Unità di riferimento Area Compliance	**REGOLAMENTO PER LE SEGNALAZIONI**
Documento redatto da: Area Compliance **e approvata dal Consiglio di Amministrazione**	**Data Emissione:** 25/02/2025 **Annulla e sostituisce:** Proc. 64/2022 del 02/02/22

Riferimenti Normativi

Normativa esterna:

D. Lgs 209/2005 Codice delle assicurazioni private (CAP) agli articoli 10-quater e 10-quinquies in materia di sistemi di segnalazione delle violazioni;

D.Lgs. 231/2001 sulla "Responsabilità amministrativa degli enti", con riguardo all'introduzione di adeguati modelli di organizzazione e di gestione (c.d. MOG) dell'ente idonei a prevenire reati;

D.Lgs. 231/2007 all'art. 48 con riguardo alle procedure per la segnalazione al proprio interno […] di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo;

D.Lgs. 9 aprile 2008, n. 81 in materia di sicurezza sul lavoro all'art. 20 prevede sull'lavoratore l'obbligo di segnalare immediatamente al datore di lavoro le anomalie presenti in attrezzature, sostanze, materiali e dispositivi;

Reg. Ue 2016/679 in materia di trattamento dei dati personali:

Direttiva UE 2016/97 (IDD) art. 35 come recepito a livello di CAP;

Direttiva UE 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione Europea;

D.Lgs. 10 marzo 2023, n. 24, di recepimento della Direttiva UE 2019/1937;

Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (Loi Sapin 2).

Normativa interna:

Codice Ético;

Procedura anticorruzione della Compagnia;

Procedura disfunzioni e rischi reputazionali;

Corpus normativa aziendale in materia di POG;

Corpus normativa aziendale in materia di sicurezza sul lavoro;

Corpus normativa aziendale in materia di GDPR;

Corpus normativo di Gruppo in ambito anticorruzione.

Scopo e finalità

Agevolazione della segnalazione di illeciti e tutela del soggetto segnalante, fornendo indicazioni chiare sui canali e sui presupposti per effettuare una segnalazione nonché sulla relativa gestione.

INDICE

1. DEFINIZIONI 3
2. DESCRIZIONE DEL REGOLAMENTO PER LE SEGNALAZIONI 4
3. CONTESTO NORMATIVO DI RIFERIMENTO 5
4. TIPOLOGIA DI SEGNALAZIONI, CONTENUTO E MODALITÀ DI EFFETTUAZIONE 7
5. GESTIONE DELLE SEGNALAZIONI 11
6. FORME DI TUTELA DEL *"WHISTLEBLOWER"* 13
7 SISTEMA SANZIONATORIO 15
8. PROTEZIONE E CONSERVAZIONE DELLA DOCUMENTAZIONE 16
9. SEGNALAZIONE ESTERNA AI SENSI DEL DECRETO *WHISTLEBLOWING* 17
10. REPORTING E CONTROLLO 19

1. Definizioni

"CAA o **Compagnia" o "Società"**	Crédit Agricole Assicurazioni S.p.A.
"Gruppo"	Il Gruppo Crédit Agricole Assurances che fa capo a Crédit Agricole S.A. e di cui la Compagnia è parte
"Decreto 231"	D.Lgs. 8 giugno 2001, n. 231 e successive modifiche ed integrazioni
"**Legge *Whistleblowing***"	il decreto legislativo 10 marzo 2023, n. 24 di "*attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*"
"**Modello 231**"	Il modello di organizzazione e di gestione, previsto dal Decreto 231, adottato dalla Compagnia
"Organismo di Vigilanza" o "**OdV":**	L'Organismo di Vigilanza istituito ai sensi del Decreto 231 e i singoli componenti dello stesso
"Testo Unico Sicurezza"	D.Lgs. 9 aprile 2008, n. 81 e successive modifiche ed integrazioni
"Codice Etico"	Il Codice Etico del sotto-gruppo Crédit Agricole Assurances Italia, adottato da Crédit Agricole Assicurazioni S.p.A.
"GDPR"	Il Regolamento (UE) 2016/679
"ANAC"	L'Autorità Nazionale Anticorruzione
"Regolamento" o "Regolamento per le segnalazioni"	Il presente documento
"Persona Coinvolta" o **"Segnalato"**	La persona fisica o giuridica menzionata nella segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata.
"*Gestore*" o "*Gestore WB*"	Il soggetto/i soggetti individuato/i quale/i destinatario/i e gestore/i delle segnalazioni ai sensi del presente Regolamento, in possesso di

	requisiti di autonomia e indipendenza necessari, autorizzato/i al trattamento dei dati e formato/i sulla gestione delle segnalazioni. Attualmente, il Gestore WB è individuato nel Responsabile dell'Area *Compliance*.
"Segnalanti" o "*Whistleblowers*"	I dipendenti, collaboratori, azionisti, persone che esercitano (anche in via di mero fatto) funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza della Società e altri soggetti terzi che interagiscano con la Società (compresi i fornitori, consulenti, intermediari, ecc.) nonché stagisti o lavoratori in prova, candidati a rapporti di lavoro ed ex dipendenti.
"Soggetti Collegati"	I soggetti per i quali sono applicabili le stesse tutele che il Decreto *Whistleblowing* prevede per il Segnalante e che sono: *(i)* i facilitatori; *(ii)* persone del medesimo contesto lavorativo della persona segnalante e che sono legate alla stessa da uno stabile legame affettivo o di parentela entro il quarto grado; *(iii)* colleghi di lavoro della persona segnalante che lavorano nel medesimo contesto lavorativo e che hanno con il segnalante un rapporto abituale e corrente; *(iv)* enti di proprietà della persona segnalante o per i quali la stessa lavora o enti che operano nel medesimo contesto lavorativo

2. Descrizione del Regolamento per le segnalazioni

Il Regolamento ha lo scopo di descrivere il sistema di segnalazione delle violazioni della normativa esterna e interna in perimetro che le diverse tipologie di segnalanti rilevino nell'ambito dell'attività svolta in relazione alla Compagnia. In particolare, il Regolamento recepisce oltre a quanto previsto dalle disposizioni del Gruppo Crédit Agricole Assurances a livello di Corpus Fides (ref. NP 2023-04 Alerte interne) anche quanto previsto dal Decreto *Whistleblowing* (e dalle linee guida dell'ANAC) in relazione ai canali di segnalazione interna, alla gestione dei medesimi e alle tutele previste in relazione all'effettuazione di una segnalazione.

La Compagnia ha ritenuto di adottare il sistema di segnalazione ivi descritto per una ampia tipologia di violazioni che possono essere segnalati dai *Whistleblowers*.

A tal fine, l'obiettivo perseguito del Regolamento è quello di fornire ai destinatari indicazioni operative chiare circa l'oggetto, il contenuto, le modalità di trasmissione e gestione delle segnalazioni, nonché circa le forme di tutela previste nell'interesse dei soggetti segnalanti e dei Soggetti Collegati.

3. Contesto normativo di riferimento

Con il termine *"whistleblowing"* si intende il sistema di segnalazione delle violazioni della normativa esterna ed interna in perimetro per il presente Regolamento. In particolare, si intende anche l'istituto giuridico volto, da un lato, a disciplinare le modalità di segnalazione di condotte illecite nell'ambito di un determinato contesto (nel caso di specie, il contesto lavorativo) e, dall'altro, a tutelare il soggetto segnalante da possibili ritorsioni.

Potrebbero essere oggetto di segnalazione di una violazione:

- **a)** un reato o illecito amministrativo tra quelli previsti nel Modello 231, tra cui anche il reato di corruzione;
- **b)** una violazione del Modello 231;
- **c)** una violazione del codice etico e delle procedure in materia di anticorruzione;
- **d)** una violazione di un obbligo internazionale;
- **e)** una grave e manifesta violazione di legge o regolamento con particolare riguardo ai provvedimenti di IVASS e in materia di IDD e distribuzione assicurativa;
- **f)** violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo.

Ai sensi del Decreto *Whistleblowing* possono, in particolare, essere segnalati:

1. 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;
2. atti o omissioni che ledono gli interessi finanziari dell'Unione europea;
3. atti o omissioni riguardanti il mercato interno, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato nonché le violazioni riguardanti il mercato interno connesse a atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
4. atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui ai precedenti numeri 1), 2) e 3) relativamente agli atti dell'Unione nei settori indicati.

Di seguito si rappresenta in sintesi il quadro normativo di riferimento per quanto riguarda la previsione dello strumento del *whistleblowing* per la segnalazione di violazioni di normativa nazionale ed europea.

a) Il **Codice delle Assicurazioni Private** o CAP ha recepito la disciplina sul whistleblowing negli articoli 10-*quater* e 10-*quinquies* (in vigore dal 1°ottobre 2018) al fine di prevenire o far emergere illeciti o irregolarità all'interno delle organizzazioni aziendali operanti nel mercato assicurativo e, più in generale, favorire una cultura della

legalità e della trasparenza. È stato attribuito all'IVASS il potere di emanare disposizioni attuative in materia (art. 10-*quater*, comma 4 e art. 10-*quinquies*, comma 1, lett. b) del CAP).

b) L'art. 20 del **Testo Unico Sicurezza sui luoghi di lavoro** prevede l'obbligo per i lavoratori di segnalare immediatamente al datore di lavoro o ai soggetti incaricati le deficienze dei mezzi e dispositivi posti a presidio della salute e sicurezza sul lavoro, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza (oltre all'obbligo di adoperarsi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli). Così, infatti, recita l'art. 20, comma II, del Testo Unico Sicurezza:

"*I lavoratori devono in particolare:* [...] *segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d)*[1]*, nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f)*[2] *per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza*".

c) il **Codice Etico** che nell'ambito del modello organizzativo adottato dalla compagnia ai sensi del Decreto 231 e del sistema adottato a livello di Gruppo ai sensi della Loi Sapin II prevede una serie di principi, tra i quali quello di legalità e correttezza che risultano rafforzati dallo strumento di *whistleblowing* come mezzo per rilevare violazioni delle relative disposizioni e potenziali situazioni di rischio per la compagnia e per il Gruppo.

d) La **Direttiva UE 2019/1937** che introduce l'esigenza di prevedere uno strumento di segnalazione delle violazioni della normativa europea anche attraverso lo strumento del *whistleblowing*, che è stata recepita a livello nazionale dal Decreto *Whistleblowing*.

e) Il **Decreto *Whistleblowing*** disciplina la protezione 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.

f) Il **Decreto 231**, che a seguito della modifica ad opera del Decreto *Whistleblowing*, all'art. 6, comma 2-*bis* prevede che "*i modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)*", mentre i commi 2-*ter* (che prevedeva la denuncia all'Ispettorato nazionale del lavoro di misure discriminatorie) e 2-*quater* (sulla

[1] Vale a dire "*utilizzare correttamente le attrezzature di lavoro* […] *nonché i dispositivi di sicurezza*" e "*utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione*".

[2] Ovverosia, non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo.

nullità del licenziamento ritorsivo o discriminatorio) del medesimo articolo 6 sono stati abrogati ad opera del Decreto *Whistleblowing*.

Le segnalazioni non possono riguardare fatti, informazioni o documenti in qualunque forma o su qualunque supporto che siano coperti dal segreto relativo alla difesa nazionale, il segreto medico o il segreto professionale tra un avvocato e il suo assistito.

Tutte le segnalazioni diverse da quelle rappresentate sopra vengono considerate "segnalazioni ordinarie". In particolare, si specifica che situazioni che non rientrino in alcuna delle categorie sopra indicate (che riguardino, ad esempio, un dissidio tra due dipendenti, una contestazione di carattere personale che attiene al rapporto di lavoro ovvero una situazione di dubbio riguardo alle proprie prospettive di crescita lavorativa, ecc.) esulano dal perimetro di applicazione del Decreto *Whistleblowing* e dall'oggetto del Regolamento e, pertanto, non dovranno essere segnalate tramite i canali ivi descritti e non dovranno essere necessariamente gestite come indicato di seguito. Per quanto riguarda tali situazioni, le segnalzioni potranno essere discusse e affrontate tramite gli altri canali disponibili (ad esempio, colloqui con il superiore gerarchico, con le Risorse Umane, ecc.).

4. Tipologia di segnalazioni, contenuto e modalità di effettuazione

4.1. Destinatari della segnalazione: Gestore WB

Le segnalazioni che riguardano la Compagnia e rientrano nel perimetro di applicazione del Regolamento sono esaminate e gestite dal Gestore (individuato nel Responsabile dell'Area *Compliance*) nel rispetto delle condizioni di autonomia e indipendenza previste dalla disciplina in materia di *whistleblowing*.

Il Gestore può avvalersi del supporto dei soggetti che operano già all'interno della sua Area /Funzione, in quanto dotati dei requisiti di autonomia e indipendenza e preventivamente autorizzati al trattamento dei dati.

In caso di conflitto di interesse del Gestore (e/o dell'intera Area *Compliance*) rispetto a una segnalazione, quest'ultimo verrà estromesso da ogni attività di gestione della segnalazione, che verrà presa in carico dal gestore delle segnalazioni di Gruppo (che dovrà rispettare quanto previsto del del Regolamento).

In caso di segnalazioni pervenute tramite i canali indicati nel del Regolamento nel periodo di assenza (temporanea e previamente comunicata) del Gestore, le stesse verranno gestite dai soggetti a supporto (operanti nel Servizio *Compliance*).

Il Gestore è competente per ricevere anche tutte le segnalazioni riguardanti violazioni del Modello 231 e fatti idonei a configurare i reati presupposto previsti dal Decreto 231 ovvero situazioni di rischio in tale ambito ("**Segnalazioni 231**").

In caso di Segnalazioni 231, il Gestore coinvolge, nel rispetto degli obblighi di riservatezza, l'Organismo di Vigilanza della Compagnia che lo supporta nelle relative valutazioni e, ove necessario, nell'attività istruttoria.

Per tutte le segnalazioni, il Gestore può, inoltre, coinvolgere eventuali soggetti interni e/o esterni competenti in base all'area oggetto di segnalazione.

In tali casi, la condivisione di una segnalazione viene effettuata, nel rispetto della riservatezza (in particolare, dovrà essere previsto l'oscuramento dei dati identificativi del Segnalante e di altri soggetti menzionati, salvo il consenso espresso del Segnalante a divulgare la propria identità) e sul presupposto che la stessa non metta in pericolo la condizione del segnalante e che lo stesso non rischi atti ritorsivi.

4.1.1. Segnalazione in merito a violazione (o possibile violazione) dei principi di cui al Modello 231

Costituisce una segnalazione di cui alla presente categoria ogni segnalazione in merito alla violazione accertata o presunta delle regole comportamentali previste dal Modello 231, per tali intendendosi sia i principi generali di comportamento sia i principi procedurali specifici relativi alle singole attività sensibili, indicati in calce alle singole Parti Speciali del Modello 231.

Esempio: il potenziale *"whistleblower"* scopre che un collega è solito non rispettare alcuni passaggi fondamentali di una procedura di diretto impatto sul funzionamento del Modello 231 (perché, ad esempio, disciplina il processo di autorizzazione dei pagamenti dei consulenti).

4.1.2. Segnalazione in merito alla commissione (o possibile commissione) di un reato di possibile rilevanza ex *Decreto 231*

Costituisce una segnalazione di cui alla presente categoria ogni segnalazione in merito alla commissione (o possibile commissione) di una fattispecie rientrante nelle categorie di illeciti richiamate all'interno del Decreto 231.

Esempio: il potenziale *"whistleblower"* scopre che un collega, indipendentemente dalla violazione o meno di un principio procedurale, ha commesso (o tentato di commettere) un reato di possibile rilevanza 231 nell'ambito dell'attività lavorativa, ovvero, comunque, ha tenuto una condotta criminosa (ad esempio, cercando di corrompere un esponente della società incaricata della revisione contabile del bilancio della Compagnia[3]).

4.1.3. Segnalazione in merito a violazione (o possibile violazione) in materia di Salute e Sicurezza sul Luogo di Lavoro

Costituisce una segnalazione di cui alla presente categoria ogni segnalazione in merito alla violazione (o possibile violazione) delle disposizioni di legge previste a tutela della salute e sicurezza sul luogo di lavoro nonché dei principi previsti dal Modello 231 in relazione a tale materia.

Si precisa che in tale caso sussiste un obbligo specifico per i lavoratori (previsto dall'art. 20 del T.U. Sicurezza) di segnalare immediatamente al datore di lavoro, o ai soggetti incaricati, le deficienze dei mezzi e dispositivi posti a presidio della salute e sicurezza sul lavoro, nonché le altre eventuali condizioni di pericolo di cui vengano a

[3] Con ciò integrando la condotta prevista e punita dall'art. 2635-*bis* c.c. (istigazione alla corruzione tra privati).

conoscenza (oltre all'obbligo di adoperarsi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli). Trattandosi, quindi, in questo caso, di un obbligo di segnalazione contenuto all'interno della normativa specifica in materia di salute e sicurezza sul lavoro, potrebbe essere preferibile per il segnalante (nel suo specifico interesse) non effettuare la segnalazione in forma anonima, giacché, così procedendo, incorrerebbe nel rischio di non poter provare, laddove necessario, di aver adempiuto a tale obbligo.

Esempio: il potenziale *"whistleblower"* scopre che in un'area degli uffici non sono presenti le misure di sicurezza necessarie a prevenire incidenti ovvero queste non sono manutenute adeguatamente (ad esempio, carenza degli estintori ovvero mancato accesso dei fornitori esterni incaricati della verifica del loro funzionamento).

4.1.4 Segnalazione di violazione (o possibile violazione) dei principi di cui al Codice Etico

La segnalazione può *riguardare* azioni o omissioni (commesse o tentate) dei principi di condotta previsti dal Codice Etico e/o nel Codice di condotta di Gruppo in relazione ai temi in questo trattati: più precisamente, la segnalazione può riguardare presunti casi di violazione dei principi comportamentali delineati nel Codice Etico di cui sono a conoscenza, ovvero qualsiasi atteggiamento o situazione di potenziale criticità.

Limitatamente alle segnalazioni concernenti nello specifico azioni o omissioni (commesse o tentate) poste in essere in violazione dei principi previsti dal Codice Etico, le stesse potranno essere effettuate alternativamente secondo le modalità previste all'interno del Codice Etico ovvero secondo le modalità previste al successivo paragrafo 4.3.

Nel caso le segnalazioni vengano effettuate ai sensi del Regolamento, vale quanto segue.

Esempio: il potenziale *"whistleblower"* scopre che un collega adotta comportamenti scorretti nei confronti della clientela, in violazione del principio che richiede ai destinatari di *"mantenere un atteggiamento professionale, leale e collaborativo".*

4.1.5 Segnalazione di violazione (o possibile violazione) della normativa nazionale ed europea nei settori indicati dal Decreto Whistleblowing

Esempi: (i) il potenziale *"whistleblower"* scopre che vengono aggirati gli obblighi di tutela dei dati personali di controparti contrattuali; (ii) il potenziale *"whistleblower"* scopre che la Società sta omettendo i versamenti delle somme dovute a titolo di IVA, oppure il potenziale *"whistleblower"* scopre che la Società sta utilizzando in modo improprio i fondi erogati dall'Unione Europea.

4.2. Contenuto minimo della segnalazione

Per essere considerata ammissibile da parte del Gestore e per consentire lo svolgimento di adeguata istruttoria in merito, è indispensabile che la segnalazione contenga quantomeno i seguenti elementi:

- una chiara e completa descrizione dei fatti oggetto di segnalazione;
- l'indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;
- se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi i fatti oggetto di segnalazione;
- se conosciute, le generalità o altri elementi (come la qualifica e il servizio in cui svolge l'attività) che consentano di identificare il soggetto/i che ha/hanno posto/i in essere i fatti segnalati;
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

Le segnalazioni prive di qualsiasi elemento che consenta di identificare il loro autore (*i.e.* segnalazioni anonime) verranno prese in considerazione a condizione che le medesime siano adeguatamente circostanziate e dettagliate, in modo da permetterne la valutazione (ad esempio, la menzione di specifiche aree aziendali, procedimenti o eventi particolari, ecc.).

4.3. Modalità di effettuazione della segnalazione

La segnalazione ai sensi del Regolamento può essere effettuata in forma scritta (tramite il *tool* indicato nel presente paragrafo) o orale (tramite incontro di persona con il Gestore).

Al fine di effettuare una segnalazione conforme alla normativa vigente, la Società mette a disposizione un ***tool* informatico** – fornito dalla Capogruppo[4] – che garantisce la riservatezza del segnalante e del contenuto della segnalazione denominato BKMS System, accessibile al seguente indirizzo web: https://www.bkms-system.com/bkwebanon/report/clientInfo?cin=3CAgr18**.**

I punti di accesso al *tool* sono molteplici per favorirne la conoscibilità e l'utilizzo ragionato nel rispetto dei principi di legalità, correttezza e trasparenza. Tra questi vi è l'intranet aziendale per i dipendenti e i collaboratori della Compagnia nonché il sito istituzione anche per terze parti, come ad esempio i fornitori e sub-fornitori, con cui la stessa intrattiene relazioni d'affari.

I dettagli per accedere ed effettuare le segnalazioni tramite il BKMS System sono rappresentati nell'Allegato 1 al Regolamento**.**

L'identità del segnalante (se desumibile dal contenuto della comunicazione o da altri elementi che identifichino il mittente) sarà conosciuta solo dal Gestore e dai soggetti a supporto dello stesso, appositamente autorizzati al trattamento, che ne garantiranno la riservatezza, fatti salvi i casi in cui questa non sia opponibile per legge (come descritto al successivo paragrafo 6.1.).

[4] Si precisa che la Capogruppo fornisce solamente l'infrastruttura per la ricezione delle segnalazioni.

Quando, su richiesta del Segnalante, la **segnalazione è effettuata oralmente nel corso di un incontro** con il Gestore, essa, previo consenso del Segnalante, è documentata mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale; in caso di verbale, il Segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

5. Gestione delle segnalazioni

Quando viene effettuata una segnalazione tramite lo strumento del *whistleblowing* in conformità al Regolamento per le segnalazioni, il Gestore assolve ai seguenti compiti:

- pronunciarsi sulla ammissibilità della segnalazione rispetto al perimetro del Regolamento per le segnalazioni;
- nel caso in cui si tratti di una segnalazione ammissibile ai sensi del presente Regolamento, garantirne il trattamento e gli adempimenti di cui al Decreto *Whistleblowing*, analizzare i fatti rappresentati e decidere su come gestire l'istruttoria volta a valutare la fondatezza della segnalazione, compreso l'eventuale coinvolgimento – a supporto – di soggetti/organi interni o esterni competenti (come indicato di seguito);
- nel caso in cui si tratti di una Segnalazione 231, coinvolgere l'Organismo di Vigilanza, nel rispetto degli obblighi di riservatezza previsti dal Decreto *Whistleblowing*;
- nel caso in cui la segnalazione non riguardi la Società bensì altra società del Gruppo, verificare la procedura/regolamento *whistleblowing* di tale società e trasmettere la segnalazione al relativo referente entro sette giorni, dandone notizia al Segnalante.

Come sopra indicato, nell'ambito delle attività di gestione delle segnalazioni e nel rispetto degli obblighi di riservatezza previsti dal Decreto *Whistleblowing*, il Gestore WB può decidere di rivolgersi a soggetti interni e/o di farsi supportare da un gruppo di lavoro interno – appositamente costituito – ristretto e sottoposto ad obblighi di confidenzialità e/o, se necessario, da un gruppo di investigazione o di esperti esterni anch'essi sottoposti alla più stretta confidenzialità.

Il gruppo di lavoro interno che supporta il Gestore nella gestione delle segnalazioni interviene in considerazione delle competenze specialistiche funzionali alla trattazione della segnalazione e ad una decisione collegiale sulle azioni da intraprendere.

Il gruppo di supporto del Gestore è composto ad esempio, dai responsabili delle seguenti aree aziendali: Risorse Umane, *Internal Audit*, Legal, che sono in possesso dei requisiti di autonomia e imparzialità e vengono autorizzati al trattamento dei dati contenuti nella segnalazione.

Nel caso in cui nella segnalazione emergessero aspetti particolarmente delicati ovvero ipotesi di conflitti di interesse dei membri del gruppo di supporto, il Gestore potrà decidere se e con chi di questi condividere la segnalazione.

Il Gestore garantisce che al Segnalante venga dato avviso di ricevimento della segnalazione **entro sette giorni** e che la segnalazione venga gestita nell'arco di un periodo ragionevole (fissato in **tre mesi** dal ricevimento della

segnalazione), provvedendo ad aggiornare regolarmente il Segnalante per informarlo degli sviluppi o per ricevere eventuali chiarimenti.

Qualora, per ragioni legate alla complessità dell'indagine questa non si concluda entro tre mesi, il Gestore fornirà comunque al Segnalante un riscontro sull'attività in corso e sui primi esiti dell'indagine, riservandosi di fornire un ulteriore riscontro al termine dell'attività di gestione della segnalazione (sia in caso di archiviazione sia in caso di valutazione di fondatezza della segnalazione).

5.1. Verifica dell'ammissibilità della segnalazione e istruttoria

La segnalazione deve considerarsi ammissibile laddove sia intrinsecamente verosimile, supportata da evidenze documentali ovvero da altri riscontri probatori (quale, ad esempio, il riferimento preciso ad altri soggetti che possano confermarla).

In particolare, il Gestore deve valutare se la segnalazione:

- sia stata presentata da uno dei soggetti legittimati ai sensi del Decreto *Whistleblowing* e/o del presente Regolamento e che l'oggetto della stessa rientri nell'ambito di applicazione dei medesimi;
- si basi su fatti sufficientemente precisi;
- consenta l'individuazione delle circostanze di tempo e luogo in cui si è verificato il fatto oggetto di segnalazione e, quindi, una descrizione dei fatti oggetto della segnalazione, e, ove presenti, anche delle modalità attraverso cui il segnalante è venuto a conoscenza dei fatti;
- contenga le generalità o altri elementi che consentano di identificare la Persona Coinvolta nella segnalazione.

Laddove il contenuto della segnalazione sia tale da non consentire la comprensione dei fatti, ovvero la segnalazione sia corredata da documentazione non appropriata o tale da non far comprendere il contenuto della stessa, il Gestorepotrà chiedere ulteriori informazioni al Segnalante al fine di procedere a una corretta classificazione della segnalazione.

Una volta appurato che la segnalazione è ammissibile, il Gestore può procedere con l'istruttoria, che consiste nell'effettuare tutte le opportune verifiche, analisi e valutazioni specifiche circa la fondatezza o meno dei fatti segnalati.

L'attività istruttoria può essere svolta, ad esempio:

- direttamente, acquisendo gli elementi informativi necessari alle valutazioni dall'analisi della documentazione/informazioni già ricevute con la segnalazione;
- attraverso eventuali documenti integrativi richiesti al fine di circostanziare meglio la segnalazione;
- mediante il coinvolgimento di altre strutture interne o anche di soggetti specializzati esterni, in considerazione delle specifiche competenze tecniche e professionali che risultano necessarie per il caso di specie;
- tramite audizione di eventuali ulteriori soggetti interni/esterni, che possano riferire sui fatti segnalati.

Il Gestore ha la facoltà di richiedere alla persona Segnalante – ove ritenuti necessari – ulteriori elementi a supporto della propria segnalazione e di sentire la Persona Coinvolta anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

Al termine dell'istruttoria, il Gestore valuta la fondatezza della segnalazione.

La fondatezza delle circostanze rappresentate nella segnalazione deve, in ogni caso, essere valutata, nel rispetto dei principi di imparzialità e riservatezza, con eventuale coinvolgimento, supporto e confronto con soggetti interni o esterni competenti e/o l'intero OdV (quest'ultimo in caso di Segnalazione 231).

5.2. Esito della fase istruttoria e relativa comunicazione

Terminata la fase istruttoria e le relative valutazioni, il Gestore può:

- archiviare la segnalazione perchè infondata, motivandone le ragioni;
- rivolgersi agli organi/funzioni interne ed esterni competenti per i relativi seguiti rispetto a una segnalazione valutata fondata.

In entrambi i casi, il Gestore fornisce riscontro al Segnalante (come indicato al paragrafo 5).

In caso di accertata fondatezza della segnalazione, l'esito della trattazione della stessa viene, in particolare, comunicato ai soggetti aziendali deputati ad adottare gli opportuni provvedimenti in merito, quali:

- il Responsabile dell'Area in cui si inquadrano le Risorse Umane, nonché il Direttore della struttura di appartenenza dell'autore della violazione accertata affinché sia espletato l'esercizio dell'azione disciplinare.

Ad integrazione di quanto sopra, l'esito della fase istruttoria della segnalazione potrebbe essere comunicato al Consiglio di Amministrazione della Società e alle strutture competenti affinché adottino gli eventuali ulteriori provvedimenti e/o azioni che nel caso concreto si rendano necessari a tutela della Società (ad esempio, azioni idonee a rimediare alla situazione che è emersa dalla segnalazione e dalle indagini interne e azioni atte a evitare che una simile situazione possa ripetersi in futuro).

6. Forme di tutela del *"whistleblower"*

Il sistema di segnalazione delle violazioni adottato dalla Compagnia assicura la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione.

La Compagnia (in conformità al Gruppo Crédit Agricole) adotta, inoltre, tutte le misure necessarie a garantire la piena tutela del segnalante contro possibili condotte ritorsive, discriminatorie o comunque sleali, che siano conseguenti alla segnalazione.

6.1. Riservatezza dell'identità del *"whistleblower"*

L'identità del Segnalante e qualsiasi altra informazione da cui può evincersi direttamente o indirettamente tale identità non possono essere rivelate, senza il consenso espresso del Segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

La protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona Segnalante.

L'identità del Segnalante è coperta da segreto in un eventuale procedimento penale (non oltre la chiusura delle indagini preliminari) e nel procedimento disciplinare attivato contro il presunto autore della condotta segnalata.

La **necessità di rilevare l'identità del Segnalante**, saranno comunicate per iscritto e potrà essere effettuata esclusivamente se rilasciato **esplicito consenso** qualora:

- una contestazione disciplinare sia fondata in tutto o in una parte sulla segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa del soggetto cui è stato contestato l'addebito disciplinare (in caso di mancato consenso, non sarà possibile utilizzare la segnalazione nell'ambito del procedimento disciplinare);

- nei procedimenti instaurati in seguito a una segnalazione, la rivelazione dell'identità del Segnalante sia indispensabile anche ai fini della difesa della persona cui è rivolta la contestazione.

Per quanto riguarda, le segnalazioni in merito a violazione (o possibile violazione) in materia di salute e sicurezza sul luogo di lavoro, si ribadisce che, in tale caso, sussiste un obbligo specifico per i lavoratori (previsto dall'art. 20 del T.U. Sicurezza) di segnalare immediatamente al datore di lavoro, o ai soggetti incaricati, le deficienze dei mezzi e dispositivi posti a presidio della salute e sicurezza sul lavoro, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza (oltre all'obbligo di adoperarsi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli). Trattandosi, quindi, in questo caso, di un obbligo di segnalazione contenuto all'interno della normativa specifica in materia di salute e sicurezza sul lavoro, potrebbe essere preferibile per il segnalante (nel suo specifico interesse) non effettuare la segnalazione in forma anonima, giacché, così procedendo, incorrerebbe nel rischio di non poter provare – laddove necessario – di aver adempiuto a tale obbligo.

6.2. Misure di protezione (in particolare, divieto di *"retaliation"*)

Le segnalazioni devono essere effettuate in buona fede. In conformità a quanto previsto dal Decreto *Whistleblowing* **è garantita l'applicabilità di specifiche misure di protezione nei confronti del Segnalante e dei Soggetti Collegati a condizione che**:

a. al momento della segnalazione, il Segnalante avesse fondato motivo di ritenere che le informazioni sulle violazioni segnalate o denunciate fossero vere e rientrassero nell'ambito delle violazioni di cui al Regolamento;

b. la segnalazione sia stata effettuata in conformità a quanto previsto dal Regolamento e dal Decreto *Whistleblowing*.

Le **misure di protezione previste** nei confronti del Segnalante e dei Soggetti Collegati sono le seguenti:

- divieto di ritorsione in ragione di una segnalazione;
- misure di sostegno, che consistono in informazioni, assistenza, consulenza a titolo gratuito da parte di enti del terzo settore indicati in un elenco disponibile sul sito dell'ANAC in merito alle modalità di segnalazione e alle previsioni normative in favore di Segnalante e della Persona Coinvolta;
- protezione dalle ritorsioni, che comprende:
    - la possibilità di comunicare all'ANAC le ritorsioni che si ritiene di aver subito a seguito di una segnalazione;
    - la previsione di nullità degli atti assunti in violazione del divieto di ritorsione, da far valere anche in sede giudiziaria;
- limitazioni di responsabilità in caso di rivelazione (o diffusione) di violazioni coperte da obbligo di segreto[5] o relative alla tutela del diritto d'autore o alla protezione dei dati personali oppure di informazioni sulle violazioni che offendono la reputazione della Persona Coinvolta o denunciata, se
    - al momento della rivelazione (o diffusione) vi fossero fondati motivi per ritenere che la stessa fosse necessaria per svelare la violazione e
    - sussistessero le condizioni di cui sopra;
- limitazioni di responsabilità, salvo che il fatto costituisca reato, per l'acquisizione delle informazioni sulle violazioni o per l'accesso alle stesse;
- sanzioni (indicate nel Decreto *Whistleblowing* e nel precedente Regolamento al paragrafo 7).

Le misure di protezione trovano applicazione anche in caso di segnalazione anonima, se il Segnalante è stato successivamente identificato e ha subito ritorsioni.

7 Sistema sanzionatorio

La violazione delle previsioni contenute nei sopra riportati paragrafi potrà attivare il procedimento sanzionatorio.

[5] Salvo il caso di informazioni classificate, segreto professionale e medico e segretezza delle deliberazioni degli organi giurisdizionali, per cui resta ferma l'applicazione della relativa normativa.

In particolare, è soggetto a **sanzioni pecuniarie** da parte dell'ANAC chiunque si renda responsabile di una delle seguenti condotte:

- compimento di ritorsioni in relazione a segnalazioni;
- ostacolo o tentato ostacolo all'effettuazione della segnalazione;
- violazione degli obblighi di riservatezza previsti dal Regolamento e dal Decreto *Whistleblowing*;
- mancata istituzione dei canali di segnalazione secondo i requisiti previsti dal Decreto *Whistleblowing*;
- mancata adozione di una procedura per l'effettuazione e la gestione delle segnalazioni o mancata conformità della stessa al Decreto *Whistleblowing*;
- mancata verifica e analisi delle segnalazioni ricevute.

Per tutte le condotte sopra elencate sono, inoltre, applicabili le **sanzioni disciplinari** previste dal Modello 231.

È, inoltre, prevista l'irrogazione di una **sanzione disciplinare nei confronti del Segnalante quando è accertata** in capo allo stesso: *(i)* anche con sentenza di primo grado, la responsabilità penale per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero *(ii)* la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave[6].Laddove, quindi, l'istruttoria abbia evidenziato che la segnalazione fosse infondata e sia accertato che il "*whistleblower"* l'abbia effettuata con dolo o colpa grave, ovvero laddove si accerti che un soggetto abbia violato la riservatezza del segnalante o abbia compiuto altri atti in violazione del Regolamento e della normativa vigente, il Gestorene darà informativa, oltre all'OdV, ai soggetti deputati ad adottare gli opportuni provvedimenti in merito, ovverosia (i) il Responsabile dell'Area in cui si inquadrano le Risorse Umane e il Direttore della struttura di appartenenza dell'autore della violazione accertata, laddove il destinatario della sanzione sia un lavoratore dipendente, oppure (ii) i componenti del Consiglio di Amministrazione e del Collegio Sindacale, laddove il destinatario della sanzione sia un amministratore, un sindaco o un membro dell'Organismo di Vigilanza.

Da ultimo, si evidenzia che il Regolamento per le segnalazioni lascia impregiudicata la responsabilità penale e disciplinare del "*whistleblower"* nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del codice penale e dell'art. 2043 c.c.

8. Protezione e Conservazione della documentazione

L'insieme di tutte le informazioni e i documenti forniti con la segnalazione sono oggetto di archiviazione ad alto livello di protezione della riservatezza per tutta la fase di istruttoria, di ammissibilità e trattazione.

[6] Ai sensi del Decreto *Whistleblowing*, nel caso *sub (ii)* è prevista anche l'applicazione di sanzioni pecuniarie da 500 a 2.500 euro da parte dell'ANAC.

I dati personali inerenti alle segnalazioni ricevute, inclusi quelli relativi all'identità del segnalante, del segnalato o di altri individui, saranno trattati dalla Società, quale Titolare autonomo del trattamento, nel rispetto delle disposizioni di cui al Codice Privacy e al GDPR.

Come anticipato sopra, l'identità del Segnalante e qualsiasi altra informazione da cui può evincersi direttamente o indirettamente tale identità non possono essere rivelate, senza il consenso espresso del Segnalante, a persone diverse dal Gestore (o dai soggetti a supporto), che devono essere espressamente autorizzate a trattare tali dati.

Il rapporto con fornitori esterni che trattano dati personali per conto della Società deve essere disciplinato ai sensi dell'art. 28 del GDPR.

Le persone competenti a ricevere o a dare seguito alle segnalazioni ai sensi del presente Regolamento devono essere autorizzate a trattare i dati personali relativi alle segnalazioni ai sensi del GDPR e del Codice Privacy.

Ai Segnalanti e alle Persone coinvolte devono essere fornite idonee informazioni ai sensi degli artt. 13 e 14 del GDPR.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti, devono essere cancellati immediatamente.

La segnalazione e relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e, comunque, non oltre cinque anni dalla data della comunicazione dell'esito finale del processo di gestione della segnalazione.

I dati personali relativi a segnalazioni considerate fuori dal perimetro di applicazione del presente Regolamento saranno distrutti o le segnalazioni comunque archiviate previa anonimizzazione dei relativi dati personali riferibili alla persona.

I dati personali relativi a segnalazioni non seguite da procedimenti disciplinari o giudiziari saranno distrutti o archiviati previa anonimizzazione dopo 12 mesi dalla chiusura del processo di trattazione.

I dati personali relativi a segnalazioni seguite da un procedimento disciplinare o giudiziario nei confronti della persona oggetto della segnalazione o dell'autore di una segnalazione abusiva sono conservati fino alla chiusura del procedimento stesso.

In tutti i casi di archiviazione di dati personali come sopra descritti si precisa che gli stessi saranno tenuti in database separati ad alto livello di protezione e ad accesso ristrotto per un periodo non eccedente quello del procedumento contenzioso.

9. Segnalazione Esterna ai sensi del Decreto *Whistleblowing*

Fermo restando la priorità del canale di segnalazione interna, il Segnalante può effettuare una segnalazione esterna tramite il canale istituito e accessibile sul sito dell'ANAC: (**https://www.anticorruzione.it/-/whistleblowing**).

Le segnalazioni che possono essere effettuate tramite il canale di segnalazione esterna dell'ANAC possono riguardare esclusivamente le seguenti violazioni:

1. 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;
2. atti o omissioni che ledono gli interessi finanziari dell'Unione europea;
3. atti o omissioni riguardanti il mercato interno, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato nonché le violazioni riguardanti il mercato interno connesse a atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
4. atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui ai precedenti numeri 1), 2) e 3) relativamente agli atti dell'Unione nei settori indicati.

Si precisa che il ricorso al canale di segnalazione esterna istituito presso l'ANAC può avvenire solo se:

- il canale di segnalazione interna indicato nel Regolamento non risulti attivo;
- il Segnalante abbia già effettuato una segnalazione al canale interno indicato nel Regolamento e la stessa non abbia avuto seguito;
- il Segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna tramite il canale previsto dal presente Regolamento, alla stessa non verrebbe dato seguito ovvero la segnalazione potrebbe determinare il rischio di ritorsione;
- il Segnalante ha fondato motivo di ritenere che la violazione da segnalare possa costituire un pericolo imminente o palese per l'interesse pubblico.

Resta ferma la possibilità di comunicare all'ANAC le ritorsioni che si ritiene di aver subito in ragione di una segnalazione.

Per l'utilizzo di tale canale di segnalazione esterna o per il ricorso alla divulgazione pubblica[7], si prega di fare riferimento alle linee guida e al sito ufficiale dell'ANAC.

[7] Ai sensi del Decreto *Whistleblowing*, i segnalanti possono effettuare direttamente una divulgazione pubblica (tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone) quando: (i) la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni; (ii) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse; (iii) la persona segnalante

10. Reporting e Controllo

Il Gestore redige, nel rispetto degli obblighi di riservatezza previsti dalla normativa vigente, la reportistica relativa alle segnalazioni ricevute al Comitato ICRC (e Direction Générale) e al Referente di Crédit Agricole Assurances Groupe trimestralmente. Tale reportistica deve integrare anche una analisi quali-quantitativa delle segnalazioni ricevute.

Allegati

Allegato 1_ Istruzioni per l'accesso e l'utilizzo del BKMS System

Allegato 2_Informativa sul trattamento dei dati dei segnalanti

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.

Quick start guide for an alert

You have just received an alert « Activity BKMS System »

Step 1: connect to the BKMS tool

https://client.bkms-system.com/bkwebanon/action/client/clientDisclaimer.do?language=fre

✓ Please take care with uppercase, lowercase, special characters

✓ After six failed login attempts, your account will be locked

1. **Please enter the Security Query**



2. **Please enter your client login data**
   (same for all group users)

client login name	client login password
Credit-Agricole	C4sa_BKMS

3. **Please enter your user login data**

user login name	user login password
name	Personal password

4. **Please enter DataPIN :**

datapin
Montrouge;

✓ Be careful, your login information is personal and must not be provided to a third party under any circumstance

In case of password loss, contact the support team , request a reset at admin.ethicsalerts@credit-agricole-sa.fr :

Step 2: Instruct the alert

- Assign the alert to a person in charge of the treatment by clicking on the « Edit » button. An email have been sent to the affected person. Assign to yourself the alert, if you are in charge of the treatment
- Send a receipt via the dialogue box, if it is created.
- If the alert is not receivable, you have to inform the whistleblower (at the latest in ten days), via the dialogue box, if it is created.
- The whistleblower select a group of categories from the eight proposed but you have to select more precisely the alert's category, and if necessary modify it. Then, notify your choice in the text area.
- Evaluate the sensitivity level of the alert. Then notify your choice in the text area.
- Schedule a reminder within 6 weeks of receiving the alert in order to respect the two-month processing deadline.
- Instruct the alert : dialogue with the whistleblower to ask for additional information, and eventually, meet him.
- Once the investigation is complete, record the conclusions by choosing the "additional information" function and select the appropriate conclusion assigned from the drop-down list.
- Close the alert, at the latest, within 2 months, according to the procedure described in the "User manual of the BKMS tool".
- Anonymize the alert within twelve months after the closure according to the procedure described in the "BKMS Tool User Manual".

The usual Caution

- Warning : the data contained in the alert is confidential. Criminal and civil penalties are provided for disclosure of identities or revealed facts.
- As soon as a document is printed or downloaded, it leaves the secure system of BKMS and requires you to take measures to ensure the confidentiality and security of outsourced information.
- Make a confidentiality agreement signed by all stakeholders in the case (referred person, expert).
- The closure of a file is irreversible and definitive, hence the necessity to put a system of 4 eyes: authorize the closing (analyst) + the closing (supervisor).
- Process the alert within 2 months. If the instruction lasts longer, inform the whistleblower.
- In the case of a complex alert, do not hesitate to ask help to Credit Agricole SA or the Alerts Management Committee of your entity (cf. "BKMS Tool User Manual").
- Be careful in the alert's treatment that can be defamatory, especially in case of anonymity.
- Inform the targeted person only if you are sure that she cannot identify the whistleblower. Protecting the identity of the whistleblower remains the top priority.
- Ensure during the anonymization phase that no personal data has been forgotten.

CRÉDIT AGRICOLE VITA

CRÉDIT AGRICOLE ASSICURAZIONI

INFORMATIVA PRIVACY

	IDENTITÀ DEL TITOLARE DEL TRATTAMENTO	Titolari del trattamento sono Crédit Agricole Vita, con sede legale in Via Università 1 - 43121 Parma IT e Crédit Agricole Assicurazione sede legale in Corso di Porta Vigentina, 9 Milano. (d'ora in poi "Titolari")			
	DATI DI CONTATTO DEL RESPONSABILE DELLA PROTEZIONE DEI DATI	Il responsabile della protezione dei dati personali è reperibile all'indirizzo e-mail: dataprotection@ca-vita.it e dataprotection@ca-assicurazioni.it			
	DATI PERSONALI RACCOLTI	• Dati identificativi: dati anagrafici (nome e cognome), dati di contatto (n. telefono, e-mail), ruolo all'interno dell'azienda; • Dati personali contenuti nella tua segnalazione, che potrebbero includere informazioni relative alla tua persona e a terzi attinenti ad esempio alla vita privata, alle preferenze sessuali, allo stato di salute, a orientamenti politici.			
	FINALITÀ DEL TRATTAMENTO		**BASE GIURIDICA PER IL TRATTAMENTO**		**PERIODO DI CONSERVAZIONE DEI DATI PERSONALI**
1.	Gestione della segnalazione (indagine sugli eventi segnalati al fine di verificarne la veridicità e adottare eventuali provvedimenti)		Legittimo interesse dei Titolari ad indagare su un evento che potrebbe costituire un comportamento illecito. Qualora l'evento abbia rilevanza ai sensi del D.lgs 231/2001, la base giuridica è costituita dall'obbligo di legge.		– 1 anno dall'apertura della segnalazione, qualora dalla stessa non seguano provvedimenti; – 5 anni dalla conclusione del procedimento qualora dalla segnalazione prenda avvio lo stesso; – i dati non necessari per le indagini sui fatti, non sono conservate
	DESTINATARI O CATEGORIE DI DESTINATARI DEI DATI PERSONALI	La segnalazione sarà gestita solo da personale a ciò predisposto. I suoi dati potranno essere comunicati a: – soggetti dell'Area Compliance e antiriciclaggio – CA.SA – La società fornitrice del tool IT BKMS "Business Keeper Gmbh" che agirà nella qualità di Responsabile del trattamento – L'Autorità giudiziaria se dalla segnalazione scaturisce un giudizio			
	TRASFERIMENTO DEI DATI PERSONALI	I Suoi dati personali non saranno trasferiti verso paesi terzi rispetto a quelli facenti parte dello Spazio Economico Europeo (SEE).			

	**DIRITTI DEGLI INTERESSATI**	Il dipendente può esercitare specifici diritti in relazione al trattamento dei suoi dati personali, quali, ad esempio, il diritto di accesso, rettifica, cancellazione, limitazione del trattamento e opposizione al trattamento. Puoi esercitare i tuoi diritti, inviando un'e-mail al Responsabile per la protezione dei dati del Titolare (dataprotection@ca-vita.it; dataprotection@ca-assicurazioni.it).
	**DIRITTO DI PRESENTARE UN RECLAMO ALL'AUTORITÀ DI CONTROLLO**	Se il dipendente ritiene che i suoi dati personali siano stati trattati in modo illecito, ha il diritto di presentare un reclamo all'Autorità Garante per la protezione dei dati personali (https://www.garanteprivacy.it/).
	**CONFERIMENTO DEI DATI PERSONALI**	Il conferimento dei suoi dati personali sarà necessario per la gestione della segnalazione. In caso di rifiuto, il Titolare procederà in ogni caso ad intraprendere l'attività di indagine mantenendo l'anonimato della sua persona. L'eventuale rifiuto a fornire i dati relativi i soggetti coinvolti nella segnalazione, comporterà l'impossibilità di gestire la segnalazione e procedere alle indagini.
	**ESISTENZA DI UN PROCESSO DECISIONALE AUTOMATIZZATO**	I dati personali raccolti non saranno soggetti ad un processo decisionale automatizzato.