell'inquadramento e della qualifica professionale, sede di lavoro e recapiti, salva in ogni caso la possibilità di inserire una segnalazione anonima;
- luogo e data/periodo in cui si è verificato il fatto oggetto della segnalazione;
- descrizione chiara e completa dei fatti oggetto di segnalazione che possano costituire una violazione ai sensi di quanto precisato nel precedente Paragrafo 3;
- generalità o altri elementi che consentano di identificare il soggetto o i soggetti che hanno posto in essere i fatti segnalati;
- eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione ed eventuali documenti che possono confermare la fondatezza di tali fatti;
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati;
- dichiarazione del segnalante in merito all'assenza o alla sussistenza di un interesse privato collegato alla segnalazione.

È comunque indispensabile che i fatti siano di diretta conoscenza del segnalante e non siano stati riferiti da altri soggetti.

La segnalazione può essere effettuata in forma scritta oppure, su richiesta della persona segnalante, in forma

orale.

La segnalazione in forma scritta può essere effettuata dal segnalante, anche in totale anonimato, attraverso l'utilizzo di una piattaforma dedicata ("*Conduct Watch*"), utilizzata dalla Società in modalità *website*, alla quale si accede direttamente mediante il seguente *link* Firstance Speak Up (deloitte-halo.com).

La piattaforma garantisce, tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, del facilitatore, della persona coinvolta o comunque dei soggetti menzionati nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. Tale piattaforma permette quindi al RSIS (o la Funzione di riserva), così come ai membri dell'Organismo di Vigilanza, di venire immediatamente a conoscenza delle segnalazioni così ricevute ed avviare pertanto le dovute attività di verifica di propria competenza. Relativamente alle modalità di interazione con tale piattaforma, si rimanda a quanto riportato nella breve guida esplicativa di cui all'**Allegato A** della Policy.

La segnalazione in forma orale è possibile, su richiesta della persona segnalante, mediante un incontro diretto con il RSIS (o la Funzione di riserva) fissato entro **3 giorni lavorativi** della richiesta. La richiesta dovrà essere effettuata attraverso il seguente indirizzo email: whistleblowing@firstance.com. Per mantenere traccia dell'incontro i dati salienti della segnalazione, nel rispetto della procedura, saranno raccolti nel *format* allegato alla presente Policy (**Allegato B** della Policy) e archiviato a cura del RSIS (o la Funzione di riserva).

La segnalazione interna presentata ad un soggetto diverso da quello indicato è trasmessa, **entro sette giorni dal suo ricevimento**, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante.

In ogni caso dovrà essere garantita la riservatezza dei dati personali del segnalante, del facilitatore, della persona coinvolta o comunque dei soggetti menzionati nella segnalazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione. Al fine di tutelare la riservatezza di tali soggetti e la finalità stessa dell'indagine, le informazioni sulla loro identità potranno essere sottratte anche all'esercizio dei diritti previsti dalle disposizioni di legge europee e nazionali in materia di protezione dei dati personali che regolano l'accesso ai dati personali per tutte le fasi della procedura, salvo loro consenso o quando la conoscenza sia indispensabile per la difesa del segnalato. In ogni caso, anche qualora l'identità di tali soggetti dovesse essere rivelata, ad esempio perché essenziale per la difesa del segnalato, dovrà altresì essere sempre garantita la tutela adeguata di tali soggetti contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione, conformemente a quanto previsto dalla Legge 30 novembre 2017, n. 179 e successive modifiche ed integrazioni.

5.2 Segnalazioni all'Autorità di Vigilanza

Ai sensi dell'articolo Art. 10-quinquies del Codice delle Assicurazioni Private, il personale della Società invia all'IVASS segnalazioni riguardanti violazioni delle norme del Codice delle Assicurazioni Private, nonché di disposizioni dell'Unione europea direttamente applicabili.

5.3 Canale di segnalazione esterno

A norma dell'art. 6 del decreto *whistleblowing*, può essere effettuata una segnalazione esterna se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

a) non è prevista, nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo non è attivo o, anche se attivato, non è conforme all'art. 4 del decreto

whistleblowing;

b) la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
c) la persona segnalante 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) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Il canale per la segnalazione esterna attivato dall'ANAC, unico ente competente alla loro gestione (ad eccezione delle denunce alle Autorità giudiziarie), garantisce, tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

Nello specifico, ANAC rende disponibile su proprio portale la piattaforma di whistleblowing, accessibile all'indirizzo https://whistleblowing.anticorruzione.it raggiungibile anche attraverso il seguente link: https://www.anticorruzione.it/-/whistleblowing.

La segnalazione esterna viene acquisita da ANAC, oltre che mediante tale piattaforma, anche tramite segnalazioni orali o incontri diretti fissati entro un termine ragionevole.

La segnalazione esterna presentata ad un soggetto diverso dall'ANAC è trasmessa a quest'ultima, entro sette giorni dalla data del suo ricevimento, dando contestuale notizia della trasmissione alla persona segnalante.

Per maggiori dettagli si rimanda a quanto previsto all'interno delle Linee Guida ANAC, adottate con Delibera n. 311 del 12 luglio 2023 come eventualmente aggiornate ed integrate, e disponibili al seguente link https://www.anticorruzione.it/-/del.311.2023.linee.guida.whistleblowing.

6. PROCEDURA DI SEGNALAZIONI INTERNE

Ricevuta la segnalazione, per il tramite della piattaforma o per via orale, il RSIS (ovvero la "Funzione di riserva" qualora ricorrano i presupposti) comunica al segnalante, (attraverso la stessa modalità di ricezione della segnalazione) (i) entro 7 giorni dalla ricezione della segnalazione, l'avvenuta ricezione della medesima e (ii) entro 20 giorni dalla ricezione della segnalazione, l'avvio del procedimento di esame e dà inizio alla verifica della fondatezza o meno della segnalazione. Le indagini conseguenti alla segnalazione vengono svolte nel rispetto dei principi di minimizzazione e limitazione della finalità di cui al GDPR e potranno implicare lo svolgimento di indagini puntuali anche sugli strumenti utilizzati per lo svolgimento delle proprie mansioni quali, ad esempio, computer, rete internet, cellulari, ma anche attraverso la visione delle telecamere. Il RSIS (ovvero la "*Funzione di riserva*" qualora ricorrano i presupposti) è tenuto a mantenere, durante il processo di verifica della fondatezza della segnalazione, le interlocuzioni con il segnalante e ha facoltà di richiedere, ove necessario, integrazioni in merito alla segnalazione effettuata.

Il segnalato è informato dell'inizio delle indagini a suo carico mediante apposita comunicazione con relativa informativa sul trattamento dei dati personali (**Allegato C** della Policy) salvo che una simile informazione comprometta l'esito dell'indagine. È opportuno documentare simili valutazioni per le quali può essere richiesto il parere del responsabile funzione legale e compliance. Nel caso in cui si ritenga di non poter informare il segnalato prima dell'indagine, quest'ultimo è in ogni caso informato all'esito della verifica.

L'informativa di cui all'Allegato C sarà resa a tutti coloro che saranno coinvolti nell'indagine successiva alla segnalazione.

In ogni caso, all'esito di tale verifica:

- nel caso di infondatezza, il RSIS comunica al segnalante (attraverso la stessa modalità di ricezione della segnalazione) l'esito motivato e la conclusione del procedimento;
- qualora dall'esito della verifica, la segnalazione risulti fondata, il RSIS procede a informare (i) il segnalante circa l'esito positivo delle indagini, (ii) il segnalato tramite comunicazione separata, (iii) il Collegio Sindacale tramite apposita comunicazione.

Il presunto responsabile della violazione (segnalato) è tutelato da ripercussioni negative derivanti dalla segnalazione nel caso in cui dal procedimento di segnalazione non emergano elementi che giustifichino l'adozione di provvedimenti nei suoi confronti[2].

Nel corso del processo di analisi della segnalazione, il RSIS effettua la valutazione della segnalazione in termini di rilevanza e gravità della stessa e procede ad informare il segnalante (attraverso la stessa modalità di ricezione della segnalazione) e il segnalato (tramite comunicazione separata) dando conferma, ove possibile, del ricevimento della segnalazione e fornendo indicazioni circa gli sviluppi del procedimento e gli esiti della valutazione stessa. Nel caso in cui si siano verificate violazioni gravi, il RSIS informa tempestivamente il Consiglio di Amministrazione ed il Collegio Sindacale affinché valutino l'eventuale adozione di provvedimenti decisionali e disciplinari di rispettiva competenza.

In qualunque fase del procedimento – e senza attendere l'esito della valutazione – il RSIS riferisce direttamente e senza indugio le informazioni rilevanti oggetto della segnalazione agli Organi Aziendali che provvedono ad adottare i relativi provvedimenti, anche d'urgenza, ove risulti necessario, ivi incluso, se del caso, informativa al Responsabile della Funzione Antiriciclaggio qualora ricorrano i presupposti per la predisposizione di una segnalazione di operazione sospetta. Qualora oggetto della segnalazione sia il medesimo RSIS e la segnalazione venga ritenuta fondata e rilevante, l'informativa tempestiva agli Organi Aziendali dovrà essere fornita direttamente dalla Funzione di riserva.

Nel caso in cui il segnalante sia corresponsabile della violazione oggetto di segnalazione, la Società può prevedere un trattamento privilegiato nei suoi confronti rispetto agli altri corresponsabili, salvi i casi in cui la condotta del segnalante risulti di particolare gravità.

Il processo sin qui descritto deve essere concluso nel più breve tempo possibile, secondo criteri che tengano conto della gravità della violazione, al fine di prevenire che il perdurare delle violazioni produca ulteriori aggravamenti per la Società. In ogni caso, la procedura deve concludersi **entro 3 mesi dalla ricezione della segnalazione**, salvo casi eccezionali e opportunamente motivati in cui l'esame e la valutazione della segnalazione possa estendersi fino a 4 mesi, previa comunicazione al Collegio Sindacale.

7. DIVULGAZIONI PUBBLICHE

L'art. 15 del decreto whistleblowing prevede come ultima istanza la possibilità di divulgazione pubblica della

[2] In caso di adozione di provvedimenti nei confronti del responsabile della violazione, costui dovrà essere tutelato da eventuali effetti negativi diversi da quelli previsti dai provvedimenti adottati

segnalazione, che può essere effettuata esclusivamente qualora ricorra 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 dagli articoli 4 e 7 del decreto whistleblowing (si veda paragrafo 5.3 della presente procedura) e non è stato dato riscontro nei termini previsti dagli articoli 5 e 8 del decreto whistleblowing 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.

8. FORME DI TUTELA DEL SEGNALANTE E DEGLI ALTRI SOGGETTI COINVOLTI

8.1. TUTELA DELL'ANONIMATO

Al fine di evitare che il timore di subire conseguenze pregiudizievoli possa indurre a non segnalare le violazioni, l'identità del segnalante non può essere rivelata, salvo il suo espresso e libero consenso, e tutti coloro che sono coinvolti nella gestione della segnalazione, sono tenuti a tutelare la riservatezza di tale informazione.

Fanno eccezione le ipotesi in cui sia configurabile in capo al segnalante una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del Codice Penale o ai sensi dell'articolo 2043 del Codice Civile, nonché le ipotesi in cui l'anonimato non sia opponibile per legge.

L'anonimato del segnalante è altresì garantito nell'ambito del procedimento disciplinare quando la contestazione al segnalato sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. L'identità del segnalante può invece essere rivelata al soggetto segnalato, con il consenso del segnalante, ovvero quando la contestazione sia basata principalmente sulla segnalazione e pertanto la conoscenza dell'identità è assolutamente indispensabile in sede penale per la difesa del segnalato.

Quando richiesto dal segnalante, le informazioni oggetto di segnalazione sono portate a conoscenza degli Organi Aziendali assicurando l'anonimato del segnalante.

La violazione dell'obbligo di riservatezza, inclusa la divulgazione di informazioni in base a cui l'identità del segnalante si possa dedurre, è considerata una violazione della presente policy ed è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

8.2 COMPORTAMENTI ED ATTI RITORSIVI

Il personale che effettua una segnalazione ai sensi della presente policy non può essere sanzionato, licenziato (salvo i casi di corresponsabilità accertata) o sottoposto ad alcuna misura discriminatoria e/o ad atti ritorsivi avente effetti sulle condizioni di lavoro per motivi collegati alla segnalazione (fermo restando quanto previsto nel successivo Paragrafo 9). Il licenziamento ritorsivo o discriminatorio del segnalante è nullo e sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del Codice Civile, nonché qualsiasi altra misura ritorsiva o

discriminatoria adottata nei confronti del segnalante. Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili.

In ottemperanza all'art. 17 del decreto *whistleblowing* sono considerati comportamenti/atti ritorsivi, pertanto vietati dalla Società:

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) 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;

m) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;

n) l'annullamento di una licenza o di un permesso;

o) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, a demansionamenti, licenziamenti, trasferimenti o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure siano fondate su ragioni estranee alla segnalazione stessa.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato Nazionale del Lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Nei casi più gravi, e qualora sia possibile, la Società può valutare di disporre il trasferimento per incompatibilità ambientale del segnalante, previo consenso del medesimo.

Il personale che ritiene di aver subito una discriminazione ne dà notizia circostanziata al RSIS che, accertata

la fondatezza, segnala la casistica agli Organi Aziendali competenti, affinché siano adottati i provvedimenti necessari a ripristinare la situazione e/o rimediare agli effetti negativi della discriminazione.

È altresì vietata ogni forma di ritorsione o discriminazione avente effetti sulle condizioni di lavoro di chi collabora alle attività di riscontro della fondatezza della segnalazione.

Le suddette misure di protezione, ai sensi del decreto *whistleblowing*, si estendono, oltre che al segnalante, anche ai seguenti soggetti:

a) al facilitatore (persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve rimanere);

b) alle persone del medesimo contesto lavorativo della persona 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;

c) ai colleghi di lavoro della persona 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 con detta persona un rapporto abituale e corrente;

d) agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

L'ANAC applica al responsabile le sanzioni amministrative pecuniarie previste dall'art.21, comma 1, del decreto whistleblowing, nei casi ivi previsti ai quali si rimanda per maggiori dettagli.

9. RESPONSABILITÀ DEL SEGNALANTE

La presente *Policy* lascia impregiudicata la responsabilità penale e disciplinare del segnalante, nell'ipotesi di segnalazione calunniosa e diffamatoria ai sensi del Codice Penale o ai sensi dell'articolo 2043 del Codice Civile.

Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente *Policy*, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il segnalato e/o altri soggetti, ed ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente *Policy*.

10. PROTEZIONE DEI DATI E ARCHIVIAZIONE DEI DOCUMENTI

Al fine di assicurare la ricostruzione delle diverse fasi del processo di segnalazione, è cura del RSIS (ovvero della Funzione di Riserva, per le segnalazioni a lui pervenute) garantire:

- la tracciabilità delle segnalazioni e delle relative attività istruttorie;
- la conservazione della documentazione inerente le segnalazioni e le relative attività di verifica, in appositi archivi (cartacei/informatici);
- la conservazione della documentazione e delle segnalazioni per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati e comunque (i) nel rispetto delle procedure *privacy* vigenti e (ii) non oltre 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Le funzioni competenti archiviano la documentazione inerente al processo sanzionatorio e disciplinare.

È tutelato, ai sensi della normativa vigente e delle procedure aziendali in materia di privacy, il trattamento dei dati personali delle persone coinvolte e/o citate nelle segnalazioni. A tal riguardo si fa presente che per il segnalante è disponibile, al momento della segnalazione, apposita informativa sul trattamento dei dati personali (**Allegato D** alla Policy).

ALLEGATO A - Guida esplicativa modalità della segnalazione sulla Piattaforma

Conduct Watch

Conduct Watch - Whistleblowing

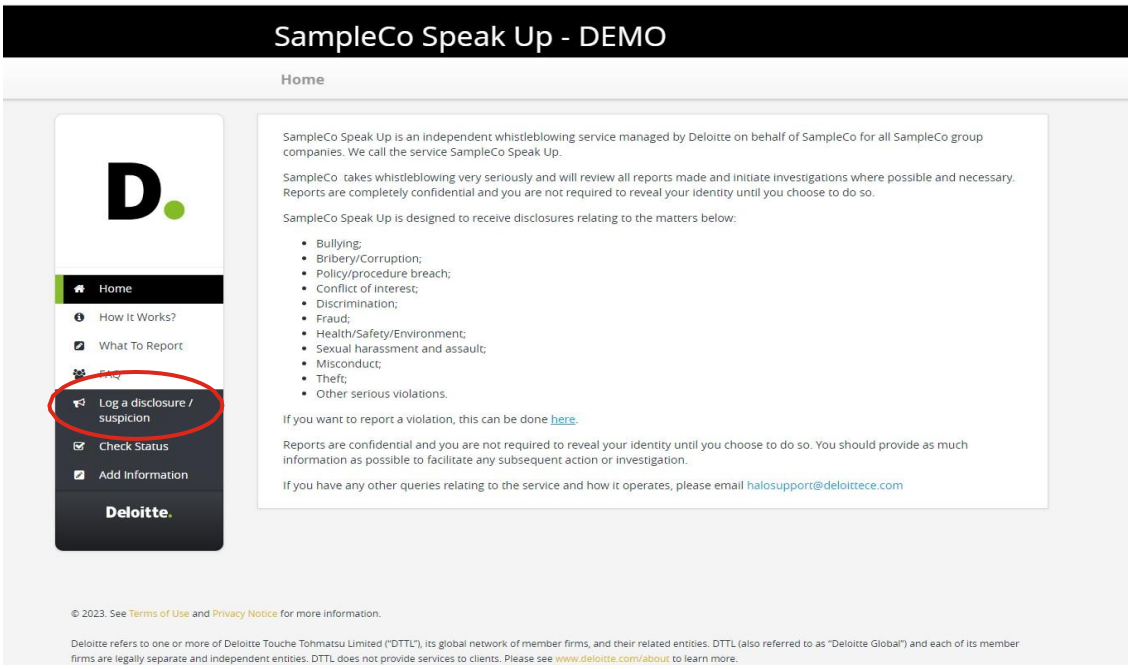
Si riporta di seguito una panoramica delle funzioni previste dal portale dedicato alla gestione delle segnalazioni Whistleblowing.

Gli *screenshot* riportati sono tratti dalla versione "demo" della piattaforma, non già personalizzata secondo le esigenze specifiche del cliente, e a sono da intendersi, così come le descrizioni riportate, puramente indicative.

Indice

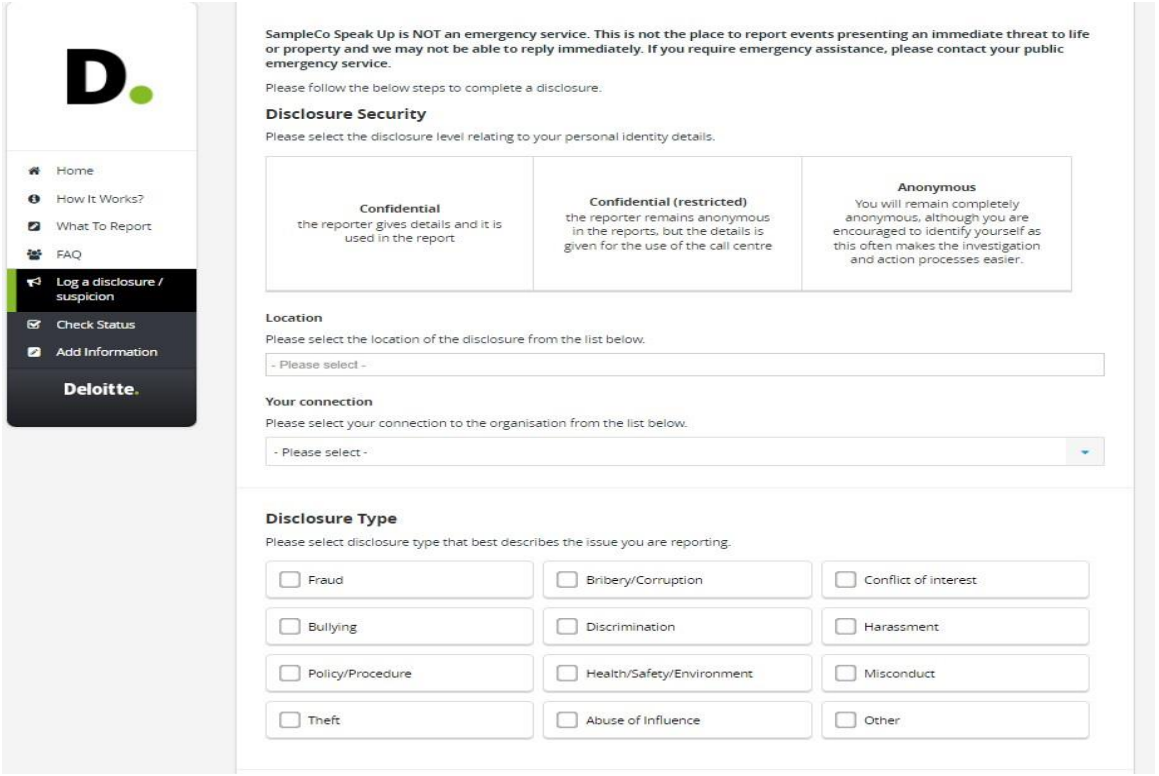
1. Inserimento segnalazione

Per inserire una nuova segnalazione, partendo dalla home page, è sufficiente cliccare sul link "*Log a disclosure / suspicion*", evidenziato in rosso nell'immagine sotto riportata.



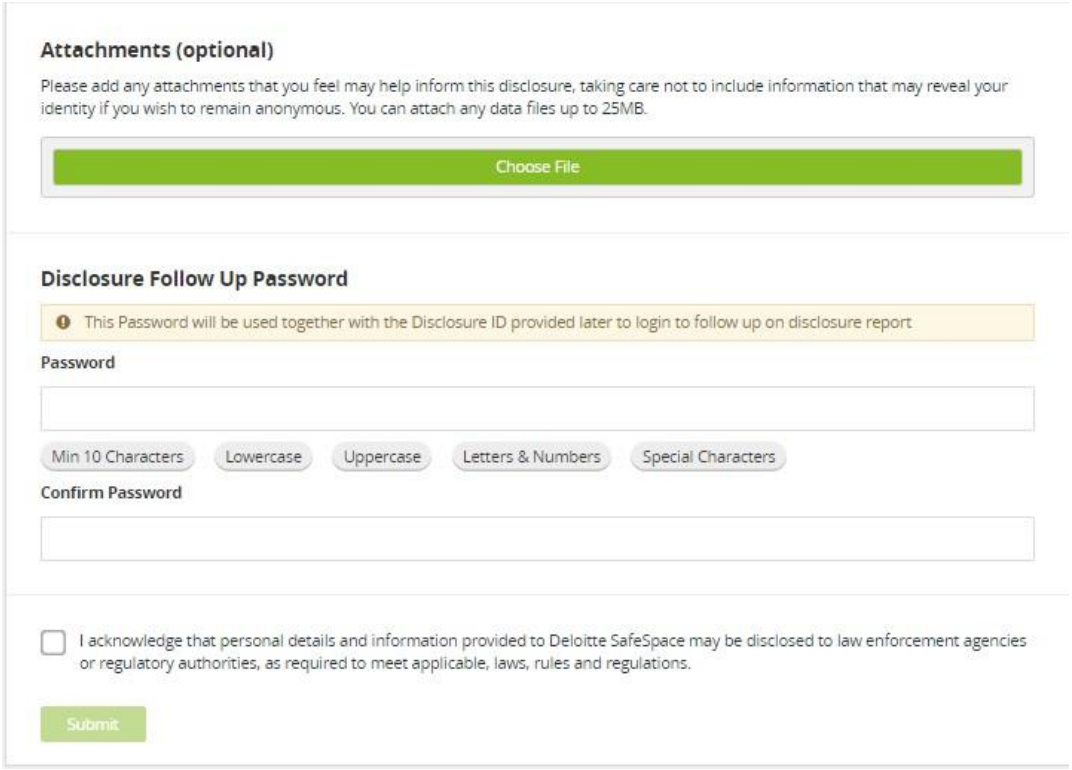
La pagina per l'inserimento della segnalazione consiste in un *form* all'interno del quale il segnalante può inserire tutti i dettagli dell'accadimento che intende riportare de quale è a conoscenza.

Il segnalante può decidere il livello di anonimato dei propri dati personali (1. confidenziale, decidendo di fornire tutti i propri dati personali e di contatto, 2. Parzialmente confidenziale, decidendo di fornire i dati personali ma ai soli fini della gestione della segnalazione, senza dare *disclosure* alla Società, 3. completamente anonimo).

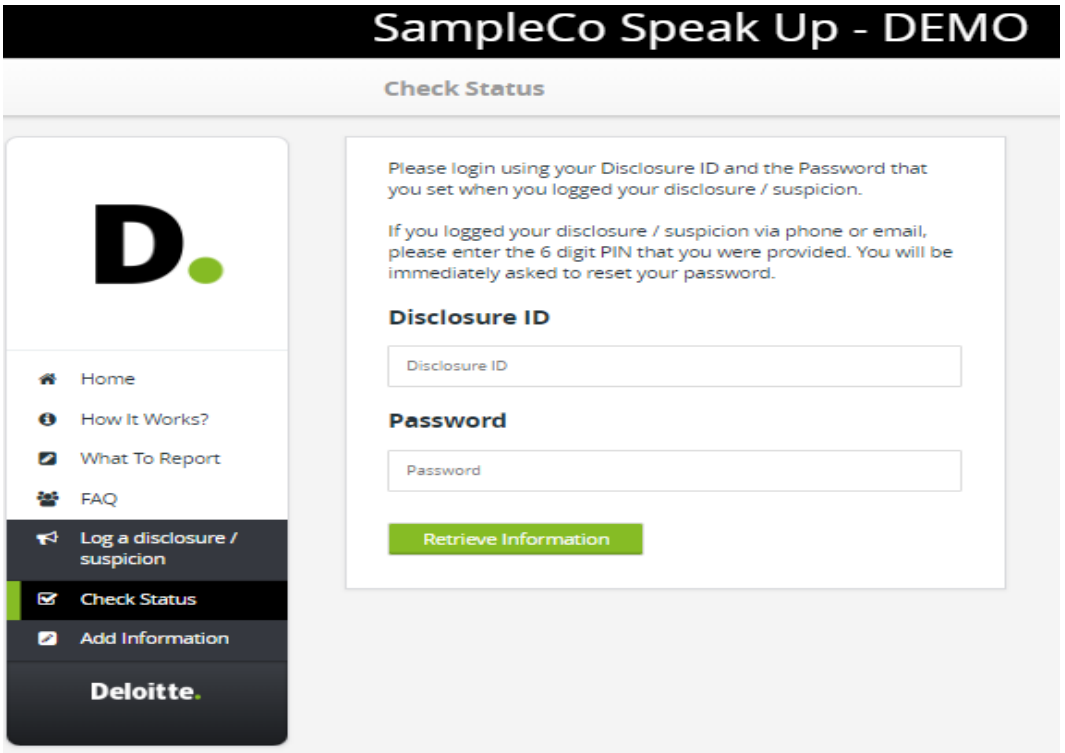


Oltre a tutte le informazioni testuali, il segnalante può allegare documentazione a supporto della segnalazione.

Infine, viene richiesto al segnalante l'inserimento di una *password* che, insieme al codice della segnalazione che verrà successivamente fornito dalla piattaforma, permetterà al segnalante di accedere anche in un secondo momento alla piattaforma per verificare l'avanzamento della lavorazione della segnalazione stessa ovvero fornire eventuali ulteriori nuovi dettagli.

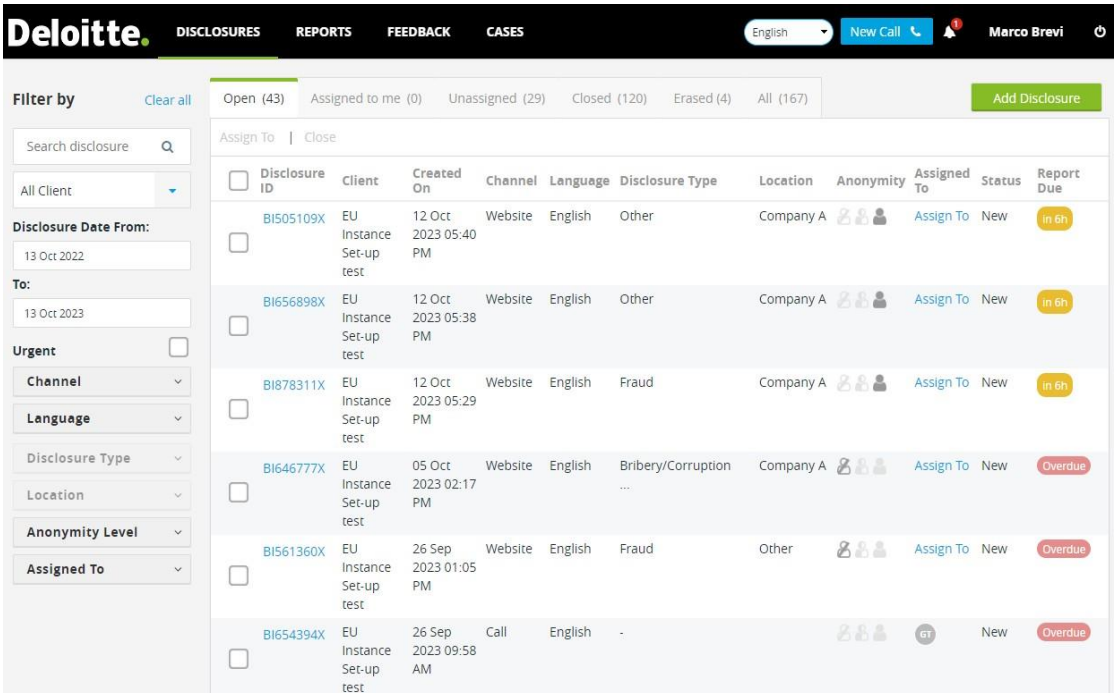


Il segnalante, per accedere nuovamente alla segnalazione, dovrà utilizzare la funzione "*check status*" e inserire il codice della segnalazione e la *password* impostata.

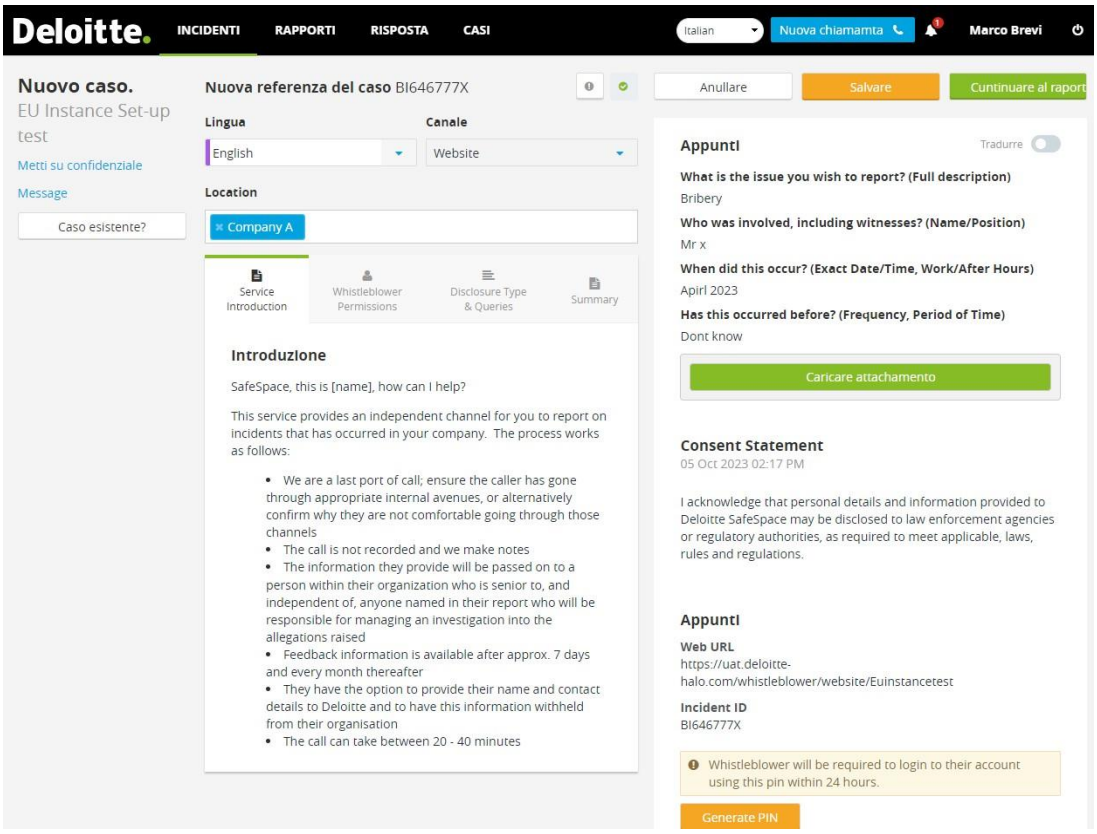


2. Gestione segnalazione

La seguente rappresentazione grafica riporta la schermata rivolta al gestore della segnalazione, in cui vengono dettagliate le segnalazioni inserite, suddivise per stato di avanzamento della lavorazione (aperta, assegnata, da assegnare, chiusa, ecc.). È possibile utilizzare una serie di filtri pre-impostati per effettuare ricerche negli elenchi.



Per ciascuna segnalazione, sono riportate le informazioni principali e un *link* per accedere al dettaglio.



3. Reportistica

Una sezione apposita della piattaforma Conduct Watch permette di visualizzare una *dashboard* ai fini di reportistica.

Il grafico riportato può essere filtrato o dettagliato secondo diversi campi (tipo di segnalazione, status, canale, *location*, ecc.).

	Jan-2019	Feb-2019	Mar-2019	Apr-2019	May-2019	Jun-2019	Jul-2019	Aug-2019	Sep-2019	Oct-2019	Nov-2019	Dec-2019
No. of Cases	1	1	2	1	2	1	3	-	-	-	1	-
Total Breakdown	1	1	2	1	2	1	3	-	-	-	1	-
EU Instance Set-up test	1	1	2	1	2	1	3	-	-	-	1	-

ALLEGATO B – Modello per la raccolta delle evidenze di eventuali segnalazioni interne orali effettuate mediante incontro diretto con il RSIS (o la Funzione di riserva)

Nome e cognome del segnalante	
Inquadramento e qualifica professionale	
Sede di lavoro	
Recapiti	
Luogo in cui si è verificato il fatto	
Data/periodo in cui si è verificato il fatto	
Descrizione dei fatti oggetto di segnalazione	
Nome/i e cognome/i del/dei soggetto/i segnalato/i	
Nome/i e cognome/i del/dei soggetto/i a conoscenza dei fatti oggetto di segnalazione (eventuale)	
Ulteriori informazioni che possono fornire utile riscontro circa la sussistenza dei fatti oggetto di segnalazione (eventuale)	
Allegati pertinenti (eventuali)	

ALLEGATO C – Informativa sul trattamento dei dati personali per il segnalato

*Ai sensi del Regolamento (UE) 2016/679 ("**GDPR**"), Firstance S.r.l. fornisce la presente informativa sul trattamento dei dati personali acquisiti in relazione alle segnalazioni di irregolarità descritte nella policy di Whistleblowing adottata al fine di regolamentarne la gestione.*

In particolare, le seguenti informazioni sono rese ai fini di trasparenza nei confronti di chi sia stato oggetto di segnalazione o comunque sia stato nominato all'interno di una procedura di whistleblowing per metterlo al corrente del trattamento dei dati nel contesto della suddetta procedura

---

1. Titolare del trattamento e DPO

Il titolare del trattamento è Firstance S.r.l. ("**Firstance**", "**Titolare**" o "**Società**"), con sede legale in Viale Certosa 2 - 20155, Milano, iscritta al Registro Unico degli Intermediari Assicurativi al n. B000350474, C.F. e P.IVA. n. 07095610965, email: info@firstance.com e PEC: firstance@legalmail.it

2. Dati personali trattati

Firstance tratterà i seguenti dati personali del segnalato indicati nella segnalazione e altri che la società raccoglie nel corso delle indagini scaturenti dalla segnalazione.

Se le segnalazioni contengono dati sensibili o giudiziari, riferiti al segnalato o a terzi, Firstance, salvo verifica della necessità di acquisizione dei detti dati ai fini della gestione della segnalazione, provvede a distruggerli, fatti salvi i casi autorizzati dalla legge o da un provvedimento dell'Autorità Garante per la protezione dei dati personali.
Con particolare riguardo ai dati che il Titolare dovesse ricevere attraverso le segnalazioni, si precisa che il relativo trattamento avviene in scrupolosa osservanza del principio di minimizzazione e che, ai sensi dell'art. 13, co. 2, del D.lgs. 24/2023, "i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente".
Inoltre, qualora venissero svolte indagini, potrebbero essere raccolti ulteriori dati personali che riguardano il Segnalato, in particolare con riguardo al suo utilizzo della strumentazione informatica del Titolare, inclusa la posta elettronica e l'utilizzo di altri strumenti di messaggistica aziendali.
I dati raccolti potranno essere trattati per tutti i fini connessi al rapporto di lavoro.
Nel caso in cui le venga chiesto la comunicazione di dati e informazioni al Titolare nel contesto delle indagini interne, le ricordiamo che collaborare è parte dei suoi doveri di lavoratore e che un suo eventuale rifiuto sarebbe quindi illegittimo e potrebbe dare luogo a conseguenze anche sul piano disciplinare.

3. Finalità e base giuridica del trattamento

I dati personali sono raccolti e trattati, tramite una piattaforma dedicata, per le finalità strettamente connesse alla gestione delle segnalazioni di condotte illecite e secondo le logiche previste dalla policy di Whistleblowing.

La base giuridica del trattamento è la necessità di adempiere a un obbligo di legge cui è soggetto il Titolare, con riferimento alle previsioni contenute nel D.lgs. n. 24/2023 recante attuazione della Direttiva (UE) 2019/1937, nonché alle linee guida ANAC in materia. Inoltre, potrebbe essere necessario trattare i dati anche per accertare, esercitare o difendere un proprio diritto in sede giudiziaria, ai sensi dell'art. 9, co. 2 lett. f) GDPR e dell'art. 6 lett. f) GDPR.

4. Tempi di conservazione

Le segnalazioni e la relativa documentazione relativa saranno conservate per il tempo strettamente necessario alla gestione delle stesse e, eventualmente, alle successive azioni che debbano essere intraprese, anche a livello di tutela in giudiziaria o comunque legale del Titolare.

Salvo esigenze di tutela dei diritti in sede giudiziaria, i dati verranno eliminati o resi anonimi dopo 5 anni dalla chiusura della segnalazione.

5. Ambito di circolazione dei dati personali

Il trattamento dei dati personali per le finalità sopra illustrate sarà effettuato dal personale interno di Firstance appositamente incaricato dello svolgimento delle mansioni connesse alla ricezione delle segnalazioni e della gestione della eventuale conseguente istruttoria.

Inoltre, i dati personali potranno essere comunicati, esclusivamente per le finalità sopraindicate, anche ai seguenti soggetti:

a) Soggetti quali società esterne o professionisti che aiutano il Titolare nella gestione della segnalazione e delle sue conseguenze che trattano i dati personali per le finalità sopra illustrate per conto di Firstance, appositamente nominati responsabili del trattamento ai sensi dell'art. 28 GDPR (ad esempio, fornitori di servizi IT);
b) soggetti pubblici o privati (ad esempio, assicurazioni, banche, consulenti legali, pubbliche autorità, organi giudiziari, agenzia delle entrate), che tratteranno i dati personali in qualità di autonomi titolari del trattamento.

6. Trasferimento dei dati personali al di fuori dello Spazio Economico Europeo

Non è previsto il trasferimento dei dati personali verso Paesi non appartenenti allo Spazio Economico Europeo ("**SEE**") o verso organizzazioni internazionali.

Qualora tale trasferimento dovesse rendersi necessario, saranno messe in atto le misure previste dal GDPR, previo aggiornamento anche della presente informativa.

7. Diritti degli interessati

Ai sensi degli artt. 15-22 GDPR, gli interessati possono rivolgersi al Titolare per esercitare specifici diritti quali:

- **Diritto di accesso**: diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali e, in tal caso, di ottenere l'accesso ai dati personali e ad ulteriori informazioni su origine, finalità, categoria di dati trattati, destinatari di comunicazione e/o trasferimento dei dati, etc;
- **Diritto di rettifica**: diritto di ottenere dal Titolare la rettifica dei dati personali inesatti senza ingiustificato ritardo, nonché l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- **Diritto alla cancellazione**: diritto di ottenere dal Titolare la cancellazione dei dati personali senza ingiustificato ritardo nel caso in cui:
  - i dati personali non sono più necessari rispetto alle finalità deltrattamento;
  - il consenso su cui si basa il trattamento è revocato e non sussiste altro fondamento

giuridico per il trattamento;

- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

- **Diritto di opposizione al trattamento**: diritto di opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al trattamento dei dati personali di cui all'art. 6, co. 1, lett. e) o f), GDPR, compresa la profilazione sulla base di tali disposizioni;
- **Diritto di limitazione di trattamento**: diritto di ottenere dal Titolare la limitazione del trattamento, nei casi in cui sia contestata l'esattezza dei dati personali (per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali), se il trattamento è illecito e/o l'interessato si è opposto al trattamento;
- **Diritto alla portabilità dei dati**: diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali e di trasmettere tali dati ad altro titolare del trattamento, solo per i casi in cui il trattamento sia basato sul consenso e per i soli dati trattati tramite strumenti elettronici.

Si ricorda tuttavia che, in ragione della normativa applicabile (in particolare art. 23 GDPR e art. 2-undecies D.lgs. 196/2003 – Codice Privacy), tali diritti potrebbero non trovare applicazione nel caso concreto, in particolare qualora dall'esercizio degli stessi possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante.

In particolare, l'esercizio di tali diritti potrà essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare la riservatezza dell'identità del segnalante.

L'interessato ha inoltre il diritto di proporre reclamo a un'autorità di controllo. In particolare, fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il GDPR ha il diritto di proporre reclamo all'autorità di controllo dello Stato membro in cui risiede o lavora abitualmente, ovvero dello Stato in cui si è verificata la presunta violazione. Per l'Italia, l'Autorità competente è il Garante per la Protezione dei Dati Personali.

ALLEGATO D – Informativa sul trattamento dei dati personali per il segnalante

*Ai sensi del Regolamento (UE) 2016/679 ("**GDPR**"), Firstance S.r.l. fornisce la presente informativa sul trattamento dei dati personali acquisiti in relazione alle segnalazioni di irregolarità descritte nella policy di Whistleblowing adottata al fine di regolamentarne la gestione.*

In particolare, le seguenti informazioni sono rese agli interessati che vogliano effettuare segnalazioni all'interno di una procedura di whistleblowing.

---

1. Titolare del trattamento e DPO

Il titolare del trattamento è Firstance S.r.l. ("**Firstance**", "**Titolare**" o "**Società**"), con sede legale in Viale Certosa 2 - 20155, Milano, iscritta al Registro Unico degli Intermediari Assicurativi al n. B000350474, C.F. e P.IVA. n. 07095610965, email: info@firstance.com e PEC: firstance@legalmail.it

2. Dati personali trattati

Firstance tratterà i seguenti dati personali degli utenti:

a) **dati anagrafici** (nome, cognome);

b) **dati identificativi** (dipartimento);

c) **dati di contatto** (e-mail, contatti telefonici);

d) **dati relativi al momento in cui viene effettuata la segnalazione**;

e) **eventuali dati particolari**.

I dati personali vengono acquisiti solo nel caso in cui l'interessato scelga di effettuare la segnalazione in forma non anonima. In caso contrario non ci sarà nessuna conservazione dei dettagli del segnalatore. La riservatezza del segnalante è tutelata come da previsione normative per cui a eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del Codice penale o dell'art. 2043 del Codice civile e delle ipotesi in cui la riservatezza non è opponibile per legge (es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del segnalante verrà protetta sin dalla ricezione della segnalazione e in ogni fase successiva.
Se le segnalazioni contengono dati sensibili o giudiziari, riferiti al segnalante o a terzi, Firstance, salvo verifica della necessità di acquisizione dei detti dati ai fini della gestione della segnalazione, provvede a distruggerli, fatti salvi i casi autorizzati dalla legge o da un provvedimento dell'Autorità Garante per la protezione dei dati personali.

3. Finalità e base giuridica del trattamento

I dati personali sono raccolti e trattati, tramite una piattaforma dedicata, per le finalità strettamente connesse alla gestione delle segnalazioni di condotte illecite e secondo le logiche previste dalla policy di Whistleblowing.

La base giuridica del trattamento è la necessità di adempiere a un obbligo di legge cui è soggetto il Titolare, con riferimento alle previsioni contenute nel D.lgs. n. 24/2023 recante attuazione della Direttiva (UE) 2019/1937, nonché alle linee guida ANAC in materia. Inoltre, potrebbe essere necessario trattare i dati anche per accertare, esercitare o difendere un proprio diritto in sede giudiziaria, ai sensi dell'art. 9, co. 2 lett. f) GDPR e dell'art. 6 lett. f) GDPR.

4. Tempi di conservazione

Le segnalazioni e la relativa documentazione relativa saranno conservate per il tempo necessario alla gestione delle stesse e, eventualmente, alle successive azioni che debbano essere intraprese, anche a livello di tutela in giudiziaria o comunque legale del Titolare.

Salvo esigenze di tutela dei diritti in sede giudiziaria, i dati verranno eliminati dopo 5 anni dalla chiusura della segnalazione.

5. Ambito di circolazione dei dati personali

Il trattamento dei dati personali per le finalità sopra illustrate sarà effettuato dal personale interno di Firstance appositamente incaricato dello svolgimento delle mansioni connesse alla ricezione delle segnalazioni e della gestione della eventuale conseguente istruttoria. Inoltre, i dati personali potranno essere comunicati anche ai seguenti soggetti:

c) soggetti quali società esterne o professionisti che aiutano il Titolare nella gestione della segnalazione e delle sue conseguenze che trattano i dati personali per le finalità sopra illustrate conto di Firstance, appositamente nominati responsabili del trattamento ai sensi dell'art. 28 GDPR (ad esempio, fornitori di servizi IT);
d) soggetti pubblici o privati (ad esempio, assicurazioni, banche, consulenti legali, pubbliche autorità, organi giudiziari, agenzia delle entrate), che tratteranno i dati personali in qualità di autonomi titolari del trattamento.

6. Trasferimento dei dati personali al di fuori dello Spazio Economico Europeo

Non è previsto il trasferimento dei dati personali verso Paesi non appartenenti allo Spazio Economico Europeo ("**SEE**") o verso organizzazioni internazionali.

Qualora tale trasferimento dovesse rendersi necessario, saranno messe in atto le misure previste dal GDPR, previo aggiornamento anche della presente informativa.

7. Diritti degli interessati

Ai sensi degli artt. 15-22 GDPR, gli interessati possono rivolgersi al Titolare per esercitare specifici diritti quali:

- **Diritto di accesso**: diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali e, in tal caso, di ottenere l'accesso ai dati personali e ad ulteriori informazioni su origine, finalità, categoria di dati trattati, destinatari di comunicazione e/o trasferimento dei dati, etc;
- **Diritto di rettifica**: diritto di ottenere dal Titolare la rettifica dei dati personali inesatti senza ingiustificato ritardo, nonché l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- **Diritto alla cancellazione**: diritto di ottenere dal Titolare la cancellazione dei dati personali senza ingiustificato ritardo nel caso in cui:
  - i dati personali non sono più necessari rispetto alle finalità deltrattamento;
  - il consenso su cui si basa il trattamento è revocato e non sussiste altro fondamento giuridico per il trattamento;

- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

❖ **Diritto di opposizione al trattamento**: diritto di opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al trattamento dei dati personali di cui all'art. 6, co. 1, lett. e) o f), GDPR, compresa la profilazione sulla base di tali disposizioni;

❖ **Diritto di limitazione di trattamento**: diritto di ottenere dal Titolare la limitazione del trattamento, nei casi in cui sia contestata l'esattezza dei dati personali (per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali), se il trattamento è illecito e/o l'interessato si è opposto al trattamento;

❖ **Diritto alla portabilità dei dati**: diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali e di trasmettere tali dati ad altro titolare del trattamento, solo per i casi in cui il trattamento sia basato sul consenso e per i soli dati trattati tramite strumenti elettronici.

Si ricorda tuttavia che, in ragione della normativa applicabile (in particolare art. 23 GDPR e art. 2-undecies D.lgs. 196/2003 – Codice Privacy), tali diritti potrebbero non trovare applicazione nel caso concreto, in particolare qualora dall'esercizio degli stessi possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante.

In particolare, l'esercizio di tali diritti potrà essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare la riservatezza dell'identità del segnalante.

L'interessato ha inoltre il diritto di proporre reclamo a un'autorità di controllo. In particolare, fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il GDPR ha il diritto di proporre reclamo all'autorità di controllo dello Stato membro in cui risiede o lavora abitualmente, ovvero dello Stato in cui si è verificata la presunta violazione. Per l'Italia, l'Autorità competente è il Garante per la Protezione dei Dati Personali.