Whistleblowing Policy

Versione n. 1/2023 emessa in data 05.12.2023

Sommario

Glossario

Premessa

1. Ambito di applicazione e quadro normativo di riferimento
2. Chi può fare la segnalazione?
3. Come si può inviare una segnalazione?
4. Il canale interno: ReBlowing
5. Caratteristiche tecniche del canale interno: ReBlowing
6. Guida all'utilizzo di ReBlowing (canale interno)
7. Titolare: iter di registrazione sul Portale ReBlowing
8. Procedura di gestione delle segnalazioni
9. Protezione dei dati personali
10. Provvedimenti sanzionatori

Aggiornamento

**Nel presente documento, l'uso del genere maschile per indicare i soggetti, gli incarichi e gli stati giuridici è utilizzato solo per esigenze di semplicità del testo ed è da intendersi riferito a entrambi i generi.*

Glossario

Archivio: (definizione ai sensi del Regolamento UE 2016/679, d'ora in poi "GDPR") qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Autorità Garante per la Protezione dei Dati Personali: (di seguito, per brevità, GPDP) (ai sensi del GDPR) autorità amministrativa indipendente istituita dalla L. 31 dicembre 1996, n. 675, poi disciplinata dal Codice Privacy (D.lg. 30 giugno 2003 n. 196), come modificato dal D.lgs 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il

GPDP è l'autorità di controllo nazionale, designata ai fini dell'attuazione dell'art. 51 del Regolamento (UE) 2016/679.

Dato personale: (ai sensi del GDPR) qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato/a); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Informazioni riservate: tutte le informazioni acquisite dall'Utente, che non siano di pubblico dominio, fornite per iscritto, in formato elettronico o in qualsiasi altra forma e/o supporto.

Trattamento di dati personali: : (ai sensi del GDPR) qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Violazioni: Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato.

Informazioni sulle violazioni: informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico ai sensi dell'articolo 3, comma 1 o 2, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.

Tipologie di segnalazioni:

- «segnalazione interna»: la comunicazione scritta od orale di informazioni sulle violazioni, presentata tramite il canale di segnalazione interno;
- «segnalazione esterna»: la comunicazione scritta od orale di informazioni sulle violazioni presentata tramite il canale di segnalazione esterno;
- «divulgazione pubblica» o «divulgare pubblicamente»: il fatto di rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

Persona segnalante: (o Whistleblower) la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo.

Persona coinvolta: La persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.

Contesto lavorativo: attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile.

Ritorsione: Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

Riscontro: Comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione.

Seguito: L'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate.

Soggetto esterno: ReNorm S.r.l. debitamente incaricata in qualità di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679 – GDPR nell'ambito della gestione del canale interno di segnalazione scelto dal Titolare.

Autorità competente: L'autorità nazionale designata a ricevere le segnalazioni conformemente al capo III e a dare un riscontro alla persona segnalante e/o designata per svolgere le funzioni previste dalla presente direttiva, in parti- colare per quanto riguarda il seguito dato alle segnalazioni.

Premessa

La presente Procedura si pone l'obiettivo di definire l'ambito di applicazione, le modalità e le norme applicabili all'istituto del Whistleblowing. La Società rientra nell'ambito di applicazione del D.Lgs. n. 24 del 10 marzo 2023 (G.U. n. 63 del 15 marzo 2023) in quanto si tratta di:

- Pubblica amministrazione
- Ente pubblico economico
- Società in House
- Società a controllo pubblico
- Concessionario di pubblico servizio
- Organismo di diritto pubblico

- ha impiegato nell'ultimo anno la media di almeno 50 lavoratori subordinati
- ha adottato un Modello Organizzativo e Gestione 231
- operante nei c.d. "settori sensibili"

Settore
pubblico

Settore
Privato

Con il termine whistleblowing si intende l'attività di segnalazione di illeciti o irregolarità che un soggetto interessato (c.d. segnalante o whistleblower) riscontra nel settore pubblico o privato ovvero in un'azienda pubblica, privata o mista. L'origine di questo termine è giuridicamente indeterminata. Tuttavia, la dottrina attribuisce il concetto all'azione dell'arbitro che fischia per segnalare un fallo e, più specificatamente, ai poliziotti inglesi che utilizzavano il fischietto appunto per "dare l'allarme".

La disciplina di questo fenomeno ha origini storiche alquanto datate. Si tratta di un'istituzione "inventata" sulla base di numerosi principi giuridici ancora usati ai giorni nostri, dai nostri avi molti secoli prima degli scandali finanziari moderni e della Direttiva (UE) del 2019. L'Avv. M. Rubini nell'articolo "La disciplina del Whistleblowing: dalle origini ai giorni nostri" (pubblicato sulla rivista Risk&Compliance) racconta che "nell'antica Roma, infatti, quello del delatore era un vero e proprio mestiere, ricompensato per le segnalazioni dei crimini o di beni sottratti al fisco".

I primi interventi in materia di whistleblowing risalgono all'epoca della Comunità Economica Europea e sono stati introdotti al fine di contrastare il riciclaggio dei proventi derivanti dal traffico di stupefacenti (Direttiva (CE) 10 giugno 1991, n. 91/308). Nello specifico, furono le banche e gli enti finanziari ad essere i primi obbligati a

identificare i loro clienti e a segnalare alle Autorità competenti le operazioni in tal senso sospette. Si trattava però di un istituto particolare in cui il dovere di segnalazione era posto a carico di istituti di credito (obbligo legale) e non un diritto riconosciuto a livello europeo ai cittadini e alle cittadine.

Nei giorni nostri, per svolgere un'azione di forte contrasto alla corruzione e alla illegalità, sia nell'ambito pubblico che in quello privato, l'ordinamento europeo – constatando la disomogeneità delle normative nazionali in materia – ha introdotto una apposita Direttiva in materia di Whistleblowing 2019/1937, che persegue l'obiettivo di introdurre uno standard minimo di tutela per l'istituto delle segnalazioni nonché per i whistleblower stessi. La Direttiva prevede che la tutela del segnalante non riguardi solo i dipendenti ma anche clienti, fornitori e stagisti. Ciò rappresenta un elemento di differenza con quanto prevede l'attuale legge italiana in materia che, secondo l'opinione prevalente, si applica solo ai dipendenti.

Il D.Lgs. n. 24/2023, che introduce la nuova disciplina del whistleblowing in Italia, è entrato in vigore il 30 marzo 2023. Le nuove disposizioni avranno effetto a partire dal 15 luglio 2023, con una deroga per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati non superiore a nr. 249.

Il trattamento dei dati personali, svolto mediante strumenti informatici, deve essere improntato all'osservanza dei principi sanciti dalla vigente normativa in materia di protezione dei dati personali (GDPR). In particolare, dovrà:

1. trattarli in **modo lecito, corretto e trasparente**;
2. raccogliarli per **finalità determinate, esplicite e legittime**;
3. trattarli in **maniera adeguata, pertinente e limitata** a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **conservarli per un arco temporale** non superiore al conseguimento delle finalità per le quali sono trattati (max 5 anni);
5. **garantire una adeguata sicurezza dei dati personali**, mediante misure di sicurezza tecniche ed organizzative adeguate, evitando trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentale;
6. **Garantire il divieto di tracciamento dei canali di segnalazione**;
7. **Designare/incaricare internamente la persona competente** per la gestione delle segnalazioni (facilitatore);
8. **Rendere ex ante ai possibili interessati un'informativa sul trattamento dei dati personali** mediante la pubblicazione di documenti informativi (es. tramite il sito web). Nella fase di acquisizione della segnalazione e della eventuale successiva istruttoria non devono invece essere fornite informative ad hoc ai vari soggetti interessati diversi dal segnalante. Laddove all'esito dell'istruttoria sulla segnalazione si avvii un procedimento nei confronti di uno specifico soggetto segnalato, a quest'ultimo va naturalmente resa un'informativa ad hoc;
9. **Nominare il soggetto esterno** che si occuperà, in qualità di Responsabile esterno (ex art. 28 del Regolamento (UE) 2016/679 GDPR) della gestione del canale interno nonché (ove applicabile) della segnalazione stessa insieme al designato / incaricato interno / organo di competenza;

10. Avvalersi di un canale interno, ai sensi del D.Lgs. 24/2023 e delle Linee guida whistleblowing - Parte prima – I canali e le modalità di presentazione delle segnalazioni § 3.1, per la ricezione e la gestione delle segnalazioni.

1. Ambito di applicazione e quadro normativo di riferimento

Nell'ordinamento giuridico italiano, il provvedimento attuativo della Direttiva (UE) 2019/1937 è il d.lgs. n. 24 del 10 marzo 2023 (G.U. n. 63 del 15 marzo 2023). Quest'ultimo raccoglie e raggruppa in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti sia del settore pubblico che privato. Ne deriva una disciplina organica e uniforme finalizzata a una maggiore riservatezza e, dunque, tutela del segnalante.

Il nuovo Decreto è entrato in vigore il 30 marzo 2023 e le disposizioni, ivi previste, avranno effetto a partire dal 15 luglio 2023, con una deroga per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati non superiore a 249: per questi, infatti, l'obbligo di istituzione del canale di segnalazione interna avrà effetto a decorrere dal 17 dicembre 2023.

Il presente Disciplinare è stato adottato sulla base seguenti disposizioni:

- D.Lgs. 10 marzo 2023, n. 24 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";
- Delibera n. 311 del 12 luglio 2023 recante "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. Procedure per la presentazione e gestione delle segnalazioni esterne";
- D.Lgs. 8 giugno 2001, n. 231 recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300";
- (ove applicabile) D.L. 7 marzo 2005, n. 82, c.d. Codice dell'Amministrazione Digitale (CAD);
- Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- D.L. 10 agosto 2018, n. 101 che reca le disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679.

2. Chi può effettuare una segnalazione?

Dalla definizione fornita dalla vigente normativa si ricava che il whistleblower è la persona che segnala, violazioni di disposizioni normative nazionali o dell'UE che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato. In questo caso:

Dipendenti pubblici

- Lavoratori subordinati del settore privato
- Lavoratori autonomi che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato
- Collaboratori, liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato
- Volontari e i tirocinanti, retribuiti e non retribuiti del settore pubblico e privato
- Azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato

3. Come si può inviare una segnalazione?

Le segnalazioni devono essere trasmesse mediante i canali appositamente predisposti secondo la norma di riferimento. La scelta del canale di segnalazione non è più rimessa alla discrezione del whistleblower in quanto in via prioritaria è favorito l'utilizzo del canale interno e, solo al ricorrere di una delle condizioni di cui all'art. 6, è possibile effettuare una segnalazione esterna.

A. Canale interno

I soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, 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».

Attenzione: La gestione del canale interno dovrà essere affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero è affidata a un soggetto esterno, anch'esso autonomo e con personale specificamente formato

B. Canale esterno

L'Autorità competente per le segnalazioni esterne, anche del settore privato, è l'Autorità Nazionale Anticorruzione (ANAC): www.anticorruzione.it Ulteriori indicazioni in merito alla raccolta, gestione ed evasione delle segnalazioni tramite il canale esterno sono contenute nel Regolamento per la gestione delle segnalazioni esterne e per l'esercizio del potere sanzionatorio ANAC in attuazione del D.Lgs. 10 marzo 2023, n. 24. Delibera n. 301 del 12 luglio 2023 (link [qui](#)).

Secondo le nuove Linee Guida dell'ANAC "la scelta del soggetto cui affidare il ruolo di gestore delle segnalazioni è rimessa all'autonomia organizzativa di ciascun ente, in considerazione delle esigenze connesse alle dimensioni, alla natura dell'attività esercitata e alla realtà organizzativa concreta". Nello specifico, le nuove linee guida chiariscono che le strutture possono affidare la gestione delle segnalazioni, alternativamente:

- a una persona interna all'amministrazione/ente;
- a un ufficio dell'amministrazione/ente con personale dedicato, anche se non in via esclusiva;
- a un soggetto esterno.

Nel caso in specie il Titolare ha scelto ai sensi dell'art. 4 e 24 GDPR di:

affidare la gestione del canale interno ad un soggetto esterno (ReNorm S.r.l.), autonomo, imparziale e indipendente, debitamente nominato in qualità di Responsabile del trattamento (ai sensi dell'art. 28 del Regolamento (UE) 2016/679

affidare inoltre la gestione delle segnalazioni ad un soggetto esterno (**ReNorm S.r.l.**), autonomo, imparziale e indipendente, debitamente nominato in qualità di Responsabile del trattamento (ai sensi dell'art. 28 del Regolamento (UE) 2016/679 che, oltre a ricevere le segnalazioni tramite il canale interno scelto si occuperà della gestione delle segnalazioni insieme al facilitatore ovvero il designato interno della struttura (incaricato ai sensi dell'art. 2 – quaterdecies del Codice Privacy). In particolare:

Referente interno dr. **Amedeo Poli** – mail: amedeo.poli@auditft.it

Il soggetto esterno (ReNorm S.r.l.) conferma che il personale interno, tenuto a gestire i dati e le informazioni fornite dai segnalanti tramite il Portale ReBlowing è stato autorizzato (ex art. 29 Regolamento (UE) 2016/679 GDPR) al trattamento dei dati personali in oggetto nonché istruito. Conferma inoltre che il personale incaricato possiede i requisiti necessari per la gestione delle segnalazioni pervenute tramite il canale interno scelto dal Titolare.

Il canale interno scelto dal Titolare è ReBlowing, disponibile al seguente link: www.renorm.it/reblowing

Il canale interno di segnalazione scelto dal Titolare, come si vedrà nel proseguo, garantisce la riservatezza, anche tramite il ricorso a strumenti di crittografia, in quanto vengono utilizzati strumenti informatici:

- della persona segnalante;
- del facilitatore;
- della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
- del contenuto della segnalazione e della relativa documentazione.

4. Il canale interno: ReBlowing

Come sopra specificato il canale scelto dal Titolare è ReBlowing, disponibile al seguente link: www.renorm.it/reblowing Il Portale ReBlowing mette a disposizione, sia dei Clienti che dei segnalanti, la documentazione di seguito indicata, volta a garantire ai medesimi l'utilizzo del Portale:

- Termini & Condizioni del Servizio ReBlowing
- Misure di sicurezza tecniche ed organizzative adottate dal responsabile del trattamento per conto del titolare del titolare
- Misure tecniche garantite dal fornitore del Web Hosting e localizzazione dei server in UE (altro responsabile art.28 GDPR)
- Istruzioni per la registrazione degli interessati sul Portale ReBlowing
- Guida all'utilizzo del Portale ReBlowing
- Informativa privacy del titolare del trattamento

La scelta del canale interno è stata tempestivamente comunicata agli interessati tramite "Comunicazione di Servizio" a cui si fa rinvio. Tale "Comunicazione" permette al segnalante di:

- Comprendere l'ambito di applicazione dell'istituto del Whistleblowing;
- Il canale di segnalazione scelto;
- Le modalità di effettuazione di una segnalazione;
- I diritti di cui godono secondo la vigente normativa.

5. Caratteristiche tecniche del canale interno: ReBlowing

La soluzione tecnologica scelta dal Titolare garantisce al segnalante la propria riservatezza in quanto la segnalazione viene raccolta dal soggetto esterno – ai sensi della vigente normativa – tramite apposito canale

digitale (Portale ReBlowing) a cui il segnalante può accedere mediante due codici di accesso (Codice 1 e Codice 2) che ha ricevuto tramite la “Comunicazione di Servizio di cui sopra”.

Il Portale ReBlowing funge soltanto da mezzo per la raccolta delle segnalazioni. Le segnalazioni pervengono direttamente al soggetto esterno (ReNorm) a cui è stata affidata la gestione delle stesse ai sensi del punto 10 “Approfondimenti sui canali e le modalità di presentazione delle segnalazioni - I canali interni” contenuto nelle Linee guida whistleblowing - Parte prima – I canali e le modalità di presentazione delle segnalazioni § 3.1 nonché dell’art. 28 del Regolamento (UE) 2016/679. Il Portale non effettua trasferimenti di dati fuori dallo Spazio Economico Europeo (SEE): i server sono all’interno dell’UE (Spagna). Ulteriori specifiche [qui](#).

Il Portale è online e non effettua alcun tipo di tracciamento. Come si evince dal Portale ReBlowing, i cookie non necessari sono stati disattivati per permettere al segnalante una maggiore riservatezza. Vengono utilizzati solo cookie tecnici come specificato nella Privacy e Cookie Policy del sito medesimo (link [qui](#)).

Il segnalante non è tenuto ad effettuare alcuna registrazione sul portale. La registrazione avviene soltanto dal Titolare del trattamento ovvero dalla struttura che decide di avvalersi del Portale ReBlowing. Si tratta di una soluzione che permette ai segnalanti di accedere (tramite il link sopra riportato), inserendo i codici di riferimento in loro possesso e di provvedere – in maniera semplice, sicura e riservata – ad effettuare la propria segnalazione con la garanzia di ricevere entro i termini definiti dalla vigente normativa (7 giorni) la conferma di presa in carico. Al segnalante arriva la conferma di avvenuta segnalazione ed un codice ID (per identificare la propria segnalazione).

Nello specifico, i codici di riferimento messi a disposizione dei segnalanti per accedere al Portale sono due:

- Il Codice 1 (Codice o Code) viene assegnato dal gestore del canale interno (ReBlowing).
- Il Codice 2 (o Password) viene assegnato, invece, automaticamente dal canale interno (ReBlowing) tramite la creazione automatizzata di un codice alfanumerico che non è né direttamente né indirettamente riconducibile ad un dato personale ovvero ad una persona fisica identificata o identificabile. I codici di riferimento vengono messi a disposizione degli interessati, tempestivamente, dal Titolare mediante:

- Comunicazione di Servizio
- Pubblicazione in Bacheca
- Pubblicazione sul sito internet
- Condivisione le rappresentanze o le organizzazioni sindacali

Il Codici assegnati sono i medesimi per tutti i segnalanti. Di conseguenza, coloro che saranno in possesso di tali codici potranno accedere al Portale ReBlowing ed effettuare una segnalazione. In caso di perdita dei codici, i segnalanti possono rivolgersi al Titolare ovvero al facilitatore / designato interno. Il Titolare può richiedere in ogni momento la generazione di nuovi codici per l’accesso al Portale ReBlowing.

Effettuata la segnalazione, il segnalante riceve la conferma di invio nella lingua scelta dallo stesso in fase di compilazione direttamente nella casella di posta elettronica da lui scelta in fase di elaborazione della segnalazione. Si consiglia al segnalante di non utilizzare un indirizzo e-mail lavorativo ma privato. Nel caso di segnalazione “anonima” il segnalante è comunque tenuto a fornire un indirizzo e-mail che verrà oscurato in fase di presa incarico e di conseguente archiviazione della segnalazione. L’indirizzo e-mail è conditio sine qua non per poter ricevere la conferma di effettuazione della segnalazione e di presa in carico dal soggetto preposto.

La segnalazione ed il contenuto della medesima arriva al soggetto esterno tenuto a raccogliere e gestire la segnalazione insieme al designato o referente interno / RPCT / ODV, debitamente istruito, autorizzato dal Titolare. A tale scopo, il soggetto esterno gestore del canale ReBlowing (ReNorm) – in fase di definizione dei ruoli

– chiede per iscritto al Titolare di individuare la persona che, all'interno della propria struttura, è autorizzata a ricevere nonché a gestire le segnalazioni pervenute. Il Titolare è pertanto tenuto a fornire tempestivamente la nomina ex art. 28 GDPR 2016/679, debitamente compilata e firmata, contenente inoltre i dati del designato (nome, cognome ed indirizzo e-mail) con cui ReNorm è tenuto a confrontarsi. Qualora ReNorm non dovesse ricevere tali informazioni è tenuta a sollecitare nuovamente il Titolare ed informarlo circa la necessità di individuare la persona di riferimento sopra indicata tale e come stabilito dalla vigente normativa Whistleblowing.

La segnalazione dovrà contenere tutti gli elementi previsti dal D.Lgs. n. 24/2023 nonché tutte le informazioni e le evidenze che il segnalante – in fase di segnalazione – ritiene opportuno fornire a supporto della stessa. Al fine di permettere una maggiore riservatezza nonché indipendenza e neutralità nel processo di ricezione e gestione della segnalazione, il soggetto esterno provvede a crittografare il contenuto della segnalazione. Solo l'autorizzato del soggetto esterno potrà accedere alla stessa in quanto unico possessore della chiave di accesso.

Il contenuto crittografato della segnalazione viene condiviso dal soggetto esterno con il designato sopra indicato debitamente istruito dal Titolare. Il soggetto esterno è tenuto a fornire – esclusivamente – al designato la segnalazione pervenuta e non ad altri soggetti interni che possano richiedere l'invio della stessa senza l'autorizzazione del Titolare (es. responsabile del personale non autorizzato). In tali casi ReNorm è tenuta ad informarsi, a reperire tutte le informazioni necessarie nonché ad informare tempestivamente il Titolare al fine di verificare l'esattezza nonché la legittimità della richiesta effettuata da un soggetto non autorizzato.

Il designato dal Titolare riceverà una prima comunicazione – tramite e-mail ovvero all'indirizzo di posta elettronica fornito – con il file crittografato a cui potrà accedere con una password automaticamente generata dal soggetto esterno e una seconda comunicazione (tramite SMS) contenente il codice di accesso che permetterà al designato di aprire il file crittografato (la comunicazione di tale codice alfanumerico avverrà tramite lo strumento Skebby di cui avvale il Responsabile esterno (ulteriori specifiche in merito alle misure di sicurezza tecniche ed organizzative garantite da Skebby – Commify Italia S.r.l. sono reperibili [qui](#)). Il designato è tenuto a mantenere il massimo riserbo relativamente al contenuto della segnalazione e all'identità del segnalante qualora il medesimo non abbia fornito il consenso alla comunicazione della propria identità a soggetti terzi o non autorizzati a trattare tali informazioni.

Il segnalante è pertanto tenuto a specificare se “acconsente la rivelazione della propria identità a persone diverse da quelle competenti a ricevere o a dare seguito alla segnalazione”. Tale possibilità viene garantita al segnalante in fase di elaborazione della segnalazione. Qualora il segnalante decidesse di non acconsentire tale trattamento, la segnalazione verrà condivisa solo con l'autorizzato del soggetto esterno (ReNorm quale responsabile del trattamento) e con il designato interno o facilitatore.

ReNorm è tenuta a conservare il contenuto della segnalazione secondo i principi stabiliti dalla vigente normativa in materia di protezione di dati personali e per il tempo strettamente necessario e non oltre 5 anni dalla ricezione della stessa ovvero per il tempo definito dal Titolare del trattamento secondo i propri principi di accountability. Ulteriori indicazioni sono contenute nella nomina ex art. 28 del Regolamento (UE) 2026/679 sottoscritta dal Titolare e dal soggetto esterno gestore del canale interno e del servizio contrattualizzato nonché nell'informativa privacy che il Titolare del trattamento metterà a disposizione di tutti gli interessati.

Su richiesta del Titolare, ReNorm potrà agire per conto dell'ente che ha ricevuto la segnalazione e potrà confrontarsi – previ accordi con il Titolare e come descritto dalle nuove Linee Guida dell'ANAC – con il segnalante. Tale possibilità permetterebbe al Titolare di agevolare l'attività istruttoria e di gestione della segnalazione. Il soggetto esterno è tenuto a fornire tutte le informazioni raccolte e gestite con il designato dal Titolare. Il soggetto esterno potrà inoltre gestire le tempistiche e tenere monitorata la gestione della segnalazione.

Il segnalante potrà richiedere eventuali aggiornamenti in merito allo status della segnalazione direttamente dal Portale ReBlowing, tramite la sezione dedicata del Portale. In tali casi, ReNorm è tenuta a trasmettere tale

ulteriore richiesta al designato entro i termini definiti dalla vigente normativa nonché a sollecitare al designato stesso un riscontro in merito allo status della segnalazione e le azioni da intraprendere a tutela del segnalante.

5. Guida all'utilizzo di ReBlowing (canale interno)

La Guida all'utilizzo di ReBlowing è disponibile direttamente sul sito web del soggetto esterno: www.renorm.it/reblowing. La Guida potrebbe subire delle modifiche nel tempo in base agli aggiornamenti del Portale. Il Portale conterrà sempre la versione aggiornata al fine di permettere ai segnalanti di avere a disposizione tutte le informazioni necessarie nonché una panoramica dell'iter per l'effettuazione di una segnalazione.

6. Titolare: iter di registrazione sul Portale ReBlowing

Le istruzioni per la registrazione sul Portale ReBlowing sono allegate alla presente procedura.

7. Procedura di gestione delle segnalazioni: schema

		Cliente Designato	ReNorm Autorizzato	
5 Steps per la gestione delle segnalazioni	1	Ricezione della segnalazione tramite il Portale ReBlowing		
		Il/la Whistleblower effettua una segnalazione tramite ReBlowing. ReNorm riceve la conferma di avvenuta ricezione di nuova segnalazione		
	2	Presa in carico della segnalazione		
		Presa in carico la richiesta della segnalazione entro 7 giorni dal ricevimento della stessa		
		Crittazione del contenuto della segnalazione		
		Trasmissione al soggetto autorizzato/designato dal Cliente, entro 30 giorni, a) tramite e-mail, un file crittato contenente il contenuto della segnalazione ed eventuali allegati; b) tramite sms al numero di telefono fornito dal soggetto autorizzato/designato dal Cliente, una password per l'apertura del contenuto della segnalazione		
	3	Gestione della segnalazione		
		Gestione della segnalazione in maniera riservata e a non rivelare il contenuto della stessa senza il consenso espresso della persona segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni	X	X
		(ove contrattualizzato) collaboratore con il soggetto autorizzato/designato dal Cliente alla gestione della segnalazione e propone misure volte alla risoluzione della stessa		X
		(ove contrattualizzato) Informare il segnalante dello status della segnalazione		X
		(ove contrattualizzato) Interfacciarsi con il segnalante		X
	4	Conservazione della segnalazione		
		Conservare la segnalazione nonché tutta la documentazione a supporto	X	X
	5	Chiusura della segnalazione		
		Risolvere la segnalazione entro i tempi definiti dalla vigente normativa.	X	
	Nei tempi previsti dalla normativa, cancellazione di tutte le informazioni ed i dati personali raccolti non più necessari	X	X	

8. Protezione dei dati personali

Ai sensi della normativa applicabile il Titolare ha adottato la seguente modulistica a cui si fa rinvio:

- Comunicazione di Servizio. Da inviare a tutti i soggetti interessati. All'interno del presente documento (o Comunicazione) si includono il codice a assegnato e la password tramite cui i segnalanti potranno effettuare le proprie segnalazioni
- Informativa privacy segnalanti. Redatta ai sensi dell'art. 13 del Regolamento (UE) 2016/679, che andrà allegata alla Comunicazione di Servizio di cui sopra
- Lettera di incarico (Designato / Facilitatore), figura che si occuperà della gestione delle segnalazioni insieme al soggetto esterno gestore del canale interno nonché (ove richiesto) della gestione delle segnalazioni
- Valutazione di Impatto – Data Protection Impact Assessment (DPIA) relativamente al trattamento in oggetto
- Nomina art. 28 GDPR 2016/679 nei confronti della Società ReNorm S.r.l.
- Aggiornamento del Registro dei trattamenti del Titolare
- Whistleblowing Policy

9. Provvedimenti sanzionatori

La presente Policy risulta correttamente portata a conoscenza di soggetti tenuti alla gestione delle segnalazioni.

L'incaricato (designato) alla gestione delle segnalazioni nonché il responsabile esterno del trattamento quale soggetto esterno che si occupa della ricezione e (ove richiesto) gestione delle segnalazioni, sono tenuti al rispetto della presente Policy. In caso di inosservanza, il Titolare potrà adottare provvedimenti di natura disciplinare/amministrativa, altre sanzioni previste dal CCNL di settore, cui si rimanda per ogni specifica, nonché procedere con le azioni civili e penali che ne dovessero scaturire anche nei confronti del soggetto esterno.

Aggiornamenti e revisione

In virtù dell'evoluzione normativa e tecnologica, la presente Policy potrà essere oggetto di aggiornamento e revisione. Ogni modifica o integrazione dovrà essere portata a conoscenza degli interessati, così da fornire le nuove istruzioni circa l'utilizzo degli strumenti e delle procedure messe a disposizione per la gestione delle segnalazioni ai sensi della vigente normativa.