



Via Jonio, 43 - 75100 MATERA

☎ 0835.259641/268807 📠 0835.309548

✉ betafin@betafin.it

PROCEDURA OPERATIVA WHISTLEBLOWING

(D. Lgs. del 10 marzo 2023, n. 24)

0					
	0	02.01.25	Emissione		
Ediz.	Rev.	Data	Descrizione revisione	DDL	

SOMMARIO

1. PREMESSA.....	3
1.1. Obiettivi	3
2. WHISTLEBLOWING	3
2.1. Normativa.....	3
2.2. Scopo della procedura.....	4
2.3. Soggetti tutelati.....	4
2.4. Riservatezza sulla persona del segnalante e degli altri soggetti coinvolti nella procedura	6
2.5. Violazioni rilevanti ai fini della segnalazione	6
2.6. Contenuto delle segnalazioni	7
3. PROCEDURE E GESTIONE DELLE SEGNALAZIONI.....	8
3.1. Canali di segnalazione interni	8
3.2. Canali di segnalazione esterni	10
4. TRATTAMENTO DEI DATI PERSONALI.....	10
5. CONSERVAZIONE DELLA DOCUMENTAZIONE.....	11
6. CONDIZIONI PER LA PROTEZIONE DEL SEGNALANTE.....	11
7. DIVIETO DI RITORSIONI.....	12
8. FORMAZIONE	13

1. PREMESSA

In ottemperanza alla normativa contenuta all'interno de D. Lgs. del 10 marzo 2023, n. 24 in materia di Whistleblowing ed alla normativa ex D. Lgs. 231/2001 in materia di Responsabilità degli Enti, la BETAFIN SPA ha istituito un apposito sistema di comunicazione nei confronti del Responsabile della Trasparenza, dott. Nicola Salerno, in grado di tutelare la riservatezza dei segnalanti e scongiurare l'ipotesi di ripercussioni nei loro confronti.

1.1. Obiettivi

Il documento nominato "Procedura Whistleblowing" ha l'obiettivo di regolamentare la gestione delle segnalazioni fatte al Responsabile della Trasparenza ai sensi della normativa in materia di Whistleblowing (D. Lgs. 24/2023), emanato in applicazione della direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. All'interno di questo documento si trova la descrizione delle misure di protezione dei soggetti tutelati dalla normativa.

Con tale documento, BETAFIN SPA intende certamente tutelare i soggetti segnalanti e prevede espressamente il divieto di condotte ritorsive, discriminatorie o, in ogni caso, sleali nei loro confronti come conseguenza delle segnalazioni. Ancora, obiettivo di tale documento è quello di adottare specifici provvedimenti disciplinari per i responsabili di tali condotte riprovevoli.

2. WHISTLEBLOWING

Il *Whistleblowing* è uno strumento di derivazione anglosassone attraverso il quale i dipendenti di una organizzazione, pubblica o privata, segnalano a specifici individui o organismi, (compresi organi di polizia e autorità pubbliche) una possibile frode, un reato, un illecito o qualunque condotta irregolare, commessa da altri soggetti appartenenti all'organizzazione. I dipendenti, intesi in senso ampio - come specificato meglio nel prosieguo - normalmente sono le prime persone che vengono a conoscenza di eventuali situazioni di rischio e, pertanto, sono anche le prime persone in grado di segnalarle tempestivamente all'organizzazione, prima che possano realizzarsi eventuali danni. Lo scopo del Whistleblowing è quello di permettere alle organizzazioni di affrontare il problema segnalato il prima possibile, rendendo note situazioni potenzialmente pericolose o incresciose, proteggendo allo stesso tempo la persona che abbia effettuato la segnalazione, garantendone, ove questa lo desideri, l'anonimato e la sicurezza contro eventuali ripercussioni nei suoi confronti.

2.1. Normativa

La legge 30 novembre 2017 n. 179, in materia di disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato, ha introdotto per la prima volta una disciplina sulle segnalazioni di illeciti e irregolarità di gestione (c.d. "Whistleblowing") con riguardo al settore privato (per quanto riguarda il settore pubblico, invece, una normativa simile era già in vigore all'interno dell'ordinamento dall'entrata in vigore della legge 6 novembre 2012 n. 190), scegliendo quale strumento per dare concretezza alla nuova normativa

il Modello di Organizzazione, Gestione e Controllo adottato dalle società commerciali e dagli altri destinatari della disciplina della responsabilità da reato degli enti (c.d. MOGC).

Il D. Lgs. 24/2023, già menzionato, ha riformato la materia rafforzando l'importanza che riveste la protezione dei whistleblowers, ossia delle persone che segnalano 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.

Per quanto riguarda il settore privato, la legge n. 179/2017 aveva già incrementato l'art. 6 del D.Lgs. n. 231/2001 con tre nuovi commi che, oltre a prevedere il divieto di atti di ritorsione o discriminatori nei confronti del segnalante e misure volte a tutelare lo stesso segnalante contro questi atti, disponevano che all'interno del MOGC si dovesse provvedere ad individuare dei canali di segnalazione per denunciare condotte illecite rilevanti ai sensi del Decreto o violazioni del MOGC. Tra questi canali era previsto che almeno uno fosse in grado di garantire la riservatezza dell'identità del segnalante.

Quello che avviene grazie al nuovo D. Lgs. 24/23 è proprio un rafforzamento della posizione del segnalante, in quanto subentra un obbligo, per le società che rivestono determinati requisiti, di adottare procedure e sistemi che garantiscano la protezione dell'identità del segnalante. La nuova normativa, inoltre, vieta categoricamente all'azienda, laddove questi sistemi dovessero fallire, di intraprendere qualunque azione ritorsiva nei confronti del segnalante eventualmente individuato.

2.2. Scopo della procedura

Lo scopo della nuova procedura è quindi quello di garantire all'azienda un canale per avere sempre cognizione di quanto accade al suo interno, così da poter gestire i problemi tempestivamente, ed allo stesso tempo mantenere la riservatezza sulla persona del segnalante proteggendolo da qual si voglia ritorsione nei suoi confronti.

La presente procedura, pertanto, è stata predisposta per regolamentare la gestione delle segnalazioni di irregolarità, a partire dal momento in cui il segnalante si determini all'inoltro sino ai successivi sviluppi.

2.3. Soggetti tutelati

Le disposizioni della presente Procedura si applicano alle seguenti persone che segnalano, denunciano all'autorità giudiziaria o contabile o divulgano pubblicamente informazioni sulle violazioni di cui sono venute a conoscenza nell'ambito del contesto lavorativo della BETAFIN SPA:

- tutti i dipendenti della BETAFIN SPA;
- i lavoratori autonomi, nonché i titolari di un rapporto di collaborazione, che svolgono la propria attività lavorativa presso la BETAFIN SPA;
- i liberi professionisti e i consulenti che prestano la propria attività lavorativa presso la BETAFIN SPA;
- i lavoratori e i collaboratori che svolgano la propria attività lavorativa presso soggetti che forniscono beni o servizi o che realizzano opere in favore della BETAFIN SPA;

- i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la BETAFIN SPA;
- le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza della BETAFIN SPA (anche qualora tali funzioni siano esercitate in via di mero fatto).

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

- quando il rapporto giuridico non sia ancora iniziato, se le informazioni sono state acquisite dal segnalante durante il processo di selezione o in altre fasi precontrattuali;
- durante il periodo di prova;
- Successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

Tutte le misure di protezione previste dalla presente Procedura si applicano altresì:

- ai facilitatori, ossia le persone che hanno assistito il soggetto segnalante nel processo di segnalazione, operanti all'interno del medesimo contesto lavorativo, la cui assistenza deve essere mantenuta riservata;
- 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.

2.4. Riservatezza sulla persona del segnalante e degli altri soggetti coinvolti nella procedura

Tutto il personale della BETAFIN SPA, ed in particolare tutti i soggetti coinvolti nel processo di gestione delle segnalazioni, garantiscono la riservatezza della segnalazione e soprattutto della persona del segnalante, del segnalato e delle persone coinvolte dalla segnalazione quali facilitatori o persone informate sui fatti. La massima riservatezza su tutti i soggetti dev'essere mantenuta fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie espressamente previste in favore della persona del segnalante. Per tale motivo tutto il personale della BETAFIN SPA viene specificatamente formato in merito agli obblighi di riservatezza previsti dalla normativa in materia di Whistleblowing.

L'identità della persona segnalante e qualunque altra informazione da cui tale identità possa evincersi, direttamente o indirettamente, non possono essere rivelate, senza il consenso espresso dello stesso segnalante, a persone diverse da quelle competenti a ricevere o a gestire le segnalazioni.

In caso di instaurazione di un procedimento disciplinare, l'identità del segnalante non può essere rivelata né se la contestazione dell'addebito disciplinare è fondata su accertamenti conseguenti alla segnalazione, né se gli stessi sono distinti e ulteriori rispetto alla segnalazione. Nel caso in cui la contestazione sia fondata, anche in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, l'identità del segnalante sarà rivelata solo in presenza del suo espresso consenso.

Il vincolo di riservatezza della persona del segnalante può essere non rispettato nei casi in cui:

- Il segnalante abbia prestato il consenso espresso a rivelare la propria identità;
- È accertata con sentenza di primo grado la responsabilità penale del segnalante per reati di calunnia, diffamazione ovvero per reati commessi per mezzo di segnalazione;
- È accertata con sentenza di primo grado la sua responsabilità civile per lo stesso titolo nei casi di dolo o colpa grave;
- L'anonimato non sia opponibile per legge e l'identità del segnalante sia richiesta dall'Autorità giudiziaria.

La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché agli articoli 5 e seguenti del D. Lgs. 14 marzo 2013, n. 33.

2.5. Violazioni rilevanti ai fini della segnalazione

Questa Procedura, come già sopra specificato, ha lo scopo di proteggere le persone che segnalano violazioni di disposizioni normative regolamentari e nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità della BETAFIN SPA, di cui siano venute a conoscenza nel contesto lavorativo aziendale.

Le tutele previste dalla presente Procedura non verranno accordate in caso di segnalazioni riguardanti contestazioni, rivendicazioni o richieste legate ad un interesse di carattere prettamente personale del segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate, per le quali sarà necessario fare ricorso alle apposite procedure istituite dalla Società. Inoltre, sono escluse dalle tutele anche le segnalazioni concernenti violazioni delle quali vi sia stata conoscenza in un contesto esterno a quello

della BETAFIN SPA ovvero fondate su voci correnti e non su fatti appresi direttamente dalla persona segnalante.

La BETAFIN SPA non ammette, anzi sanziona, le segnalazioni fatte con lo scopo di danneggiare il soggetto segnalato, effettuate con dolo o colpa grave, che si rivelino palesemente infondate.

La Segnalazione può avere ad oggetto diversi tipi di comportamenti:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del D. Lgs. 231/2001 o in violazione del modello di organizzazione e gestione della BETAFIN SPA o in violazione del Codice Etico della BETAFIN SPA;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali 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;
- atti od omissioni che ledono gli interessi finanziari dell'Unione;
- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto e la finalità delle disposizioni di cui agli atti dell'Unione.

2.6. Contenuto delle segnalazioni

Non esistono obblighi per il segnalante che decida di rendere nota la violazione. Tuttavia, è opportuno che il *whistleblower* fornisca tutti gli elementi di cui sia a conoscenza e che utilmente consentano al destinatario della segnalazione di procedere agevolmente alle dovute e appropriate verifiche per accertare la fondatezza dei fatti oggetto della segnalazione. A tal fine, le segnalazioni devono avere contenuto circostanziato e devono essere fondate su elementi di fatto precisi e concordanti (ossia non devono essere suscettibili di interpretazioni differenti), ovvero convergenti nella medesima direzione.

Le segnalazioni non possono riguardare meri sospetti o notizie riferite da terzi o, comunque, che non abbiano elementi di fatto o documenti univoci a supporto degli stessi. Ad ogni modo, non è necessario che la persona segnalante abbia certezza dell'effettivo avvenimento dei fatti segnalati e dell'autore degli stessi, essendo sufficiente che, in base alle proprie conoscenze e nel rispetto del principio di buona fede, nonché sulla base di una ragionevole convinzione fondata su elementi di fatto, lo ritenga altamente probabile.

Affinché siano considerate valide, è necessario che le segnalazioni abbiano quali elementi essenziali:

- una precisa descrizione dell'oggetto della segnalazione, con indicazione delle circostanze di tempo e luogo in cui sono stati commessi/omessi i fatti;
- gli elementi che consentano, ove possibile, una chiara identificazione del soggetto segnalato ritenuto il presunto autore della condotta illecita e/o della violazione del Modello.

Inoltre, la persona segnalante può comunicare, se ritiene, le proprie generalità e ulteriori elementi, se conosciuti, quali:

- eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- 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.

3. PROCEDURE E GESTIONE DELLE SEGNALAZIONI

3.1. Canali di segnalazione interni

La gestione delle segnalazioni è affidata al Responsabile della Trasparenza, che può eventualmente avvalersi dell'ausilio di collaboratori individuati dalla Società e specificamente formati in materia. Qualora la segnalazione dovesse erroneamente pervenire ad un soggetto diverso dal Responsabile della Trasparenza (o suo collaboratore), questo è tenuto a trasmetterla a quest'ultimo entro sette giorni dal suo ricevimento, nel rispetto degli obblighi di riservatezza previsti dalla presente procedura, dando contestuale notizia della trasmissione al segnalante.

Le segnalazioni possono essere effettuate in forma scritta o in forma orale attraverso i seguenti canali informativi:

- portale TRUSTY REPORT il cui seguente link di accesso è
 - <https://betafin.trusty.report>
ed è pubblicato anche sul sito dell'azienda nell'apposita sezione "Trasparenza";
- incontro diretto con il Responsabile della Trasparenza, previo appuntamento da concordare telefonicamente

3.1.1. Gestione delle segnalazioni

Il Responsabile della Trasparenza, ricevuta la segnalazione, deve svolgere le seguenti attività:

1. rilasciare al segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
2. mantenere le interlocuzioni con la persona segnalante e, se ritiene, può chiedere allo stesso di effettuare delle integrazioni;
3. dare diligente seguito alla segnalazione ricevuta;
4. fornire riscontro al segnalante entro tre mesi dalla data di scadenza del termine per rilasciare avviso di ricevimento della segnalazione, a prescindere dal fatto che l'avviso sia stato rilasciato o meno.

Il Responsabile della Trasparenza prenderà in carico le segnalazioni anonime solo se adeguatamente circostanziate e fondate su elementi di fatto precisi e concordanti.

Al ricevimento di una segnalazione, il Responsabile della Trasparenza, indipendentemente dal canale tramite cui gli sia pervenuto, provvede tempestivamente a compilare il registro delle segnalazioni in cui devono essere riportati:

1. il numero identificativo progressivo che ne consenta l'identificazione univoca;

2. la data di ricezione;
3. il canale di ricezione utilizzato;
4. la classificazione della segnalazione attribuita a seguito di valutazione preliminare del suo contenuto (Rilevante, Carente, Non Pertinente);
5. risultanze emerse e conclusioni.

Le segnalazioni vengono preliminarmente classificate dal Responsabile della Trasparenza nelle seguenti categorie:

- **RILEVANTE**, segnalazione pertinente e sufficientemente circostanziata, tale da consentire l'avvio delle indagini di verifica;
- **CARENTE**, segnalazione con contenuto insufficiente ad avviare le indagini di verifica. Il Responsabile della Trasparenza deve chiedere al segnalante informazioni integrative al fine di poter avviare gli accertamenti sui fatti oggetto della segnalazione e poter riclassificare la segnalazione come **RILEVANTE**. Il mancato invio delle integrazioni richieste non comporta l'automatica archiviazione della segnalazione. Il Responsabile della Trasparenza è tenuto a valutare le eventuali ragioni sottese al rifiuto, qualora indicate, nonché a tentare di reperire le informazioni necessarie mediante ricorso a canali alternativi;
- **NON PERTINENTE**, segnalazione non attinente al campo di applicazione della normativa in materia di Whistleblowing in quanto afferente a persone non strettamente connesse con la realtà aziendale o fatti, azioni o comportamenti che non configurano alcuna tra le condotte illecite indicate al precedente punto 2.3. Tuttavia, nel caso in cui il Responsabile della Trasparenza, pur classificandola come **NON PERTINENTE**, ritenga fondata la segnalazione, può trasmetterla al soggetto che ritenga responsabile e competente ad espletare le opportune verifiche.

Qualora la segnalazione riguardi l'Amministratore Unico, il Responsabile della Trasparenza ne dà immediata comunicazione all'Organo di Controllo (Revisore Unico).

Ove la segnalazione concerna condotte rilevanti ai sensi del D. Lgs. 231/01, ovvero evidenze violazioni del Modello Organizzativo, il Responsabile della Trasparenza ne dà immediata notizia all' Organismo di Vigilanza, il quale può presentare osservazioni in merito alla linea di indagine da seguire e deve essere informato sull'esito delle indagini.

Per gli accertamenti interni, necessari a verificare la fondatezza dei fatti denunciati tramite segnalazione, il Responsabile della Trasparenza può avvalersi di consulenti esterni. Questi ultimi sono tenuti ad osservare l'obbligo di riservatezza sui fatti di cui vengono a conoscenza nell'espletamento delle attività di consulenza e sull'identità delle persone coinvolte.

Qualora la segnalazione risulti fondata, il Responsabile della Trasparenza è tenuto a contestare tempestivamente e formalmente le violazioni denunciate alla Persona Segnalata, la quale può, entro trenta giorni dalla ricezione della contestazione, chiedere di essere sentita, ovvero presentare osservazioni scritte e documenti.

Conclusi gli accertamenti necessari, il Responsabile della Trasparenza predisponde un'apposita relazione da consegnare all'Amministratore Unico in cui viene formalizzato il contenuto, il quadro normativo e procedurale di riferimento, le attività di verifica svolte, i risultati emersi, i documenti e/o altri elementi comprovanti la condotta illecita o la violazione commessa, l'eventuale proposta di sanzione.

In caso di segnalazioni vietate, ossia effettuate con dolo o colpa grave, che si rivelino palesemente infondate, il Responsabile della Trasparenza informa di tale circostanza l'Organo Amministrativo della Società che deve dare avvio al procedimento disciplinare nei confronti del segnalante. In questa circostanza, il Responsabile della Trasparenza deve darne comunicazione anche al soggetto segnalante per consentirgli l'esercizio del diritto di difesa.

3.2. Canali di segnalazione esterni

Oltre ai canali di segnalazione interni sopra individuati, la segnalazione può essere anche effettuata attraverso apposito canale esterno, attivato dall'ANAC, se ricorrono i seguenti presupposti:

- a. La persona segnalante ha già effettuato una segnalazione interna nelle modalità disciplinate al precedente punto 3.1. e la stessa non ha avuto seguito;
- b. La persona segnalante ha fondati motivi di ritenere che se effettuasse una segnalazione interna alla stessa non verrebbe dato efficace seguito, ovvero che la stessa segnalazione possa determinare rischio di ritorsione;
- c. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Questo tipo di segnalazione avviene mediante accesso al portale dedicato dell'ANAC: <https://whistleblowing.anticorruzione.it/#/>

3.3. Divulgazioni pubbliche

Per divulgazione pubblica si intende il rendere di pubblico dominio informazioni che concernono le violazioni, tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

Il segnalante che effettui una divulgazione pubblica beneficia della protezione prevista dalla presente Procedura se, al momento della divulgazione pubblica, ricorre una delle condizioni di seguito riportate:

1. 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 dalla presente Procedura e non è stato dato riscontro nei termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
2. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
3. 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.

4. TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali, in ogni sua forma - inclusa la comunicazione tra autorità competenti -, che tale Procedura contempla, deve essere effettuato nel rispetto della normativa dettata dal Regolamento (UE) 2016/679, dal D. Lgs. 30 giugno 2003, n. 196 e dal D. Lgs. 18 maggio 2018, n. 51.

I dati personali, raccolti in occasione di segnalazione e accertamenti, devono essere conservati fino alla conclusione delle attività e successivamente cancellati. Se si ritiene che determinati dati non siano utili all'esame della segnalazione, questi non vengono acquisiti o, se acquisiti accidentalmente, devono essere prontamente cancellati e/o distrutti.

Nel rispetto delle normative vigenti, la BETAFIN SPA predispone un modello di ricevimento e gestione delle segnalazioni interne che si avvale di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, individuati attraverso una valutazione d'impatto sulla protezione dei dati e collaborando, ove necessario, con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'art. 28 del Regolamento (UE) 2016/679 o dell'articolo 18 del D. Lgs. n. 51 del 2018.

5. CONSERVAZIONE DELLA DOCUMENTAZIONE

Tutta la documentazione, inerente alle segnalazioni interne ed esterne vengono conservate per il tempo necessario allo svolgimento della procedura e comunque non oltre cinque anni, a decorrere dalla data di comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui al precedente punto 2.3.

Le segnalazioni che vengono effettuate mediante utilizzo di linea telefonica, se appositamente istituita, possono essere registrate e conservate su supporti elettronici idonei a garantirne la riservatezza previo consenso del segnalante; in caso di mancanza del consenso le segnalazioni devono essere documentate per iscritto mediante verbale dettagliato della conversazione.

Se la segnalazione è effettuata oralmente, il personale addetto, previo consenso del segnalante, può registrare su dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale.

La documentazione viene conservata attuando misure tecniche organizzative adeguate ad impedirne la loro perdita, distruzione o danno accidentale.

6. CONDIZIONI PER LA PROTEZIONE DEL SEGNALANTE

Le misure di protezione previste dal D. Lgs. 24/2023, e richiamate nella presente Procedura, si applicano alle persone segnalanti quando ricorrono le seguenti condizioni:

- 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;
- la segnalazione o divulgazione pubblica è stata effettuata sulla base di quanto previsto dal Decreto 24/2023;

I motivi che inducono la persona a segnalare o denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione, salvo quanto segue.

Le tutele previste dal Decreto non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare 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.

7. DIVIETO DI RITORSIONI

I soggetti tutelati dalla presente Procedura, in ottemperanza a quanto disciplinato dal Decreto Legislativo 24/2023, non possono – meglio, non devono – subire alcuna ritorsione da parte della BETAFIN SPA. Per ritorsione deve intendersi qualsiasi comportamento, atto o omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile ovvero della divulgazione pubblica, e che provoca o può provocare alla persona segnalante – o a colui che denuncia -, in via diretta o indiretta, un danno ingiusto.

Nel caso in cui tali comportamenti vengano ad esistenza, vige la presunzione che gli stessi siano stati attuati in conseguenza della segnalazione. 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.

Vengono di seguito elencate, a titolo esemplificativo non esaustivo, talune fattispecie che si presumono atti ritorsivi nel caso siano riconducibili ad una segnalazione:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- 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;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- 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'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;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- a richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Tali atti, assunti in violazione della presente Procedura devono ritenersi nulli. I soggetti che siano stati licenziati a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile hanno diritto a essere reintegrate nel posto di lavoro, ai sensi della vigente normativa, in ragione della specifica disciplina applicabile al lavoratore.

Gli enti e le persone segnalanti possono comunicare all'ANAC le ritorsioni che ritengono di avere subito. In caso di ritorsioni commesse nel contesto lavorativo di un soggetto del settore privato l'ANAC informa l'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza. L'autorità giudiziaria adita adotta tutte le misure, anche provvisorie, necessarie ad assicurare la tutela alla situazione giuridica soggettiva azionata, ivi compresi il risarcimento del danno, la reintegrazione nel posto di lavoro, l'ordine di cessazione della condotta posta in essere e la dichiarazione di nullità degli atti adottati in violazione del medesimo articolo. L'ANAC applica al responsabile anche sanzioni amministrative pecuniarie.

8. FORMAZIONE

L'azienda organizza periodicamente sessioni informative e formative al personale, volte a:

- dare un quadro delle normative cogenti in materia ivi comprese quelle in merito al trattamento dei dati del segnalante e di tutte le altre persone eventualmente coinvolte nel processo (segnalanti e facilitatori) – normativa in materia di protezione dei dati personali;
- illustrare la procedura aziendale in modo che le persone abbiano chiaro il canale da utilizzare;
- sensibilizzare sulla materia chiarendo le tutele e le garanzie di riservatezza in caso di segnalazioni.

8.1 Guida Trusty Report

Innanzitutto, suggeriamo di non accedere al sito web dell'applicazione per le segnalazioni tramite il link fornito dall'organizzazione. Di solito, l'organizzazione pubblica questo link sulla sua homepage o intranet. Per aumentare la tua protezione, copia l'indirizzo del sito web delle segnalazioni o aggiungilo ai segnalibri ed entra direttamente nel sito web.

Una volta entrato nel sito web, puoi iniziare a inviare la tua segnalazione cliccando sul pulsante "Effettua una segnalazione".



Make a report

The report should be made in good faith. Please note, mandatory questions are marked with an asterisk (*) and you will not be able to proceed without filling in the respective fields. After submitting the report, your username and password will be automatically generated and displayed on your screen. Please write them down as you will need them to enter your inbox and follow up on your report.

Nel passaggio successivo troverai informazioni su come utilizzare l'applicazione in modo sicuro e su come vengono elaborati i dati inviati.

Secure usage of the application

If you do not wish to reveal your identity, be careful not to submit any information that may personally identify you. Check whether your internet connection is safe and the browser you are using, displays a padlock icon. Enter the application directly by saving the entry page to bookmarks.

ABC Transparency GmbH guarantees the technical anonymity of the reporting person and ensures that his/her identity cannot be traced by technical means.

Data processing

The organization is the controller of the submitted personal data.

Details

I confirm that I have read and understood the warnings about security, confidentiality, the data processing provisions, as well as my obligations regarding anonymity, and hereby



Devi confermare di aver letto e compreso le informazioni fornite spuntando la casella per procedere.

Nei due passaggi successivi ti verrà chiesto di fornire quante più informazioni possibili sulla violazione segnalata. Potrai allegare documenti, tuttavia, prima di allegarli, ti suggeriamo di controllare i file per i metadati che potrebbero rivelare la tua identità. Se non sei ancora sicuro, puoi anche inviare i documenti in formato cartaceo all'indirizzo dell'organizzazione, annotando su di essi il nome utente che ti verrà assegnato al termine della tua presentazione.

Reporting a breach

For successful processing of your report it is important to provide as much information on the subject matter as possible. Mandatory questions are marked with an asterisk and you will not be able to proceed without filling in the respective fields. Information provided in non-mandatory fields is most welcome. However, you can skip these fields if you do not have the relevant knowledge.

When and where did the breach occur?

Persons suspected to be involved

Full name	Position	Organization
<input type="text"/>	<input type="text"/>	<input type="text"/>

+

Is anyone else aware of the breach?

Full name	Position	Organization
<input type="text"/>	<input type="text"/>	<input type="text"/>

+

Please describe the breach in your own words *

test

Please note that any reported person may be notified of the report at an appropriate time by the organization.

Attach documents:

Prior to their attachment, check your files for metadata that may reveal your identity. We recommend sending the documents in a pdf format or in paper to the address of the organization and writing your username which will be assigned to you upon completion of your submission

Reporting a breach

In which country did the alleged breach occur? *

Austria

Page 2 of 5

Alla fine del processo, ti verrà chiesto se desideri rivelare la tua identità. Se vuoi rimanere anonimo, fai semplicemente clic sul pulsante "Invia".

Reporting a breach

You may submit your report anonymously, or you may decide to disclose your identity to the organization either now or even later. In both cases you will be assigned a username and password, which you will need to access your inbox.

Disclosed ID of the reporting person usually allows for a more productive and efficient processing of the report and his/her protection against retaliation. Please refer to the organization's policies for further details on protection against retaliation and confidentiality.

Are you willing to disclose your identity? *

No, I prefer to remain anonymous.

 Yes, I would like to disclose my identity.

Page 4 of 5

Se decidi di identificarti, potrai inserire i tuoi dati nei campi della pagina successiva. I campi con l'asterisco sono obbligatori.

Riceverai una conferma della ricezione della tua segnalazione all'indirizzo email che inserisci nel campo dedicato.

Spuntando la casella in fondo alla pagina puoi attivare l'opzione per essere notificato via email di eventuali messaggi dell'organizzazione che ti aspettano nella tua casella di posta, a condizione che tu abbia inserito l'indirizzo email, ovviamente.

Please enter your details here:

First name *

Last name *

E-mail address

Telephone number *

Relationship towards the organization

Receive E-mail notifications Please send me notifications about responses via E-mail.

Page 5 of 5

Una volta inviata la tua segnalazione, l'applicazione genererà un nome utente e una password. **SCRIVILI E CONSERVALI IN UN POSTO SICURO.**

Ti serviranno per accedere alla tua casella di posta dove potrai seguire la tua segnalazione e ricevere feedback dall'organizzazione. Inoltre, assicurati di proteggere il tuo nome utente e password per evitare che terze parti possano scoprirli e abusarne.

You have successfully submitted your report!

Find your username and password below. Please, write them down. You can use them to access your inbox where you will be able to follow the processing of your report, securely communicate with the organization and receive its feedback. Protect the username and password from disclosure to third parties to prevent their abuse.

If you forget your username or password, you will need to submit a new report. For security reasons and protection of your anonymity, we cannot recover your username or password.

Username: XJ2949

Password: zs1hsaF

Accedere alla Tua Casella

Puoi accedere alla tua casella dalla homepage dell'applicazione cliccando sul pulsante "La tua casella".

Here you can follow the status of your report, including confirmation of its receipt, continue secure communication with and receive feedback from the organization.



Dopo aver confermato gli avvertimenti sulla sicurezza e l'elaborazione dei dati, ti verrà chiesto di effettuare l'accesso con il tuo nome utente e password che hai ricevuto dopo aver inviato la tua segnalazione.

Login

Enter your username and password into the designated fields below. If this is your first log in, use the username and password you received upon completion of the submission of your report.

Username

Password

Nella tua casella troverai informazioni sullo stato del tuo caso di segnalazione e potrai comunicare con l'organizzazione in modo sicuro e confidenziale.

Se desideri inviare un messaggio all'organizzazione, inseriscilo semplicemente nel campo di testo e fai clic sul pulsante "Invia".

Nel caso in cui inizialmente avessi deciso di rimanere anonimo, puoi rivelare la tua identità quando decidi di farlo cliccando sul link "Desidero rivelare la mia identità" in fondo alla pagina.

Follow your report

Content of the report is not shown for security reasons.

Entry date: 20.01.2022
Case status: Received

Your messages:

20.01.2022 - Demo
Please tell us more.

Your reply

I would like to add...

Prior to their attachment, check your files for metadata that may reveal your identity. We recommend sending the documents in a pdf format or in paper to the address of the organization and writing your username which will be assigned to you upon completion of your submission.

[I wish to disclose my identity](#)

Cliccando sull'icona del menu a panino nell'angolo in alto a destra della tua casella potrai cambiare la tua password. La nuova password deve avere almeno 8 caratteri.

Change password

Current password

New password

Repeat new password

