POLICY IN MATERIA DI SEGNALAZIONE INTERNA DELLE VIOLAZIONI

WHISTLEBLOWING

Sommario

1 PREMESSA

La Banca di Cividale S.p.A. (di seguito, per brevità, anche "la Banca") ha sviluppato al proprio interno un sistema di segnalazione delle violazioni, alternativo alle ordinarie linee di *reporting* che rappresenta un utile campanello di allarme finalizzato ad intraprendere le misure appropriate per mantenere integra la reputazione aziendale.

La Banca si impegna a diffondere e ad incentivare presso tutti i soggetti interessati la cultura e l'utilizzo del sistema di segnalazione interna (*whistleblowing*) attraverso una capillare diffusione della normativa aziendale in cui si illustra il procedimento di segnalazione adottato e i presidi posti a garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione.

Il presente documento rappresenta pertanto un punto di riferimento volto a rimarcare la possibilità da parte di tutti i dipendenti di segnalare in totale sicurezza e sotto le dovute tutele legate alla riservatezza, comportamenti illeciti che possano costituire una violazione delle norme disciplinanti l'attività bancaria di cui sono venuti a conoscenza.

2. SCOPO DEL DOCUMENTO

Il presente documento descrive le procedure che la Banca ha posto in atto per la gestione dei sistemi di segnalazione interna (c.d. *whistleblowing*) che coinvolgano a livello trasversale tutte le funzioni aziendali e per identificare un sistema di regole che permetta la prevenzione e la correzione di atti o fatti che possono costituire una violazione delle norme disciplinanti l'attività della Banca, mettendo altresì i dipendenti nella condizione di comunicare senza ostacoli con gli organi aziendali preposti in caso di segnalazione di eventuali condotte illecite.
La Policy fornisce indicazioni riguardo a:

- i soggetti abilitati ad effettuare le segnalazioni;
- l'oggetto e i contenuti della segnalazione;
- i soggetti responsabili dei sistemi interni di segnalazione delle violazioni, i soggetti preposti alla ricezione e all'esame delle segnalazioni e le funzioni aziendali coinvolte;
- i canali di comunicazione e le modalità che consentono un adeguato svolgimento delle procedure di *whistleblowing,* permettendo un appropriato invio e una conseguente corretta ricezione, analisi e valutazione delle segnalazioni di comportamenti contrari alle norme disciplinanti l'attività bancaria;
- fasi e tempi di svolgimento del processo di gestione delle segnalazioni;
- le forme di tutela nei confronti dei soggetti segnalanti, al fine di evitare possibili condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione, nonché le modalità di informazione al segnalato.

3. NORMATIVA DI RIFERIMENTO

Di seguito viene riepilogata la normativa di riferimento della presente Policy:

- L'art. 52 bis del D. Lgs. 1° settembre 1993, n. 385 - Testo unico delle leggi in materia bancaria e creditizia (TUB) – ha recepito le disposizioni della direttiva CRD IV in materia di obblighi per le banche di dotarsi di sistemi interni di segnalazione delle violazioni (c.d. procedure di Whistleblowing). Banca d'Italia ha dato attuazione al predetto articolo attraverso l'11° aggiornamento della Circolare n. 285 – "Sistema dei controlli interni, Sistema informativo, Continuità operativa e Governo e gestione del rischio di liquidità" – del 21 luglio 2015.
- Il D. Lgs. 25 maggio 2017, n. 90 di recepimento della Quarta Direttiva Antiriciclaggio (Direttiva 2015/849/UE) è intervenuto a riformare e integrare il D. Lgs. 21 novembre 2007, n. 231 concernente la prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento al terrorismo. In particolare, con l'art. 48 del novellato D. Lgs. 231/2007 è stato introdotto l'obbligo di adottare procedure per la segnalazione, da parte di dipendenti o di persone in posizione comparabile, di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo (c.d. "Whistleblowing").

- Le Società che hanno adottato il modello di organizzazione, di gestione e controllo ai sensi del D. Lgs. 8 giugno 2001, n. 231 provvedono a ricomprendere la presente Policy nell'ambito del Modello, ai sensi di quanto previsto all'articolo 6, comma 2 bis del Decreto stesso, come modificato dalla Legge 30 novembre 2017, n. 179.
- Il D. Lgs. 21 maggio 2018, n. 68, di recepimento della Direttiva sulla distribuzione assicurativa – IDD (Direttiva UE 97/2016), ha introdotto nel Codice delle Assicurazioni Private (D. Lgs. 7 settembre 2005, n. 209), il nuovo art. 10 quater che prevede in capo alle imprese di assicurazione e agli intermediari assicurativi, compresi quelli accessori, l'obbligo di adottare procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire violazione delle norme disciplinanti l'attività assicurativa (c.d. procedure di Whistleblowing).
- L'art. 4 undecies D. Lgs. 24 febbraio 1998, n. 58 ha stabilito che i soggetti di cui alle parti II [intermediari] e III [disciplina dei mercati] adottano procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta, nonché del Regolamento (UE) n. 596/2014 (c.d. MAR).

Inoltre, la procedura di whistleblowing è prevista anche da normative non rientrati nello specifico perimetro dell'attività bancaria, quali:

- il D. Lgs. 81/2008, Testo Unico in materia di sicurezza;
- il D. Lgs. 196/2003, Codice in materia di protezione dei dati personali;
- il Codice di autodisciplina di Borsa Italiana;
- il D. Lgs. 165/2001, Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, aggiornato alla Legge 30 novembre 2017, n. 179 "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".

4. SOGGETTI ABILITATI AD EFFETTUARE LE SEGNALAZIONI

Il *whistleblower* è qualsiasi soggetto dipendente di un'organizzazione pubblica o privata che nel corso della propria attività lavorativa, venendo a conoscenza di un illecito o di un'irregolarità sul luogo di lavoro, decide di segnalare i fatti e/o gli atti di cui è venuto a conoscenza, attraverso l'utilizzo di canali protetti e specificatamente dedicati a tale categoria di denunce.

Tutto il personale della banca è abilitato ad effettuare segnalazioni[1].
Per personale si intende "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", ai sensi di quanto previsto dall'art. 1, comma 1, lettera h*novies* del Testo Unico Bancario.

Anche i soggetti terzi sono abilitati ad effettuare le segnalazioni. All'interno di tale categoria rientrano i clienti, i fornitori, i partner, i consulenti, i soci, nonché tutti coloro che a qualsiasi titolo collaborano con la Banca.

[1] Il personale potenzialmente abilitato ad effettuare le segnalazioni è definito di seguito anche "segnalante".

5. OGGETTO E CONTENUTI DELLA SEGNALAZIONE

5.1 Oggetto della segnalazione

Si premette che, essendo estremamente ampio l'ambito delle segnalazioni delle violazioni previsto dalla normativa in oggetto, risulta particolarmente complesso in questa sede redigere una lista tassativa ed esaustiva di reati o irregolarità che possono costituire l'oggetto dell'attività di *whistleblowing*.

Vengono, infatti, considerate rilevanti le segnalazioni di tutti quei comportamenti illegittimi, attivi od omissivi, verificatisi nello svolgimento dell'attività lavorativa, che possano essere perniciosi o pregiudizievoli per la Banca o per i suoi dipendenti e che:

- siano illeciti, scorretti o immorali;
- violino le disposizioni normative e regolamentari; o
- non siano conforme alle normative interne.

Si precisa che non possono costituire oggetto di segnalazione nel perimetro *whistleblowing* altri ambiti non interessati dalla normativa disciplinante l'attività bancaria, tra cui a titolo di esempio:

- meri sospetti o voci;
- eventuali inefficienze organizzative;
- rimostranze di carattere personale del segnalante o richieste che attengono alla disciplina del rapporto di lavoro o ai rapporti col superiore gerarchico o colleghi, per le quali occorre fare riferimento al competente Ufficio del Personale.

5.2 Contenuto della segnalazione

La segnalazione consente di portare all'attenzione dei soggetti e degli organi competenti le violazioni della normativa di cui il Segnalante sia venuto a conoscenza.

Al fine di consentire ai soggetti e/o agli organi preposti di procedere alle opportune analisi e verifiche, il *segnalante* è tenuto a fornire tutti gli elementi utili a circoscrivere il più possibile l'ambito della segnalazione e a riscontrare la fondatezza dei fatti oggetto di segnalazione.

A tal riguardo, la segnalazione deve contenere i seguenti elementi:

- le generalità del soggetto che effettua la segnalazione;
- descrizione chiara e completa degli atti o fatti oggetto di segnalazione;
- se conosciute, le generalità, la qualifica e/o il ruolo che permettano di identificare il/i soggetto/i che hanno posto in essere i fatti;
- le circostanze di luogo e di tempo in cui sono state commesse le violazioni;
- l'inoltro di eventuali documenti che possano ulteriormente circoscrivere e/o confermare i fatti segnalati;
- la dichiarazione al Responsabile dei sistemi interni di segnalazione delle violazioni riguardo un suo eventuale interesse privato collegato agli atti o ai fatti comunicati tramite la segnalazione;
- dichiarazione di eventuali corresponsabilità riguardo alla violazione segnalata; • qualsiasi altra informazione utile al riscontro della fondatezza dei fatti segnalati.

6. SOGGETTI PREPOSTI E MODALITA' DI SEGNALAZIONE DELLE VIOLAZIONI

6.1 Soggetto preposto alla ricezione e all'analisi della segnalazione

L'attività di ricezione, esame e valutazione delle segnalazioni è affidata al Responsabile della Funzione Internal Audit (di seguito, per brevità, Responsabile IA).

Tale attività include, in particolare, il compito di:

- monitorare costantemente i canali di comunicazione attivati per l'inoltro delle segnalazioni;
- effettuare l'esame preventivo di verifica sulla ricevibilità formale delle segnalazioni;
- inoltrare le segnalazioni al Responsabile (vedi punto 6.2) con gli esiti delle analisi svolte inclusa l'eventuale proposta di archiviazione ove le stesse venissero ritenute irricevibili o palesemente infondate;
- effettuare, nel caso in cui la segnalazione non venisse archiviata, la valutazione di merito della stessa, disponendo le necessarie azioni di accertamento dei fatti descritti, nel rispetto del principio di imparzialità e riservatezza, nonché nel rispetto della normativa in tema di protezione dei dati personali, dei principi di legge in materia del lavoro e della disciplina contrattuale di settore;
- al termine delle attività di analisi, sottopone al Responsabile del Sistema di segnalazione interna (vedi punto 6.2) l'esito delle risultanze ottenute per le decisioni conseguenti.

Qualora la segnalazione sia stata ritenuta ricevibile ed idonea ad essere trasmessa, il Responsabile IA si occupa di verificare se sussistono eventuali conflitti di interesse che lo coinvolgono o riguardano la struttura dallo stesso coordinata. In caso di esito positivo, provvederà all'inoltro immediato della stessa all'Organismo di Vigilanza, specificando tale circostanza.

Nel caso di assenze prolungate e non programmate (es: per malattia) del Responsabile Internal Audit, l'ODV, può individuare un altro soggetto ad accedere con l'utenza di gestione delle segnalazioni. Di tale evenienza viene data opportuna informazione al Responsabile Internal Audit. Solo in tali casi il Responsabile IT, previamente informato dall'ODV, è autorizzato a contattare formalmente l'ousoucer della piattaforma di segnalazione "Comunica Whistleblowing" per l'attivazione del sostituto.

L'utenza e password del soggetto abilitato in sostituzione del responsabile Internal Audit viene prontamente disabilitata al rientro del Suddetto Responsabile

6.2 Responsabile dei sistemi interni di segnalazione delle violazioni

La Banca individua nell'Organismo di Vigilanza istituito ai sensi del DLgs 231/2001, (di seguito anche ODV) il soggetto Responsabile dei sistemi interni di segnalazione delle violazioni (di seguito anche solo "Responsabile" o "ODV").

Il "Responsabile", avvalendosi del supporto del Responsabile IA e con le modalità ivi previste e anche tramite l'applicativo informatico dedicato di cui al paragrafo seguente:

- assicura il corretto svolgimento della procedura di *whistleblowing*, garantendo che le attività di istruttoria delle segnalazioni svolte dal Responsabile IA avvengano nel rispetto dei criteri di correttezza e riservatezza;
- riceve, analizza e valuta le segnalazioni provenienti dai segnalanti;
- richiede al segnalante di comunicare espressamente e obbligatoriamente se ha un interesse privato collegato alla segnalazione;
- sulla scorta dell'analisi compiuta dal Responsabile IA, decide riguardo all'archiviazione ovvero alla trasmissione alle fasi successive della segnalazione;
- informa, nell'ambito delle sue mansioni, il segnalante e, qualora sia ritenuto necessario, il segnalato sugli sviluppi del procedimento, nel pieno rispetto delle tutele che la normativa sul *whistleblowing* attribuisce ai soggetti coinvolti;
- riferisce direttamente agli organi aziendali le informazioni contenute all'interno della segnalazione, qualora il contenuto della stessa sia ritenuto particolarmente rilevante;
- redige una relazione annuale contenente le informazioni principali sul funzionamento della procedura di allerta interna nonché sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute;
- si assicura che gli organi aziendali approvino e mettano a disposizione del personale della banca la relazione di cui al precedente punto.

In caso di violazioni di particolare gravità il "Responsabile" provvederà ad informare tempestivamente il Presidente del Consiglio di Amministrazione, anche ai fini dell'eventuale inoltro alle Autorità competenti.

6.3 Applicativo informatico per la segnalazione delle violazioni

Al fine di conformarsi alle disposizioni in materia di sistemi interni di segnalazione delle violazioni, la Banca ha individuato l'applicativo "*Comunica Whistleblowing*" di Unione Fiduciaria quale procedura informatica finalizzata alla gestione degli stessi.
Tale applicativo costituisce un canale di comunicazione specifico, autonomo e indipendente dalle ordinarie linee di reporting, volto alla ricezione delle segnalazioni e alla corretta gestione dei flussi informativi ad esse collegati. In particolare, è volto alla gestione delle attività legate all'intero processo di segnalazione, tra cui si elencano le seguenti:

- gestione anonima delle informazioni;
- tutela del soggetto segnalante;
- informativa al soggetto segnalante e segnalato; • fase di istruttoria successiva alla segnalazione;
- inoltro di allegati e documenti.

6.4 Altri canali di comunicazione

La Banca, nell'ambito della sua autonomia organizzativa e secondo le proprie reali esigenze, ha inoltre attivato ulteriori canali di comunicazione al fine di attribuire maggiori possibilità di scelta al soggetto segnalante:

- via posta elettronica, all'indirizzo odv@civibank.it
- via posta ordinaria, all'indirizzo
- *Banca di Cividale / ODV- Riservta/ Via G.Pelizzo 8/1 33043 Cividale del Friuli UD*

Nel caso di posta ordinaria questa non dovrà essere aperta in nessun caso da alcun dipendente ed il personale incaricato dovrà consegnarla al Responsabile dell'Internal Audit che avrà cura di recapitarla integra direttamente all'ODV

Tramite tali canali potrà in particolare essere inoltrata una richiesta diretta del segnalante al "Responsabile" per un colloquio confidenziale diretto e relativa verbalizzazione dello stesso.

6.5 Identità ed obblighi del segnalante

La procedura adottata dalla Banca garantisce la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione a fatti oggetto delle segnalazioni.
L'identità del segnalante deve essere protetta in ogni fase e contesto successivo alla segnalazione, ad eccezione del caso in cui l'anonimato non sia opponibile per legge, quando le informazioni richieste sono necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione. L'identità del segnalante può essere conosciuta dal

Responsabile del sistema di segnalazione interna e dai soggetti preposti alle attività istruttorie conseguenti alla segnalazione.

Pertanto, fatte salve le eccezioni di cui sopra, l'identità del segnalante non può essere rivelata, e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione.

Il soggetto segnalante è obbligato a dichiarare al "Responsabile" un suo eventuale interesse privato collegato agli atti o ai fatti comunicati tramite la segnalazione.

7. FASI E TEMPI DI SVOLGIMENTO DEL PROCESSO DI GESTIONE DELLE SEGNALAZIONI

Il Processo di gestione delle segnalazioni è distinto nelle seguenti fasi:

1. ricezione della segnalazione da parte del Responsabile dell'IA o suo delegato;
2. analisi e gestione della segnalazione, ossia:
   2.1 esame della segnalazione sotto il profilo della ricevibilità formale della stessa, intesa come coerenza rispetto agli ambiti disciplinati dalla presente Policy;
   2.2 valutazione del merito della segnalazione;
   2.3 decisioni conseguenti all'esito della valutazione, ovvero:
      2.3.1 archiviazione nel caso di accertata insussistenza delle irregolarità segnalate;
      2.3.2 inoltro all'Organismo di Vigilanza ove si rilevi la fondatezza della segnalazione per le valutazioni di competenza;
      2.3.3 L'OdV esamina e valuta i risultati dell'istruttoria e le azioni successive (sia finalizzate a procedere con l'iter disciplinare o eventuali informative al Consiglio di Amministrazione); indica alle competenti strutture aziendali la necessità di avviare un iter disciplinare relativamente al soggetto segnalato qualora vi siano i presupposti ad esito dell'istruttoria.

Qualora la segnalazione riguardi il Responsabile IA o la struttura dallo stesso coordinata o siano ravvisati eventuali potenziali conflitti di interesse correlati alla segnalazione tali da comprometterne l'imparzialità e l'indipendenza di giudizio, il segnalante può rivolgersi direttamente, all'ODV, specificando tale circostanza, utilizzando i seguenti canali:

- posta elettronica, scrivendo all'indirizzo: odv@civibank.it;
- posta ordinaria, scrivendo all'indirizzo:

Banca di Cividale/ODV Riservata/ Via G. Pelizzo 8/1- 33043 Cividale del Friuli (UD)

Nel caso di posta ordinaria questa non dovrà essere aperta in nessun caso da alcun dipendente ed il personale incaricato dovrà consegnarla al Responsabile dell'Internal Audit che avrà cura di recapitarla integra direttamente all'ODV.

I tempi di lavorazione, avendo a riferimento il processo sopra descritto, sono i seguenti:

- l'esame della ricevibilità formale e la valutazione del merito della segnalazione dovranno essere svolte entro 30 giorni dal ricevimento della stessa, salvo proroga , per giustificato motivo, di ulteriori 15 giorni;
- il termine per la conclusione del procedimento e chiusura con eventuale inoltro alle funzioni competenti per le eventuali decisioni conseguenti all'esito della valutazione viene fissato in 120 giorni di calendario, dalla data del ricevimento della segnalazione, fatta salva la proroga dei termini se l'accertamento risulta particolarmente complesso.

È prevista una deroga al processo suddetto con possibilità di porre in essere una o più proroghe in presenza di motivate ragioni che rendano necessario il prolungamento dei tempi di lavorazione.

8. FORME DI TUTELA E INFORMATIVA AI SOGGETTI SEGNALANTI E SEGNALATI

8.1 Protezione del soggetto segnalante

Il segnalante, nell'ambito della propria attività di segnalazione, non subirà condotte ritorsive, discriminatorie o comunque sleali conseguenti, direttamente o indirettamente, la segnalazione medesima (a titolo di esempio: licenziamento, demansionamento, *mobbing*, ecc.) e potrà richiedere il trasferimento in altro ufficio. La Banca si impegna a garantire, laddove ragionevolmente opportuno, il soddisfacimento della predetta richiesta.

Ove il segnalante abbia dichiarato la propria corresponsabilità nel fatto oggetto della segnalazione, la Banca gli riserverà un trattamento privilegiato rispetto agli altri corresponsabili, compatibilmente con la normativa applicabile al caso in specie.

La Banca assicura che il segnalante, anche nel caso in cui la segnalazione da questi effettuata dovesse risultare infondata, non sarà oggetto di azione disciplinare, tranne nei casi in cui la segnalazione stessa sia avvenuta per dolo e/o colpa grave.

La Banca garantisce la riservatezza del segnalante e la confidenzialità delle informazioni ricevute. Costituiscono eccezione i casi in cui la loro divulgazione:

- sia richiesta dalla normativa nazionale (ad esempio, se sia necessaria perché richiesta dall'Autorità giudiziaria o risulti indispensabile per garantire la difesa del segnalato);
- sia necessaria per prevenire o ridurre danni di particolare gravità alla salute o della sicurezza delle persone.

È vietata, fuori dai casi sopra elencati, la divulgazione dell'identità del segnalante ovvero di informazioni contenute nella segnalazione.

8.2 Informazioni al soggetto segnalante

La Banca si impegna ad informare tempestivamente il segnalante, entro un termine ragionevolmente breve dal momento della ricezione della segnalazione, riguardo l'avvenuta ricezione e la presa in carico della segnalazione medesima.
Inoltre, tiene lo stesso informato, non appena possibile e a prescindere dall'esito delle verifiche svolte, sugli sviluppi del procedimento posto in essere, inclusa la decisione di archiviare ovvero di trasmettere alle fasi successive la segnalazione.

Le predette informazioni vengono inoltrate tramite l'applicativo dedicato di cui al par. 6.3 o in base ai recapiti forniti in caso di utilizzo dei canali alternativi di cui al per. 6.4.

8.3 Informazioni al soggetto segnalato

Compatibilmente con la necessità di non compromettere l'attività di analisi della segnalazione e di tutela del segnalante, la Banca informa il soggetto segnalato riguardo l'eventuale apertura di un procedimento a suo carico, attraverso i canali di comunicazione descritti al paragrafo 6.3.
La Banca non è tenuta ad alcuna comunicazione nei suoi confronti nel caso di archiviazione della segnalazione.

8.4 Responsabilità del segnalante

La presente Policy lascia impregiudicata la responsabilità penale e disciplinare nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del codice penale e dell'art. 2043 del codice civile.
Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente policy, quali le segnalazioni manifestamente opportunistiche e/o compiute con il solo scopo di danneggiare il denunciato o altri soggetti e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente procedura.

8.5 Archiviazione dei documenti

La documentazione raccolta nel corso dell'intera procedura di segnalazione è confidenziale e deve essere archiviata sull'applicativo informatico di cui al par. 6.3. anche se presentata in formato cartaceo o via mail.
Considerata la delicatezza dei dati trattati, CiviBank ha adottato particolari misure tecniche ed organizzative per la loro protezione, in conformità con le norme in vigore sul trattamento dei dati personali.

L'applicativo messo a disposizione per la segnalazione provvede all'archiviazione della documentazione elettronica secondo gli standard di sicurezza, permettendo di separare i dati identificativi del segnalante dal contenuto della segnalazione e prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima.

Possono accedere ai predetti documenti, esclusivamente i soggetti espressamente indicati dalla banca e/o i soggetti coinvolti nelle eventuali azioni disciplinari conseguenti la segnalazione , previa autorizzazione del "Responsabile".

I dati e documenti oggetto della segnalazione vengono conservati per 10 anni decorrenti dalla data di ricezione della segnalazione . o per il periodo più lungo necessario al passaggio in giudicato di una sentenza o altro provvedimento giudiziale, eventualmente esperito.

9. FLUSSI INFORMATIVI

In linea con le previsioni normative, il "Responsabile" redige con periodicità annuale una relazione contenente le informazioni aggregate sulle risultanze dell'attività svolta, che viene approvata dagli organi aziendali.
Una rappresentazione sintetica viene inoltre messa a disposizione del personale della Banca.

10.MONITORAGGIO E REVISIONE DELLA POLICY

La Policy, approvata dal Consiglio di Amministrazione della Banca, è soggetta a monitoraggio periodico e va sottoposta a revisione ogniqualvolta se ne ravvisi la necessità. Il suo contenuto deve essere portato a conoscenza del personale in maniera chiara, precisa e completa, con illustrazione degli aspetti relativi ai diritti, ai doveri ed alle tutele di ciascun soggetto interessato.

La Compliance è tenuta a valutare la conformità della Policy alle disposizioni vigenti e provvede a verificare l'adeguatezza delle procedure.