Segnalazioni Whistleblowing

Linee guida per i segnalanti

Indice

1. Scopo 3
2. Chi può segnalare 3
3. Quando utilizzare il canale di segnalazione 3
4. Come effettuare una segnalazione 4
4.1 Canali disponibili 4
4.2 Contenuto minimo della segnalazione 4
4.3 Segnalazioni anonime 5
5. Come viene gestita la segnalazione 5
6. Tutele per il segnalante 5
6.1 Riservatezza 5
6.2 Divieto di ritorsione e misure di protezione 6
7. Responsabilità e sanzioni 6
8. Segnalazione esterna all'ANAC 6

1. Scopo

Crédit Agricole Vita S.p.A. (la "Compagnia") ha adottato un sistema di segnalazione delle violazioni (whistleblowing) con l'obiettivo di agevolare la segnalazione di illeciti e tutelare chi segnala. Il presente documento sintetizza il Regolamento per le segnalazioni whistleblowing approvato dal Consiglio di Amministrazione e fornisce indicazioni su chi può segnalare, cosa segnalare, come utilizzare il canale messo a disposizione, come viene gestita la segnalazione e quali tutele sono previste.

Il sistema è adottato in conformità, tra l'altro, al D.Lgs. 10 marzo 2023, n. 24 (Decreto Whistleblowing), agli artt. 10-quater e 10-quinquies del Codice delle Assicurazioni Private, al D.Lgs. 231/2001, al D.Lgs. 231/2007 (Antiriciclaggio) e al Regolamento (UE) 2016/679 (GDPR).

2. Chi può segnalare

Possono effettuare una segnalazione:

- dipendenti e collaboratori;
- azionisti e persone che esercitano, anche di mero fatto, funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza della Compagnia;
- soggetti terzi che interagiscono con la Compagnia, compresi fornitori, consulenti e intermediari;
- stagisti, lavoratori in prova, candidati a rapporti di lavoro ed ex dipendenti.

Le stesse tutele del segnalante si applicano ai "Soggetti Collegati": facilitatori; persone del medesimo contesto lavorativo legate al segnalante da stabile legame affettivo o di parentela entro il quarto grado; colleghi con cui il segnalante ha un rapporto abituale e corrente; enti di proprietà del segnalante o per i quali lavora, o che operano nel medesimo contesto lavorativo.

3. Quando utilizzare il canale di segnalazione

Il canale deve essere utilizzato per segnalare violazioni, accertate o presunte, di cui si è venuti a conoscenza nell'ambito dell'attività svolta in relazione alla Compagnia. In particolare:

- reati o illeciti amministrativi previsti dal Modello 231, compresa la corruzione;
- violazioni del Modello 231;
- violazioni del Codice Etico e delle procedure anticorruzione;
- violazioni di un obbligo internazionale;
- gravi e manifeste violazioni di legge o regolamento, con particolare riguardo ai provvedimenti IVASS e alla distribuzione assicurativa (IDD);
- violazioni, potenziali o effettive, della normativa antiriciclaggio;
- violazioni in materia di salute e sicurezza sul luogo di lavoro;
- illeciti nei settori indicati dal Decreto Whistleblowing: 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, salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata, protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti o omissioni che ledono gli interessi finanziari dell'Unione europea o riguardanti il mercato interno (inclusi concorrenza, aiuti di Stato e imposta sulle società), nonché atti che ne vanificano l'oggetto o la finalità.

Alcuni esempi

Ambito	Esempio di situazione da segnalare
Modello 231	Un collega non rispetta passaggi fondamentali di una procedura rilevante per il Modello 231 (ad es. autorizzazione dei pagamenti ai consulenti).
Reati 231	Un collega tenta di corrompere un esponente della società di revisione del bilancio della Compagnia.
Salute e sicurezza	In un'area degli uffici mancano o non sono manutenute le misure di sicurezza (ad es. carenza di estintori).
Antiriciclaggio	Un collega omette sistematicamente l'adeguata verifica della clientela o una segnalazione di operazione sospetta.
Codice Etico	Un collega adotta comportamenti scorretti nei confronti della clientela.
Normativa UE/nazionale	Aggiramento degli obblighi di tutela dei dati personali di controparti; omessi versamenti IVA; uso improprio di fondi UE.

Cosa non segnalare tramite questo canale

- Fatti, informazioni o documenti coperti da segreto relativo alla difesa nazionale, segreto medico o segreto professionale tra avvocato e assistito.
- Questioni di carattere personale estranee alle categorie sopra indicate (ad es. dissidi tra colleghi, contestazioni personali relative al rapporto di lavoro, dubbi sulle prospettive di crescita professionale). Tali situazioni possono essere affrontate tramite altri canali, come il superiore gerarchico o le Risorse Umane.

4. Come effettuare una segnalazione

4.1 Canali disponibili

La segnalazione può essere effettuata:

- **in forma scritta**, tramite il tool informatico BKMS System, che garantisce la riservatezza del segnalante e del contenuto della segnalazione, accessibile al seguente indirizzo: BKMS System
- **in forma orale**, su richiesta del segnalante, tramite incontro di persona con il Gestore delle segnalazioni. Previo consenso del segnalante, l'incontro è documentato mediante registrazione oppure mediante verbale, che il segnalante può verificare, rettificare e confermare con la propria sottoscrizione.

Il tool è accessibile dall'intranet aziendale per dipendenti e collaboratori e dal sito istituzionale anche per i soggetti terzi, come fornitori e sub-fornitori.

Le segnalazioni relative esclusivamente a violazioni dei principi del Codice Etico possono essere effettuate, in alternativa, anche secondo le modalità previste dal Codice Etico stesso.

4.2 Contenuto minimo della segnalazione

Per essere ammissibile e consentire un'adeguata istruttoria, la segnalazione deve contenere almeno:

1. una chiara e completa descrizione dei fatti;
2. l'indicazione di eventuali documenti che possano confermarne la fondatezza;
3. se conosciute, le circostanze di tempo e di luogo in cui i fatti sono stati commessi;
4. se conosciuti, le generalità o altri elementi (es. qualifica, servizio di appartenenza) che consentano di identificare l'autore dei fatti;

5. ogni altra informazione utile a riscontrare i fatti segnalati.

4.3 Segnalazioni anonime

Le segnalazioni anonime sono prese in considerazione a condizione che siano adeguatamente circostanziate e dettagliate (ad esempio, con menzione di specifiche aree aziendali, procedimenti o eventi).

> **Salute e sicurezza sul lavoro.** I lavoratori hanno l'obbligo (art. 20 D.Lgs. 81/2008) di segnalare immediatamente al datore di lavoro o ai soggetti incaricati le carenze dei dispositivi di sicurezza e le condizioni di pericolo. In questo caso può essere preferibile, nell'interesse del segnalante, non effettuare la segnalazione in forma anonima, per poter dimostrare, se necessario, di aver adempiuto all'obbligo.

5. Come viene gestita la segnalazione

Le segnalazioni sono ricevute e gestite dal Gestore delle segnalazioni, individuato nel Responsabile dell'Area Compliance, in condizioni di autonomia e indipendenza. Il Gestore può avvalersi di soggetti autorizzati della propria Funzione e, nel rispetto della riservatezza, di altri soggetti interni o esterni competenti (ad es. Risorse Umane, Internal Audit, Legal). In caso di conflitto di interessi del Gestore o dell'Area Compliance, la segnalazione è gestita dal gestore delle segnalazioni di Gruppo.

Fase	Cosa avviene
Ricezione	Il segnalante riceve un avviso di ricevimento entro 7 giorni.
Ammissibilità	Il Gestore verifica che la segnalazione provenga da un soggetto legittimato, rientri nel perimetro e sia sufficientemente precisa e circostanziata. Può chiedere informazioni integrative al segnalante.
Istruttoria	Il Gestore svolge verifiche e analisi sulla fondatezza dei fatti, anche tramite documenti integrativi, coinvolgimento di strutture interne o esperti esterni, audizioni. Per le segnalazioni relative al D.Lgs. 231/2001 è coinvolto l'Organismo di Vigilanza.
Riscontro	Il segnalante riceve un riscontro entro 3 mesi dal ricevimento. Se l'indagine è complessa, entro tale termine riceve un aggiornamento sull'attività in corso e un ulteriore riscontro alla conclusione.
Esito	La segnalazione è archiviata con motivazione se infondata; se fondata, è trasmessa agli organi e funzioni competenti per i provvedimenti del caso, inclusi quelli disciplinari.

Se la segnalazione riguarda un'altra società del Gruppo, il Gestore la trasmette al relativo referente entro 7 giorni, dandone notizia al segnalante.

6. Tutele per il segnalante

6.1 Riservatezza

L'identità del segnalante e ogni informazione da cui possa evincersi non possono essere rivelate, senza il suo consenso espresso, a persone diverse da quelle competenti a ricevere o dare seguito alla segnalazione. La riservatezza è estesa alle persone coinvolte e menzionate nella segnalazione fino alla conclusione dei procedimenti avviati.

L'identità del segnalante può essere rivelata solo previa comunicazione scritta e con il suo consenso esplicito qualora sia indispensabile per la difesa della persona cui è contestato un addebito disciplinare o di

altro procedimento fondato sulla segnalazione. In assenza di consenso, la segnalazione non può essere utilizzata nel procedimento disciplinare. Per le segnalazioni in materia antiriciclaggio, l'identità può essere rivelata solo con il consenso del segnalante o quando ciò sia indispensabile per la difesa del segnalato.

6.2 Divieto di ritorsione e misure di protezione

Le misure di protezione si applicano al segnalante e ai Soggetti Collegati se, al momento della segnalazione, il segnalante aveva fondato motivo di ritenere vere le informazioni e rientranti nel perimetro, e la segnalazione è stata effettuata in conformità al Regolamento e al Decreto Whistleblowing. Le misure comprendono:

- divieto di ritorsione in ragione della segnalazione;
- misure di sostegno gratuite (informazioni, assistenza, consulenza) da parte degli enti del terzo settore inclusi nell'elenco pubblicato sul sito ANAC;
- possibilità di comunicare all'ANAC le ritorsioni subite e nullità degli atti ritorsivi;
- limitazioni di responsabilità nei casi previsti dal Decreto Whistleblowing.

Le tutele si applicano anche alle segnalazioni anonime, se il segnalante viene successivamente identificato e subisce ritorsioni.

7. Responsabilità e sanzioni

Le segnalazioni devono essere effettuate in buona fede. Sono soggetti a sanzioni pecuniarie da parte dell'ANAC, oltre che a sanzioni disciplinari, coloro che compiono ritorsioni, ostacolano o tentano di ostacolare una segnalazione o violano gli obblighi di riservatezza.

Sono previste sanzioni disciplinari nei confronti del segnalante quando ne sia accertata la responsabilità penale (anche con sentenza di primo grado) per diffamazione o calunnia, ovvero la responsabilità civile per lo stesso titolo in caso di dolo o colpa grave.

8. Segnalazione esterna all'ANAC

Fermo restando la priorità del canale interno, è possibile effettuare una segnalazione esterna tramite il canale dell'ANAC, esclusivamente per le violazioni del diritto UE e nazionale nei settori indicati dal Decreto Whistleblowing, e solo se:

- il canale interno non è attivo;
- è già stata effettuata una segnalazione interna senza seguito;
- vi sono fondati motivi di ritenere che alla segnalazione interna non sarebbe dato seguito o che possa determinare rischio di ritorsione;
- vi è fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per l'interesse pubblico.

Per la segnalazione esterna e per la divulgazione pubblica si rinvia alle linee guida e al sito ufficiale dell'ANAC: Canale ANAC.

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.