



POLICY DI WHISTLEBLOWING

Aggiornamenti al documento

Edizione	Descrizione
Dicembre 2015	Prima Adozione approvata dal Consiglio di Amministrazione con delibera del 17/12/2015
Ottobre 2018	Approvata dal Consiglio di Amministrazione con delibera del 11/10/2018
Dicembre 2023	Approvata dal Consiglio di Amministrazione con delibera del 14/12/2023
Dicembre 2024	Approvata dal Consiglio di Amministrazione con delibera del 19/12/2024

Indice e sommario

1. Premessa.....	4
2. Aggiornamento del documento	6
3. Perimetro di applicazione.....	7
4. Responsabile dei Sistemi Interni di Segnalazione.....	8
5. Processo di segnalazione	9
5.1. Processo di segnalazione interno.....	9
Canali di segnalazione interni	9
Contenuto della segnalazione.....	9
Valutazione delle segnalazioni e provvedimenti decisionali	10
5.2. Processo di segnalazione esterno	12
Segnalazioni esterne tramite il canale ANAC	12
Diffusione pubblica	12
6. Riservatezza dei dati personali del Segnalatore e del Segnalato e tutela del Segnalatore.	14
7. Conservazione della documentazione	16
8. Obblighi informativi del Responsabile dei Sistemi Interni di Segnalazione	17
9. Sanzioni.....	18
10..... Allegati	19

1. Premessa

Il 29 dicembre 2017 è entrata in vigore la Legge 179/2017 recante “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” (cd. “Legge sul *Whistleblowing*”) che consolida la disciplina esistente in materia nel settore pubblico e in quello privato, rafforzando gli strumenti a tutela dei segnalanti. Nello specifico, per il settore privato, il d.lgs. 231/2001, come successivamente modificato, prevede un apparato di misure dedicate al «Whistleblower privato» e indirizzate agli enti che abbiano scelto di adottare i Modelli Organizzativi (art. 2, Legge. 179/2017).

Il D.lgs. 24 del 10 marzo 2023 in materia di *whistleblowing*, entrato in vigore a partire dal 15 luglio 2023, introduce per gli enti privati l’obbligo (e non più la facoltà) di istituire canali di segnalazione interna in materia di *whistleblowing* e l’obbligo di introdurre strumenti approntati alla concreta tutela dei soggetti segnalanti (i “**Segnalatori**”).

Per gli enti privati, infatti, l’istituzione di tali sistemi era, sino al D.lgs. 24 del 10 marzo 2023, rimessa alla libera scelta di dotarsi di un Modello di organizzazione gestione e controllo conforme al D.Lgs.n.231/2001.

Le disposizioni relative ai meccanismi di segnalazione interna ed esterna previste dalla Legge sul *Whistleblowing* si affiancano a quanto già previsto da altre normative e previsioni regolamentari di vario rango, tra cui:

- gli articoli 52-*bis* e 52-*ter* del D.Lgs. 385/1993 (“TUB”), inseriti dall’art. 1, comma 18, del D.Lgs. 12 maggio 2015, n. 72, cui successivamente è stata data attuazione nella Circolare n. 285/2013 di Banca d’Italia “Disposizioni di vigilanza per le banche”;
- gli articoli 4-*undecies* e 4-*duodecies* del D.Lgs. 58/1998 (“TUF”), inseriti dall’art. 1 del D.Lgs. n. 129 del 3 agosto 2017;
- l’articolo 7 del Codice di Autodisciplina di Borsa Italiana S.p.A.;
- l’articolo 48 del D.Lgs. 231/2007 (modificato dal D.Lgs. 90/2017).;
- il Capo III-*bis* del D.Lgs. 7 settembre 2005, n. 209 (“Codice delle Assicurazioni Private”, modificato dal D.Lgs. 68/2018)

L’obiettivo di tali Disposizioni è quello di delineare i requisiti minimi necessari per la definizione di sistemi di *whistleblowing*, volti a consentire al Personale¹ di segnalare atti e fatti che possano costituire una violazione delle norme che regolano l’attività della Banca, garantendo la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto segnalato, ferme restando le regole che disciplinano le indagini ovvero i procedimenti avviati dall’Autorità Giudiziaria in relazione ai fatti oggetto di segnalazione.

A tale riguardo Arepo BP S.p.A. (di seguito “Arepo BP” o la “Capogruppo”), nell’esercizio del ruolo di indirizzo e coordinamento delle Società del Gruppo bancario Banca Profilo (“Gruppo”), ha definito tramite apposita Direttiva le linee guida e i criteri in materia di *whistleblowing* per il perimetro del Gruppo, pur nel rispetto dell’autonomia giuridica di ciascuna entità e tenuto conto delle specificità normative applicabili alle singole controllate.

¹ Laddove per personale si intendono “i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l’inserimento nell’organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato” (Cfr. art. art.1, comma 1, lettera i-*ter* del D.lgs. 58/1998 e art. 1, comma 2, lettera h-*novies* del D.lgs. 385/1993).

La Direttiva è stata adottata dal Consiglio di Amministrazione di Arepo BP nella seduta del 16 dicembre 2015 e recepita dal Consiglio di Amministrazione di Banca Profilo S.p.A. (di seguito “Banca Profilo” o la “Banca”) sia in sede di prima adozione, sia in sede di successive modifiche.

Il presente documento (di seguito **Policy**) è finalizzato a disciplinare il funzionamento dei Sistemi Interni ed Esterni di Segnalazione di atti e fatti che possano costituire una violazione delle norme che regolano l’attività della Banca, in conformità a quanto previsto dalle disposizioni normative sopra richiamate ed in linea con il principio di proporzionalità, e in particolare:

- definisce il perimetro di applicazione della disciplina ([Capitolo 3](#));
- identifica il Responsabile dei Sistemi Interni di Segnalazione e il suo sostituto ([Capitolo 4](#));
- delinea il processo di segnalazione interno ed esterno ([Capitolo 5](#));
- norma la riservatezza delle informazioni e la tutela del segnalatore ([Capitolo 6](#));
- tratta gli obblighi informativi e la redazione della relazione annuale del Responsabile dei Sistemi Interni di Segnalazione ([Capitolo 7](#)).

2. Aggiornamento del documento

Il presente documento ed i successivi aggiornamenti devono essere approvati dal Consiglio di Amministrazione della Banca.

Il processo di aggiornamento della policy è promosso dal Responsabile dei Sistemi Interni di Segnalazione, così come definito al successivo [Capitolo 4](#).

3. Perimetro di applicazione

Nel presente capitolo vengono identificati i soggetti che possono attivare la procedura di segnalazione interna (c.d. **Segnalatori**) e gli atti o i fatti che possono essere oggetto di segnalazione.

I **Segnalatori** sono le 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.

Rientrano nella categoria dei **Segnalatori**: il **Personale** della **Società** (inclusi ex dipendenti, parenti e "**facilitatori**"²), i **candidati** e i **tirocinanti** della **Società**, i **liberi professionisti** e i **consulenti** della **Società**, gli **Amministratori** e **Sindaci** della **Società**, i **membri della società di revisione contabile** della **Società** e, infine, **gli Azionisti** della **Società**.

Le segnalazioni presentate dai **Segnalatori** possono riguardare:

1. condotte illecite rilevanti ai sensi del D.lgs.231/2001 (per l'individuazione dei reati rilevanti ai fini del citato decreto si rinvia all'Allegato 1 del Modello di Organizzazione, Gestione e Controllo adottato dalla Banca ("MOG")) o violazioni del MOG stesso (art. 6, comma 2 *bis* del D.lgs. 231/2001);
2. atti o fatti che possono costituire una violazione delle norme disciplinanti l'attività bancaria (art. 52 *bis* e 52 *ter* del D.lgs. 385/1993 ("TUB") e delle Disposizioni di Vigilanza per le banche – Circolare 285/2013 di Banca d'Italia);
3. atti o fatti che possano costituire violazione delle norme inerenti l'attività svolta da intermediari, emittenti, nonché la disciplina del Regolamento UE 596/2014 (*Market Abuse Regulation*) (art. 4 *undecies*, comma 1 del D.lgs. 58/1998 ("TUF"));
4. violazioni potenziali o effettive delle disposizioni in materia di prevenzione di riciclaggio e del finanziamento del terrorismo (art. 48 del D.lgs. 231/2007) e atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta da imprese di assicurazione o riassicurazione, intermediari assicurativi e riassicurativi, inclusi gli intermediari assicurativi a titolo accessorio, di cui al Codice delle Assicurazioni Private (D.lgs. 209/20015)

² "Facilitatori": coloro che assistono i segnalanti nel processo di segnalazione e operanti all'interno del medesimo contesto lavorativo.

4. Responsabile dei Sistemi Interni di Segnalazione

Il Consiglio di Amministrazione di Banca Profilo individua il **Responsabile dei Sistemi Interni di Segnalazione** (o **Responsabile Whistleblowing**), secondo i criteri previsti dalla normativa applicabile³, ed in coerenza con le disposizioni emanate dalla Capogruppo per il tramite della Direttiva in materia di Whistleblowing. Nello specifico, il **Responsabile Whistleblowing** ha il compito di:

- ricevere, esaminare e valutare le segnalazioni ricevute dai **Segnalatori**;
- riferire direttamente e senza indugio ai soggetti competenti le informazioni oggetto di segnalazione, ove rilevanti;
- redigere una relazione annuale sulle attività di segnalazione interna, così come dettagliato al [Capitolo 7](#);
- verificare il corretto funzionamento delle procedure di segnalazione;
- promuovere il processo di aggiornamento della presente **Policy**.

Al fine di poter svolgere correttamente le proprie funzioni, il **Responsabile Whistleblowing** opera libero da condizionamenti e senza alcuna limitazione nello svolgimento dei propri compiti. In ordine alle segnalazioni ricevute, il **Responsabile Whistleblowing** può svolgere l'attività istruttoria in via autonoma, oppure può richiedere specifici approfondimenti ai Responsabili delle Funzioni **Internal Audit** e/o **Compliance e Antiriciclaggio**, oppure a professionisti esterni. A tal fine al Responsabile Whistleblowing è assegnato un *budget* annuale.

Il Consiglio di Amministrazione di Banca Profilo individua, inoltre, un **Responsabile Sostituto dei Sistemi Interni di Segnalazione** (o **Responsabile Sostituto**), secondo i richiamati criteri previsti dalla normativa applicabile, ed in coerenza con le disposizioni emanate dalla Capogruppo per il tramite della **Direttiva in materia di Whistleblowing**. Nello specifico, le segnalazioni devono essere inviate al **Responsabile Sostituto** nel caso in cui il **Responsabile Whistleblowing** sia il presunto responsabile della violazione ovvero abbia un potenziale interesse correlato alla segnalazione tale da compromettere l'imparzialità di giudizio ovvero il **Segnalatore** coincida con il **Responsabile Whistleblowing**. In tal caso, il **Responsabile Sostituto** esaminerà e valuterà le segnalazioni ricevute, riferendo direttamente e senza indugio ai soggetti competenti le informazioni oggetto di segnalazione, ove rilevanti.

Il Consiglio di Amministrazione di Banca Profilo dell'11 ottobre 2018 ha assegnato all'Organismo di Vigilanza la funzione **Responsabile dei Sistemi Interni di Segnalazione** (il "**Responsabile Whistleblowing**") e al Responsabile della Funzione Internal Audit la funzione di **Responsabile Sostituto dei Sistemi Interni di Segnalazione** (il "**Responsabile Sostituto**"), secondo i richiamati criteri previsti dalla normativa applicabile, e in coerenza con le disposizioni emanate dalla Capogruppo per il tramite della **Direttiva "in materia di Whistleblowing"**.

³ Nella Circolare n. 285/2013 di Banca d'Italia (Parte I, Titolo IV, Capitolo 3, Sezione VIII) è previsto che "le banche nominano un responsabile dei sistemi interni di segnalazione, il quale assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti". "Il soggetto preposto alla ricezione, all'esame e alla valutazione della segnalazione non deve essere gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato, non essere esso stesso presunto responsabile della violazione e non avere un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio".

5. Processo di segnalazione

5.1. Processo di segnalazione interno

Canali di segnalazione interni

I Segnalatori comunicano mediante il tool di segnalazione “Whistleblower Software” (di seguito il **tool di segnalazione**), attraverso il link reso disponibile sul sito di Banca Profilo Spa, al **Responsabile Whistleblowing** (ovvero, nelle sole situazioni indicate nel [Capitolo 4](#), al **Responsabile Sostituto** ()) gli eventi, indicati al precedente [Capitolo 3](#), dei quali vengano a conoscenza. Tanto il responsabile Whistleblowing quanto il responsabile sostituto sono designati con lettera di nomina quali persone autorizzate al trattamento dei dati personali e sensibili di cui verranno a conoscenza.

Le segnalazioni effettuate per mezzo del **tool di segnalazione**, possono essere effettuate sia in forma anonima che in forma confidenziale (non anonima); sono garantiti specifici presidi di riservatezza dell’identità del segnalante nelle diverse fasi di gestione della segnalazione, così come indicato al successivo [Capitolo 6](#).

È altresì possibile effettuare segnalazioni al **Responsabile Whistleblowing** in forma orale, attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta dei **Segnalatori**, mediante un incontro diretto con il **Responsabile Whistleblowing** fissato entro un termine ragionevole oppure registrare direttamente nel **tool di segnalazione** un messaggio vocale che a discrezione del segnalante può essere anche criptato per garantire la totale riservatezza ed anonimato

In via residuale, è possibile far pervenire al **Responsabile Whistleblowing** ovvero, nelle sole situazioni indicate nel [Capitolo 4](#), al **Responsabile Sostituto**, segnalazioni anonime e/o confidenziali, tramite lettera raccomandata. In vista della protocollazione riservata della segnalazione, è necessario che la segnalazione venga inserita in due buste chiuse: la prima con i dati identificativi del segnalante unitamente alla fotocopia del documento di riconoscimento; la seconda con la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all’esterno la dicitura “riservata” al gestore della segnalazione (ad es. “riservata al RPCT”).

Tutte le modalità alternative all’utilizzo del **tool di segnalazione** possono essere integrate all’interno dello stesso mediante apposita funzione, disponibile ai gestori delle segnalazioni, che consente di inserire manualmente segnalazioni pervenute attraverso canali differenti dal **tool di segnalazione** stesso.

Si evidenzia che, al fine di facilitare la verifica della fondatezza delle segnalazioni anonime, è necessario che le stesse vengano documentate adeguatamente ovvero che vengano redatte con dovizia di particolari e siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati. I

Contenuto della segnalazione

Le segnalazioni devono essere complete degli elementi utili alla ricostruzione dei fatti. A tal fine, ogni segnalazione (sia anonima che confidenziale) deve contenere i seguenti elementi:

- in caso di segnalazione confidenziale (non anonima), generalità del **Segnalatore** (l'identità sarà nota solo al personale incaricato di gestire la segnalazione), , con indicazione della società associata alla segnalazione e dei propri recapiti;
- circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- chiara e completa descrizione dei fatti oggetto di segnalazione e pertinente indicazione della categoria associata alla segnalazione;
- generalità o altri elementi che consentano di identificare il/i soggetto/i che ha/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 utile a ricostruire i fatti segnalati.

In aggiunta a quanto sopra, in caso di segnalazione confidenziale, il **Segnalatore** deve specificare se acconsente o meno a rivelare la propria identità ai soggetti coinvolti nel processo di segnalazione (il consenso alla trasparenza verrà richiesto solo se necessario all'elaborazione interna della segnalazione). Si rammenta che tutti i dettagli inerenti la riservatezza dei dati personali sono riportati al [Capitolo 6](#).

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

Il **Segnalatore** è inoltre obbligato a dichiarare se ha un interesse privato collegato alla segnalazione ovvero se sia corresponsabile delle violazioni. In quest'ultimo caso, si evidenzia che le strutture e gli organi ai quali competono le valutazioni disciplinari garantiranno a quest'ultimo un trattamento privilegiato rispetto agli altri corresponsabili, compatibilmente con la disciplina applicabile.

Si precisa, infine, che non devono essere oggetto di segnalazione le doglianze di carattere personale del **Segnalatore** o rivendicazioni ed istanze che attengono alla disciplina del rapporto di lavoro o ai rapporti con il superiore gerarchico o i colleghi, per le quali occorre fare riferimento alla **Funzione Risorse Umane e Welfare** e le doglianze in materia di sicurezza e difesa nazionale.

Valutazione delle segnalazioni e provvedimenti decisionali

Una volta ricevuta la segnalazione, il **Responsabile Whistleblowing** (ovvero il **Responsabile Sostituto**), gestisce la stessa mediante il Tool di segnalazione e provvederà ad inviare automaticamente al Segnalante tutti gli aggiornamenti e le modifiche di stato intercorrenti. Per ogni caso sono previste due scadenze. La prima avviene tra la creazione di un caso e la sua ricezione dopo 7 giorni. La seconda scadenza è tra la ricezione di un caso e la chiusura, prevista entro 90 giorni.

Per verificare la fondatezza dei fatti denunciati il **Responsabile Whistleblowing** (ovvero il **Responsabile Sostituto**) può avvalersi di tutti i mezzi ritenuti necessari e, se lo ritiene opportuno, può sentire in audizione i colleghi diversi dal **Segnalatore**, ove noto, e dal **Segnalato** e/o personale esterno alla Banca ed è tenuto ad annotare e ad archiviare le informazioni e i documenti acquisiti. Il **Responsabile Whistleblowing** mantiene le interlocuzioni con il **Segnalatore** e può richiedere a quest'ultimo, attraverso il **Tool di segnalazione**, delle integrazioni informative o documentali

Nel caso di infondatezza, il **Responsabile Whistleblowing** (ovvero il **Responsabile Sostituto**) comunica l'esito motivato e la conclusione del procedimento al **Segnalatore** mediante il Tool di segnalazione

Qualora, invece, dall'esito della verifica, la segnalazione risulti fondata, il **Responsabile Whistleblowing** (ovvero il **Responsabile Sostituto**) ne valuta la gravità e procede ad informare il **Segnalatore**, ove noto, il **Segnalato**, il **Responsabile gerarchico del Segnalato**, il **Responsabile della Funzione Risorse Umane**, l'**Amministratore Delegato** e **Direttore Generale**, nonché l'**Organismo di Vigilanza** in caso di reati rilevanti ai fini della responsabilità prevista dal D.Lgs. n. 231/2001, se diverso dal **Responsabile Whistleblowing**.

Per valutare la "gravità" della segnalazione il **Responsabile Whistleblowing** (ovvero il **Responsabile Sostituto**) può considerare, a titolo esemplificativo, i seguenti elementi soggettivi e oggettivi:

- la posizione ricoperta dal soggetto **Segnalato** e la durata della carica;
- la negligenza professionale del soggetto **Segnalato** e se essa è imputabile a titolo di colpa o dolo;
- la rilevanza delle carenze riscontrate in relazione agli interessi protetti dalla norma violata;
- la durata della violazione e l'eventuale reiterazione della condotta posta in essere in violazione delle norme;
- le azioni poste in essere dal soggetto **Segnalato** per eliminare o attenuare le conseguenze della violazione.

Nei casi in cui si siano verificate violazioni di particolare gravità, il **Responsabile Whistleblowing** (ovvero il **Responsabile Sostituto**) provvede inoltre ad informare immediatamente il **Consiglio di Amministrazione**, l'**Organismo di Vigilanza** (se diverso dal Responsabile Whistleblowing) ed il **Comitato Controllo e Rischi**.

I provvedimenti disciplinari vengono valutati e adottati dall'**Amministratore Delegato** di concerto con il **Responsabile delle Risorse Umane e Welfare Aziendale** e dei Responsabili delle Funzioni di volta in volta pertinenti, nel rispetto dei principi che guidano il sistema disciplinare delineato nel Modello di Organizzazione, Gestione e Controllo adottato dalla Banca.

I provvedimenti disciplinari adottati vengono comunicati al **Responsabile Whistleblowing** (ovvero al **Responsabile Sostituto**).

Il **Responsabile Whistleblowing** è tenuto a mantenere i contatti con il **Segnalatore**, dando seguito alla segnalazione e fornendogli riscontro entro tre mesi dalla data di ricezione di quest'ultima.

Le segnalazioni ricevute, la documentazione esaminata, le informazioni e gli atti acquisiti in audizione, sono conservati, a cura del **Responsabile Whistleblowing**, ovvero, nei casi previsti, a cura del **Responsabile Sostituto**, secondo le modalità previste nel successivo paragrafo "**Conservazione della documentazione**".

5.2. Processo di segnalazione esterno

Oltre al processo di segnalazione interno, sono previsti specifici processi di segnalazione esterni.

Segnalazioni esterne tramite il canale ANAC

I **Segnalatori** possono altresì inviare una segnalazione esterna all'**ANAC** (Autorità Nazionale Anti Corruzione), seguendo le Linee Guida adottate dall'**ANAC** stessa visionabili presso il sito internet della citata Autorità (<https://www.anticorruzione.it/-/del.311.2023.linee.guida.whistleblowing>), quando essi:

- operano in un contesto lavorativo nel quale non è prevista l'attivazione obbligatoria del canale o la sua predisposizione non è conforme ai requisiti normativi;
- hanno già effettuato una segnalazione a cui non è stato dato seguito;
- hanno fondato motivo di ritenere che una segnalazione interna possa determinare il rischio di ritorsione;
- hanno fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le segnalazioni esterne sono effettuate in forma scritta tramite la piattaforma informatica oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta dei **Segnalatori**, mediante un incontro diretto fissato entro un termine ragionevole.

La segnalazione esterna presentata ad un soggetto diverso dall'**ANAC** è trasmessa a quest'ultima, entro 7 giorni lavorativi dalla data del suo ricevimento, dando contestuale notizia della trasmissione ai **Segnalatori**.

L'**ANAC** rappresenta un canale di comunicazione indipendente e autonomo, ad ulteriore garanzia dell'efficacia della disciplina e di tutela dei **Segnalatori**.

Anche l'**ANAC** ha specifici doveri di attivazione e di riscontro nei confronti dei **Segnalatori**, secondo le tempistiche e le modalità previste dal successivo paragrafo "[Valutazione delle segnalazioni e provvedimenti decisionali](#)".

Diffusione pubblica

È prevista l'ulteriore possibilità di segnalare gli illeciti mediante delle **divulgazioni pubbliche** tramite i mass media che possono essere effettuate solo al ricorrere di specifici presupposti.

I **Segnalatori** possono dunque utilizzare la stampa e mezzi elettronici, o comunque di diffusione in grado di raggiungere un numero elevato di persone.

L'utilizzo di tali strumenti risulta valido qualora si siano precedentemente effettuate una segnalazione interna e una esterna (o direttamente una segnalazione esterna) oppure si abbia fondato motivo di ritenere che:

- la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;

- la segnalazione esterna possa comportare ritorsioni o non avere efficace seguito.

6. Riservatezza dei dati personali del Segnalatore e del Segnalato e tutela del Segnalatore

I soggetti che ricevono, esaminano e valutano le segnalazioni e ogni altro soggetto coinvolto nella procedura, devono garantire, in ogni caso, la riservatezza delle informazioni acquisite e che il trattamento dei dati personali del **Segnalatore** del soggetto **Segnalato** avvenga nel rispetto delle previsioni della normativa applicabile e delle disposizioni contenute nel **Vademecum del dipendente** e nella **Carta dei principi e codice di comportamento** e all'informativa sul trattamento dei dati personali da fornire al segnalante e al segnalato (Appendice 1)..

L'utilizzo del tool di segnalazione "Whistleblower Software", anche in forma confidenziale, prevede che il Segnalatore e la segnalazione siano registrati e posti sotto la tutela della legislazione in materia della protezione degli informatori sin dal primo contatto effettuato. Il software utilizza dati crittografati e crittografia end-to-end: tutti i dati vengono crittografati sia quando sono in transito che a riposo. Questo assicura:

1. l'integrità dei dati, in quanto i dati non possono essere corrotti o modificati durante il trasferimento,
2. la privacy, in quanto i dati non possono essere intercettati da terze parti, e
3. l'autenticazione, in quanto l'utente finale può essere certo che il sito a cui si collega sia effettivamente Whistleblower Software by Formalize

Il **Segnalatore** è protetto dal divieto di atti di ritorsioni, anche indiretti, nei suoi confronti, tra i quali si segnalano in particolare i seguenti: licenziamento, sospensione, retrocessione di grado o mancata promozione, demansionamento, cambiamento del luogo o dell'orario di lavoro, riduzione dello stipendio, referenze negative, misure disciplinari o sanzioni pecuniarie, intimidazioni o molestie e danni reputazionali.

Sul soggetto che abbia posto in essere condotte ritorsive, discriminatorie o comunque sleali nei confronti del **Segnalatore**, grava l'inversione dell'onere probatorio che gli impone di dimostrare che tali condotte siano state attuate per ragioni estranee alla segnalazione, alla divulgazione o alla denuncia.

I provvedimenti assunti nei confronti del **Segnalatore** in violazione del divieto di ritorsione sono nulli; il **Segnalatore** che sia stato licenziato a causa della segnalazione, della divulgazione pubblica o della denuncia all'Autorità giudiziaria o contabile ha diritto ad essere reintegrato nel posto di lavoro

L'identità del **Segnalatore** non può essere rivelata, se non con l'esplicito consenso dello stesso, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati, raccolto tramite apposito modulo (Appendice 2 - Modulo per la raccolta del consenso del segnalante).

Nel caso di segnalazioni che abbiano comportato l'instaurazione di un procedimento penale, la riservatezza del **Segnalatore** è tutelata nei limiti previsti dall'art. 329 c.p.p..

E' esclusa la responsabilità del **Segnalatore** nel caso in cui diffonda o riveli, attraverso i canali di segnalazione interni o esterni, informazioni coperte dall'obbligo di segreto relative alla tutela del diritto d'autore o alla protezione dei dati personali, a condizione che vi sia il fondato motivo di ritenere che la rivelazione di tali informazioni fosse necessaria per svelare la violazione.

La violazione dell'obbligo di riservatezza, inclusa la divulgazione di informazioni in base a cui l'identità del **Segnalatore** si possa dedurre, è considerata una violazione della presente **Policy** ed è fonte di responsabilità disciplinare.

I dati personali del **Segnalatore** e del soggetto **Segnalato** saranno trattati unicamente dal **Responsabile Whistleblowing** (ovvero dal **Responsabile Sostituto**) e non dagli addetti delle rispettive Funzioni. In particolare, il Titolare del Trattamento dei dati personali è Banca Profilo mentre il Responsabile è individuato nell'Organismo di Vigilanza.

7. Conservazione della documentazione

Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre **5 anni** a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione; i dati vengono cancellati automaticamente trascorso questo periodo temporale.

Se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, compresa la registrazione vocale direttamente nel tool di segnalazione, la segnalazione, previo consenso del **Segnalatore**, è documentata a cura del **Responsabile Whistleblowing** mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto, mediante trascrizione integrale

Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato, la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del **Responsabile Whistleblowing** che provvede anche ad integrarla manualmente all'interno del tool di segnalazione per garantire la riservatezza del segnalante in tutti i passaggi successivi, e le corrette modalità di conservazione dei dati

Quando, su richiesta del **Segnalatore**, la segnalazione è effettuata oralmente nel corso di un incontro con il **Responsabile Whistleblowing**, essa, previo consenso del **Segnalatore**, è documentata a cura del **Responsabile Whistleblowing** mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale ed opportunamente integrata manualmente all'interno del tool di segnalazione come già indicato in precedenza.

8. Obblighi informativi del Responsabile dei Sistemi Interni di Segnalazione

Il **Responsabile Whistleblowing** riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti.

Nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali, il **Responsabile Whistleblowing** redige annualmente una relazione sul corretto funzionamento dei sistemi interni di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute.

Tale relazione viene sottoposta all'approvazione del **Consiglio di Amministrazione**, sentito il **Comitato Controllo e Rischi**, entro il 31 marzo di ogni anno, ed inviata alla Capogruppo per informativa nonché messa a disposizione al personale della Banca sulla *Intranet Aziendale* (**Documentazione > Banca Profilo > Disposizioni Interne > Whistleblowing**).

9. Sanzioni

Oltre ai profili di responsabilità in cui può incorrere il soggetto segnalato, è previsto un regime sanzionatorio applicabile nei casi in cui vengano riscontrate violazioni in materia di *whistleblowing*.

In particolare, l'**ANAC** può infliggere al responsabile delle sanzioni amministrative pecuniarie qualora:

- siano state commesse delle ritorsioni, o qualora si accerti che la segnalazione sia stata ostacolata o che l'obbligo di riservatezza sia stato violato;
- non siano stati istituiti canali di segnalazione, non siano state adottate procedure per l'effettuazione e la gestione delle segnalazioni, oppure l'adozione di tali procedure non sia conforme alla normativa.

Al **Segnalatore** che abbia effettuato segnalazioni diffamatorie o calunniose, commesse con dolo o colpa grave, è irrogata una sanzione disciplinare quando viene accertata, anche con sentenza di primo grado, la responsabilità penale del **Segnalatore**.

10. Allegati

Di seguito si descrivono i contenuti delle appendici al presente Regolamento che sono riportati in un documento a parte.

Appendice 1 - Informativa sul trattamento dei dati personali da fornire al segnalante e al segnalato

Appendice 2 - Modulo per la raccolta del consenso del segnalante

Si tratta del modulo per la raccolta del consenso del segnalante alla rivelazione della sua identità, nei casi in cui la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato nell'ambito del procedimento disciplinare. La scansione di tale modulo viene caricata manualmente nel tool di segnalazione, ad integrazione delle informazioni già presenti.