



Procedura per l'utilizzo e la gestione del sistema di segnalazione delle violazioni

GRUPPO CERVED



INDICE

1.	Obiettivo	3
2.	Ambito di applicazione	4
3.	Definizioni	5
4.	Principi generali	6
5.	Condotte segnalabili	8
6.	Processo di gestione delle segnalazioni	10
6.1.	Canali di segnalazione e canali alternativi	10
6.2.	Segnalazioni anonime	12
6.3.	Accesso al canale digitale di segnalazione e invio delle segnalazioni	12
6.4.	Presa in carico e valutazione preliminare	14
6.5.	Valutazione	14
6.6.	Decisione	15
6.7.	Reporting	16
6.8.	Flussi informativi in merito alle segnalazioni rilevanti.....	16
6.9.	Informativa al segnalato.....	17
6.10.	Interesse privato e corresponsabilità del segnalante	17
6.11.	Rivelazione dell'identità del segnalante	17
6.12.	Trattamento dei dati personali	18
7.	Adozione della Procedura e informazione ai Destinatari	19
8.	Supporto e assistenza	19
9.	Tracciabilità del processo di gestione delle segnalazioni.....	19
10.	Aggiornamento della procedura.....	20

1. Obiettivo

Il Gruppo Cerved svolge il proprio business con lealtà, correttezza, trasparenza, onestà, integrità e nel rispetto delle leggi, regolamenti e normative in genere, standard e linee guida, sia nazionali sia internazionali, che si applicano alle attività del Gruppo.

Il Gruppo promuove l'adozione di strumenti volti a prevenire, scoprire e comunicare condotte illecite e/o comunque poste in essere in violazione dei principi etici perorati dal Gruppo. **Per questo, si incoraggiano tutti i legali rappresentanti, amministratori, dirigenti e dipendenti delle società del Gruppo nonché si invitano tutti gli altri soggetti terzi che interagiscono con il Gruppo a segnalare qualsiasi violazione rilevante ai fini della presente Procedura di cui gli stessi vengano a conoscenza.**

Per consentire l'effettuazione di tali segnalazioni, il Gruppo Cerved ha adottato il **Sistema di Segnalazione**, oggetto della presente Procedura, che ha le seguenti caratteristiche:

- è un sistema multicanale, comprensivo anche di un'avanzata piattaforma *web*, del tutto separata e indipendente dai sistemi informatici del Gruppo, che consente di effettuare le segnalazioni da qualunque dispositivo, in modo altamente confidenziale e facilitato, garantendo la protezione dei dati identificativi dei segnalanti;
- è un sistema unico per tutto il Gruppo Cerved, e gestito a livello centrale (sono in ogni caso garantiti i necessari flussi informativi previsti nell'ambito del processo di gestione delle segnalazioni verso gli organi delle società del Gruppo interessati dalla segnalazione, in ragione della materia trattata o dei soggetti coinvolti);
- garantisce elevati *standard* di riservatezza delle informazioni e della identità del segnalato e del segnalante, lasciando la possibilità al segnalante di inserire la segnalazione anche in modalità anonima.

Scopo della presente Procedura è quello di illustrare i principi posti a salvaguardia dei soggetti segnalanti, le modalità di invio delle segnalazioni, il relativo processo di gestione, nonché ogni possibile azione conseguente alle violazioni riscontrate.

Il *training* sulla presente Procedura costituisce parte del processo di formazione dei destinatari della stessa e viene realizzato su base regolare, a seconda delle necessità.

2. Ambito di applicazione

Il rispetto delle leggi, delle regole del Gruppo Cerved e, in particolare, di questa Procedura è obbligatorio per tutte le Persone di Cerved. La procedura si applica a Cerved Group SpA e alle Società da essa controllate nell'ambito dell'attività di direzione e coordinamento esercitata; alle segnalazioni ricevute da Cerved e/o dalle società controllate, in Italia e all'estero.

La Procedura è stata esaminata e approvata, per la prima volta, dal Consiglio di Amministrazione di Cerved Group SpA il **29 ottobre 2018** e la sua adozione e attuazione è obbligatoria per tutte le società del Gruppo.

Ciascuna società del Gruppo Cerved adotterà questa Procedura e nominerà il proprio Responsabile del Sistema tramite deliberazione del proprio Consiglio di Amministrazione (o del corrispondente organo/funzione/ruolo qualora la governance della rispettiva società controllata non preveda tale organo) tempestivamente nel corso della prima riunione utile e in ogni caso entro e non oltre 120 giorni dall'approvazione della Procedura da parte del Consiglio di Amministrazione di Cerved Group SpA.

Le società che dovessero essere costituite e/o entrare a far parte del Gruppo Cerved successivamente all'approvazione della presente Procedura adotteranno la Procedura e nomineranno il proprio Responsabile del Sistema tramite deliberazione del proprio Consiglio di Amministrazione (o del corrispondente organo/funzione/ruolo qualora la governance della rispettiva società controllata non preveda tale organo) tempestivamente nel corso della prima riunione utile e in ogni caso entro e non oltre 90 giorni dalla data di costituzione o, a seconda dei casi, dall'ingresso nel Gruppo Cerved.

La presente procedura è stata predisposta anche in linea con gli adempimenti ed i requisiti previsti dallo standard UNI ISO 37001 – Sistemi di gestione anticorruzione.

3. Definizioni

- **CANALE DIGITALE DI SEGNALAZIONE:** il canale *web* per la ricezione delle segnalazioni e la relativa piattaforma digitale di gestione delle segnalazioni accessibile per le Persone di Cerved e per i soggetti terzi che interagiscono con il Gruppo attraverso il sito internet company.cerved.com.
- **CANALI DI SEGNALAZIONE ALTERNATIVI INTERNI:** ulteriori canali interni per la ricezione delle segnalazioni mediante posta elettronica, posta ordinaria ed in forma orale.
- **CANALI DI SEGNALAZIONE ESTERNI:** ovvero canali di segnalazione esterni a Cerved, ai quali il segnalante può rivolgersi sia avendo effettuato precedentemente una segnalazione mediante uno dei canali interni (ivi incluso il canale digitale di segnalazione), sia ricorrendo direttamente ai canali di segnalazione messi a disposizione dalle autorità e, se del caso, a istituzioni, organi e organismi dell'Unione di volta in volta competenti per la materia oggetto di segnalazione¹.
- **CERVED o GRUPPO CERVED o GRUPPO:** Cerved Group S.p.A. e le società nei confronti delle quali Cerved Group S.p.A. esercita attività di direzione e coordinamento.
- **CODICE DI ACCESSO:** il codice di accesso, univoco per tutte le Persone di Cerved, fornito per accedere al Canale Digitale di Segnalazione.
- **CODICE DI ACCESSO SOGGETTI TERZI:** il codice di accesso, univoco per tutti i soggetti diversi dalle Persone di Cerved, fornito per accedere al Canale Digitale di Segnalazione.
- **CODICE ETICO:** documento che esplicita i valori ed i principi di riferimento che disciplinano l'attività ed i rapporti verso tutti i soggetti con cui il Gruppo entra in relazione per il conseguimento del proprio oggetto sociale.
- **FUNZIONE / ORGANO COMPETENTE:** la funzione e/o l'organo incaricati di individuare le possibili azioni correttive idonee a porre rimedio alle conseguenze della violazione e proporre, eventualmente, l'adozione di eventuali misure disciplinari. Con esclusivo riferimento al D. Lgs. 231/2001 la funzione competente è sempre l'Organismo di Vigilanza nominato dalla Società del Gruppo cui attiene la segnalazione.
- **MODELLO 231:** il Modello di Organizzazione, Gestione e Controllo adottato da ciascuna società del Gruppo Cerved ai sensi del Decreto Legislativo 231/2001.
- **PERSONE DI CERVED:** componenti degli Organi Sociali, tutti i Dipendenti e, più in generale, tutti i soggetti che svolgono in favore di Cerved la propria attività lavorativa e ogni altro soggetto, persona fisica o giuridica, con cui Cerved entri in contatto nello svolgimento di relazioni d'affari.

¹ Dir. UE 2019/1937, art. 9, par. 1, lett. g).

- **RESPONSABILE DEL SISTEMA:** è identificato nel Responsabile della Funzione Internal Audit, per tutte le società del Gruppo, salvo che per le società Cerved Rating Agency S.p.A. e Cerved Master Services S.p.A. per le quali è identificato nel Responsabile della Funzione Compliance. Il Responsabile del Sistema ha il compito di assicurare lo svolgimento del procedimento di gestione delle segnalazioni in conformità alle normative in vigore. Qualora il Responsabile del Sistema versi in una delle situazioni di cui al successivo § 6.1, la gestione delle segnalazioni è affidata al gestore alternativo indicato nel sopra citato paragrafo.
- **SEGNALAZIONE RILEVANTE (O SEGNALAZIONI RILEVANTI):** segnalazione che presenta almeno una delle seguenti caratteristiche:
 - a) ha ad oggetto atti o fatti che coinvolgono amministratori o membri dell'organo di controllo di una società del Gruppo Cerved;
 - b) ha ad oggetto atti o fatti che coinvolgono l'Amministratore Delegato e l'alta dirigenza di una società del Gruppo Cerved;
 - c) ha ad oggetto atti o fatti di rilevanza penale;
 - d) ha ad oggetto atti o fatti che coinvolgono le Persone di Cerved di più strutture aziendali o di più società del Gruppo;
 - e) può comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo o significativi impatti sulla situazione finanziaria o patrimoniale del Gruppo, danni di reputazione e/o malfunzionamenti di procedure informatiche critiche;
 - f) ha ad oggetto atti o fatti che possono avere un impatto economico rilevante in termini di reputazione o di sanzioni;
 - g) ha ad oggetto violazioni ripetute sistematicamente; e/o
 - h) ha un impatto significativo sul sistema di controllo interno del Gruppo.
- **SISTEMA DI SEGNALAZIONE o SISTEMA:** il sistema multicanale per la ricezione e la gestione delle segnalazioni oggetto della presente Procedura.

4. Principi generali

Il funzionamento del Sistema di Segnalazione si basa sui seguenti principi fondamentali:

- **Accesso:** al fine di effettuare una segnalazione, al Sistema possono accedere solamente i Destinatari (come definiti nel punto successivo).
- **Destinatari:** tutte le Persone di Cerved e tutti i soggetti terzi che interagiscono con il Gruppo sono autorizzati a effettuare segnalazioni attraverso il Sistema descritto nella presente Procedura.
- **Dovere di segnalare condotte illecite:** i Destinatari hanno il dovere di segnalare le violazioni di cui vengano a conoscenza o di cui abbiano un ragionevole sospetto.

- **Divieto di atti ritorsivi, vessatori o discriminatori verso il segnalante:** i segnalanti sono tutelati contro qualsiasi atto ritorsivo, vessatorio o discriminatorio, diretto o indiretto, per motivi collegati, direttamente o indirettamente, alla segnalazione; tale protezione è garantita al segnalante anche quando la segnalazione, seppur infondata, si basi su criteri di buona fede e ragionevolezza. In caso di violazione di tale divieto è prevista l'instaurazione di un apposito procedimento disciplinare. A tal fine, il Responsabile del Sistema, con l'ausilio della Funzione Human Resources del Gruppo, monitora eventuali comportamenti ritorsivi, sleali, vessatori e discriminatori nei confronti dei soggetti segnalanti, attraverso l'analisi e la valutazione complessiva di appositi "*Red Flags*" (a titolo esemplificativo: cambi di ufficio o di mansione, trasferimenti di sede, richieste di modifica mansioni, lunghe assenze per malattia, contestazioni/provvedimenti disciplinari, richieste di aspettativa non retribuita, valutazioni negative della performance, ecc.). I segnalanti che dovessero ritenere di aver subito condotte ritorsive o vessatorie, in conseguenza di una valutazione precedentemente effettuata, sono invitati ad inoltrare una nuova segnalazione avente ad oggetto le ritorsioni subite. In tali casi è garantito lo svolgimento tempestivo delle relative indagini da parte del Responsabile del Sistema, con il supporto delle funzioni interessate dai fatti oggetto di segnalazione.
- **Divieto di comportamenti volti ad ostacolare le segnalazioni²:** tenendo conto del punto precedentemente illustrato, è parimenti vietato qualsiasi comportamento volto ad ostacolare l'effettuazione di una segnalazione. In caso di violazione di tale divieto è prevista l'instaurazione di un apposito provvedimento disciplinare. I segnalanti (o in generale i Destinatari) che dovessero ritenere di aver subito comportamenti ostativi in tal senso, sono tenuti a comunicarlo in occasione della segnalazione stessa.
- **Divieto di effettuare segnalazioni manifestamente infondate e/o diffamatorie:** è vietato effettuare segnalazioni manifestamente infondate e/o effettuate con dolo a fini diffamatori; in caso di segnalazioni manifestamente infondate e/o diffamatorie, potranno essere intraprese iniziative a carattere disciplinare per la tutela di Cerved e del segnalato.
- **Dovere di indipendenza e professionalità nella gestione delle segnalazioni:** tutti i soggetti coinvolti, a qualsivoglia titolo, nel processo di gestione delle segnalazioni devono svolgere i relativi compiti nel rispetto dei doveri di indipendenza e garantendo l'accurata ed efficiente gestione di tutte le segnalazioni.
- **Tutela dell'identità del segnalante e della riservatezza delle informazioni:** Cerved garantisce la confidenzialità dell'identità del segnalante e la riservatezza delle informazioni contenute nelle segnalazioni in ogni fase del processo di segnalazione, nei limiti in cui l'anonimato e la riservatezza siano opponibili in base alle norme di legge; le misure a tutela della riservatezza del

² Dir. UE 2019/1937, art. 23, par. 1, lett. dalla a) alla d).

segnalante sono volte, tra l'altro, a garantire che lo stesso non sia soggetto ad alcuna forma di ritorsione. La violazione di tale principio può comportare l'avvio di un procedimento disciplinare nei confronti dell'autore di tale violazione e l'irrogazione delle relative misure disciplinari, conformemente a quanto previsto dalla normativa giuslavoristica nazionale applicabile.

- **Tutela del segnalato:** i soggetti segnalati sono tutelati per quanto attiene sia alla confidenzialità delle segnalazioni che li riguardano e delle eventuali indagini svolte, sia alla protezione degli stessi da eventuali segnalazioni ritorsive e/o diffamatorie.
- **Tutela dell'integrità delle segnalazioni:** il Canale Digitale di Segnalazione garantisce che nessuna segnalazione (dalla fase della notifica a quella della decisione) possa essere cancellata e/o alterata.
- **Divieto di rinuncia ai diritti³:** i diritti e i mezzi di ricorso previsti dalla direttiva 2019/1937 non possono essere oggetto di rinuncia o limitazione in virtù di accordi, regimi, forme o condizioni di lavoro, compreso un accordo arbitrale precontenzioso.

5. Condotte segnalabili

La presente Procedura trova applicazione con riguardo alle segnalazioni che hanno ad oggetto violazioni che possano avere impatto sulle società del Gruppo Cerved e sull'attività dalle stesse esercitata.

In particolare, attraverso il Sistema di Segnalazione è possibile segnalare atti o fatti che coinvolgono legali rappresentanti, amministratori, dirigenti e/o dipendenti del Gruppo Cerved, delle società non controllate nelle quali il Gruppo detiene partecipazioni rilevanti, delle *joint venture* e/o – in ogni caso – chiunque agisca in nome, per conto o nell'interesse di Cerved (a titolo esemplificativo: consulenti, fornitori, agenti, etc.).

Gli atti o fatti oggetto di segnalazioni possono riguardare i seguenti aspetti:

- in relazione a tutte le società del Gruppo:
 - ✓ violazioni del Codice Etico di Gruppo,
 - ✓ condotte illecite, rilevanti ai sensi del D. Lgs. 231/2001 e violazioni del Modello 231 adottato dalle società del Gruppo,
 - ✓ violazioni delle procedure adottate dalle Società del Gruppo, in particolare violazioni del Sistema di Gestione Anticorruzione, della Politica Anticorruzione di Gruppo e/o della Procedura "Due diligence anti-corrruzione delle Terze Parti Rilevanti" nonché della

³ Dir. UE 2019/1937, art. 24.

- procedura in materia di conflitto di interesse e le procedure collegate al programma di compliance antitrust;
- ✓ condotte illecite, rilevanti ai sensi delle normative applicabili alle attività svolte dal Gruppo (ad es. Normativa antitrust, Normativa anticorruzione, Normativa di diritto dell'Unione Europea ...)
 - ✓ violazioni del Codice di Autodisciplina delle Società Quotate predisposto dal *Comitato per la Corporate Governance* di Borsa Italiana,
 - ✓ tematiche di *business integrity* (ad esempio, furti, condotte scorrette nella gestione degli affari, utilizzo non corretto delle risorse aziendali, eventi dannosi che coinvolgono la clientela, conflitti di interesse), che includono anche quanto relativo a potenziali atti di corruzione, compiuti, tentati o presunti (sia in senso attivo sia in senso passivo), e/o
 - tematiche di *financial integrity* (ad esempio, *insider trading*, violazioni in materia contabile, frodi societarie), in relazione alle società del Gruppo Cerved che esercitano attività di recupero crediti, oltre a quanto sopra previsto con riferimento a tutte le società del Gruppo, violazioni della normativa in materia di antiriciclaggio di cui al D. Lgs. n. 90/2017 e smi;
 - in relazione a Cerved Master Services S.p.A., oltre a quanto sopra previsto con riferimento a tutte le società del Gruppo:
 - ✓ violazioni della normativa che disciplina l'attività bancaria, intesa come le attività principali e strumentali indicate nell'art. 10, commi 1, 2 e 3, TUB, (ivi incluse le Disposizioni di vigilanza per le banche emanate da Banca d'Italia), e/o
 - ✓ violazioni della normativa in materia antiriciclaggio di cui al D. Lgs. n. 90/2017 e smi;
 - in relazione a Cerved Rating Agency S.p.A., oltre a quanto sopra previsto in relazione a tutte le società del Gruppo, violazioni del Regolamento n. 1060/2009 del Parlamento Europeo e del Consiglio del 16 settembre 2009 e smi, relativo alle agenzie di rating del credito, nonché le normative e procedure interne di Cerved Rating Agency S.p.A..

Le suddette violazioni non devono essere riportate attraverso il Sistema nel caso in cui le stesse siano emerse nell'ambito di audit, ovvero di qualunque ulteriore attività investigativa.

Si rammenta che il Sistema non va utilizzato per rimostranze di carattere personale del segnalante o rivendicazioni/istanze che rientrano nella disciplina del rapporto di lavoro o rapporti col superiore gerarchico o colleghi, per le quali occorre fare riferimento alla funzione Human Resources di Gruppo.

I clienti Cerved che desiderano segnalare problematiche di natura commerciale e/o relative ai servizi del Gruppo possono farlo attraverso i canali dedicati disponibili sul sito www.cerved.com.

6. Processo di gestione delle segnalazioni

6.1. CANALI DI SEGNALAZIONE E CANALI ALTERNATIVI

6.1.1 CANALE DIGITALE DI SEGNALAZIONE E CANALI ALTERNATIVI INTERNI

Le segnalazioni devono essere inviate attraverso il Canale Digitale di Segnalazione – in quanto appositamente studiato per garantire facilità di utilizzo, anonimato, confidenzialità e riservatezza e ciò, quindi, anche per la migliore protezione dei segnalanti – accessibile da qualsiasi pc, tablet o smartphone (sia privati che aziendali).

I segnalanti possono ricorrere ai **canali interni alternativi** al Canale Digitale di Segnalazione successivamente indicato al par. 6.3:

- **posta elettronica ai seguenti indirizzi**, accessibili esclusivamente al Responsabile del Sistema di ciascuna società del Gruppo:

- (i) per Cerved Master Services S.p.A.: whistleblowingCMS@cerved.com;
- (ii) per Cerved Rating Agency S.p.A.: whistleblowingCRA@cerved.com;
- (iii) per tutte le altre Società del Gruppo: whistleblowing@cerved.com;

- **posta ordinaria** agli indirizzi di ciascuna società del Gruppo presso la rispettiva sede legale, all'attenzione del Responsabile del Sistema.

In caso di utilizzo di modalità differenti dal Canale Digitale di Segnalazione per l'invio delle segnalazioni, al fine di usufruire di una maggiore garanzia di riservatezza, è necessario che la segnalazione venga inserita in una busta chiusa che rechi all'esterno la dicitura "riservata/personale" oppure che l'oggetto della email contenga la predetta dicitura.

- **Segnalazioni in forma orale**, per via telefonica o attraverso altri sistemi di messaggistica vocale, o, su richiesta del segnalante stesso, mediante un incontro diretto entro un termine ragionevole dall'avanzamento della rispettiva richiesta⁴.

Se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, subordinatamente al consenso del segnalante, il Responsabile del Sistema ha il diritto di documentare la segnalazione orale facendo una registrazione della conversazione su un supporto durevole che consenta l'accesso alle informazioni, oppure mediante una trascrizione completa e accurata della conversazione. È consentito al segnalante di verificare, rettificare e approvare la trascrizione della chiamata mediante l'apposizione della propria firma⁵.

Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato, il Responsabile del Sistema ha il diritto di documentare la

⁴ Dir. UE 2019/1937, art. 9, par. 2.

⁵ *Ivi*, Art. 18, par. 2.

segnalazione orale mediante un resoconto dettagliato della conversazione. Al segnalante è offerta la possibilità di verificare, rettificare e approvare il resoconto della conversazione mediante l'apposizione della propria firma⁶.

Se per la segnalazione il segnalante richiede un incontro con il Responsabile del Sistema, quest'ultimo assicura, subordinatamente al consenso della persona segnalante, che sia conservata una documentazione completa e accurata di tale incontro su un supporto durevole che consenta l'accesso alle informazioni. Il Responsabile del Sistema ha il diritto di documentare l'incontro facendo una registrazione della conversazione su un supporto durevole che consenta l'accesso alle informazioni, oppure mediante un verbale dettagliato dell'incontro. Al segnalante è offerta la possibilità di verificare, rettificare e approvare il verbale dell'incontro mediante l'apposizione della propria firma⁷.

Si precisa che anche le segnalazioni pervenute attraverso canali interni alternativi al Canale Digitale di Segnalazione verranno in seguito inserite nel Canale Digitale di Segnalazione.

Si rinnova tuttavia l'invito a utilizzare il Canale Digitale di Segnalazione, salvo che per ragioni di carattere tecnico non sia possibile accedervi, poiché:

- i. l'uso di canali alternativi non può garantire il medesimo livello di protezione dei segnalanti e di efficienza nella gestione delle segnalazioni;
- ii. in caso di segnalazione anonima, l'uso del Canale Digitale di Segnalazione è l'unica modalità che consente di chiedere chiarimenti al segnalante, mantenendo il suo anonimato, sulla base delle modalità descritte al successivo paragrafo 6.2.

Chiunque riceva una segnalazione attraverso canali interni alternativi al Canale Digitale di Segnalazione deve prontamente inoltrarla al Responsabile del Sistema - o ad uno dei soggetti di seguito indicati come "Gestore Alternativo" - il quale provvederà a inserirla nel Canale Digitale di Segnalazione.

Al fine di evitare che il Responsabile del Sistema, in relazione a una specifica segnalazione, possa trovarsi in una delle seguenti situazioni:

- i. essere gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato;
- ii. essere il presunto responsabile della violazione; o
- iii. avere un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio,

⁶ Dir. UE 2019/1937, art. 18, par. 3.

⁷ *Ivi*, art. 18, par 4.

è prevista la presenza di un Gestore Alternativo al quale rivolgersi quando il Responsabile del Sistema si trovi in una delle situazioni di potenziale “conflitto d’interessi” sopra elencate. Il Gestore Alternativo è l’**Organismo di Vigilanza** della società del Gruppo di volta in volta interessata. Le comunicazioni al Gestore Alternativo andranno inoltrate all’Organismo di Vigilanza di volta in volta competente direttamente attraverso il sistema di segnalazione.

Nelle situazioni di conflitto di interessi sopra elencate il Gestore Alternativo assume tutti i compiti propri del Responsabile del Sistema nell’ambito delle fasi di gestione della segnalazione; il Gestore Alternativo può essere attivato direttamente dal segnalante al momento dell’invio della segnalazione oppure, nella fase di valutazione preliminare della segnalazione, dal Responsabile del Sistema.

6.1.2 CANALI DI SEGNALAZIONE ESTERNI

È sempre prevista la possibilità per il segnalante di effettuare la segnalazione anche mediante l’utilizzo di **canali di segnalazione esterni**⁸, sia dopo aver utilizzato uno dei canali interni di cui al precedente punto 6.1.1, sia effettuando la segnalazione direttamente attraverso i canali di segnalazione esterni⁹ messi a disposizione dalle autorità e, se del caso, da istituzioni, organi e organismi dell’Unione¹⁰ di volta in volta competenti per la materia oggetto di segnalazione.

6.2. SEGNALAZIONI ANONIME

Cerved prevede la possibilità di effettuare segnalazioni in forma anonima¹¹. Queste saranno prese in carico e gestite, al pari delle segnalazioni nominative, per quanto attiene tutte le condotte segnalabili di cui al punto 5 della presente procedura. Le modalità attraverso cui verrà raccolta la segnalazione anonima sono esplicitate al successivo punto 6.3.

In ogni caso, dal momento che le segnalazioni nominative agevolano l’interazione con il segnalante e la richiesta di chiarimenti allo stesso, assicurando, al contempo, massima tutela e riservatezza per il segnalante e protezione dalle segnalazioni ritorsive e/o diffamatorie, le segnalazioni nominative sono fortemente incoraggiate¹².

6.3. ACCESSO AL CANALE DIGITALE DI SEGNALAZIONE E INVIO DELLE SEGNALAZIONI

Per accedere al Canale Digitale di Segnalazione (<https://ewhistle.cerved.com>) a tutte le Persone di Cerved viene fornito un identico Codice di Accesso, che dovrà essere custodito riservatamente senza essere reso noto a terzi. Analogamente, ai soggetti terzi che interagiscono con il Gruppo viene

⁸ Dir. UE 2019/1937, art. 9, par. 1, lett. g).

⁹ *Ivi*, art. 10.

¹⁰ Art. 9, par. 1, lett. g), dir. UE 2019/1937.

¹¹ *Ivi*, art. 9, par. 1, lett. e).

¹² Parere EDPB WP117 del 2006, par. 1, punto iii.

reso noto un Codice di Accesso Soggetti Terzi, uguale per tutti i soggetti terzi e differente dal Codice di Accesso.

Il Codice di Accesso e il Codice di Accesso Soggetti Terzi, essendo uguali – rispettivamente - per tutte le Persone di Cerved e per tutti i soggetti terzi, non consentono di identificare il singolo utente che accede al Canale Digitale di Segnalazione. Ciò assume particolare rilievo in relazione alle segnalazioni anonime.

In caso di segnalazione anonima, il segnalante immette nella pagina “compilativa” del Canale Digitale di Segnalazione direttamente la violazione riscontrata (compilando tutti i campi ivi richiesti).

In caso di segnalazione nominativa, il segnalante inserisce i propri dati identificativi negli appositi campi della pagina compilativa del Canale Digitale di Segnalazione e riporta la violazione riscontrata (compilando tutti i campi ivi richiesti).

Il Canale Digitale di Segnalazione consente al segnalante di inserire la segnalazione selezionando la tipologia a cui si riferisce la condotta illecita (D. Lgs. 231/01, Codice Etico, Antiriciclaggio, normativa bancaria, anticorruzione, etc.) e di indicare la società del Gruppo alla quale la segnalazione si riferisce.

La segnalazione deve:

- contenere una precisa descrizione dei fatti oggetto della segnalazione e delle persone coinvolte (potenziali responsabili e possibili testimoni);
- essere integrata allegando eventuale documentazione a supporto del fatto contestato, utilizzando l'apposita funzione di *upload* dei documenti.

Ricevuta la segnalazione, il Canale Digitale di Segnalazione rende anonimi i dati del segnalante e del segnalato e li inserisce automaticamente in un archivio separato gestito con modalità informatiche dal Responsabile del Sistema ed accessibile solo a quest'ultimo, nel quale tali dati verranno custoditi. I dati personali contenuti in ciascun archivio sono criptati mediante l'utilizzo di chiavi di criptazione dedicate e differenti.

Il Canale Digitale di Segnalazione visualizza quindi una informativa iniziale di conferma della ricezione e presa in carico della segnalazione e fornisce il **codice identificativo univoco** della segnalazione, attraverso il quale il segnalante potrà accedere al Canale Digitale di Segnalazione per verificare eventuali richieste di chiarimenti e lo stato di valutazione della segnalazione. Tale codice non consente di identificare in alcun modo il segnalante, che pertanto può rimanere anonimo e, nello stesso tempo, accedere alla segnalazione, verificarne lo stato e rispondere a eventuali richieste di chiarimento.

Si raccomanda al segnalante di accedere periodicamente al Canale Digitale di Segnalazione per verificare l'eventuale presenza di richieste di chiarimenti relative alla segnalazione inoltrata. A tale riguardo, si precisa che eventuali richieste di integrazioni/chiarimenti verranno trasmesse al

segnalante entro e non oltre 20 giorni lavorativi dalla comunicazione della segnalazione attraverso il Canale Digitale di Segnalazione.

È dovere di ciascun segnalante custodire diligentemente il codice identificativo univoco della segnalazione, non rilasciarlo ad altri e non consentire a terzi di accedere alle informazioni sulla segnalazione.

6.4. PRESA IN CARICO E VALUTAZIONE PRELIMINARE

Ricevuta la segnalazione, il Canale Digitale di Segnalazione provvede a trasmettere un avviso di ricezione di una nuova segnalazione (senza fornire informazioni in merito al contenuto della segnalazione medesima) alla casella di posta elettronica del Responsabile del Sistema.

All'avvenuta ricezione di una segnalazione (sia mediante il Canale Digitale di Segnalazione sia mediante i canali alternativi) il Responsabile del Sistema effettua una valutazione preliminare e procede alla classificazione della segnalazione, sulla base della relativa natura.

In questa fase, il Responsabile del Sistema può ignorare e non gestire (“cestinare”) immediatamente le segnalazioni che risultino palesemente infondate, strumentali o al di fuori dell’ambito di applicazione della presente Procedura. Anche le segnalazioni “cestate” sono salvate nell’archivio informatico del Canale Digitale di Segnalazione, che non consente alcuna forma di cancellazione e/o alterazione (cfr. § 9). Si precisa che le segnalazioni che non rientrano nell’ambito di applicazione oggettivo della presente Procedura si considereranno come non ricevute e pertanto non saranno tenute in alcuna considerazione né verranno trasmesse ad altri organi/funzioni sociali eventualmente competenti in relazione all’oggetto delle stesse.

Qualora, nel corso della gestione della segnalazione, emergano situazioni di potenziale conflitto di interessi, il Responsabile del Sistema non può procedere a “cestinare” e provvede all’adozione delle misure ritenute più idonee a garantire la corretta gestione della segnalazione. In tal caso trova applicazione quanto previsto al successivo § 6.8.

La fase di presa in carico deve concludersi entro 10 giorni lavorativi dalla ricezione della segnalazione.

6.5. VALUTAZIONE

Il Responsabile del Sistema verifica, per le segnalazioni che non siano state immediatamente “cestate”, se ciascuna di esse è corredata da elementi sufficienti per valutarne la fondatezza; qualora la segnalazione, pur non palesemente infondata, strumentale o al di fuori dell’ambito di applicazione della presente Procedura, risulti non sufficientemente dettagliata, il Responsabile del Sistema formula le opportune richieste di integrazioni/chiarimenti al segnalante.

Tali richieste di integrazioni/chiarimenti verranno trasmesse al segnalante entro e non oltre 20 giorni lavorativi dalla comunicazione della segnalazione attraverso il Canale Digitale di Segnalazione.

Effettuata tale prima valutazione e ottenuti i chiarimenti ritenuti opportuni, il Responsabile del Sistema procede:

- all'archiviazione delle segnalazioni che, a seguito dell'esame preliminare, risultino prive di fondamento e/o non adeguatamente documentate, nonostante i chiarimenti ottenuti

ovvero

- con la fase istruttoria, per le segnalazioni che, a seguito della verifica preliminare, siano risultate ragionevolmente fondate e supportate da elementi sufficienti per procedere con la fase istruttoria.

In tale ultimo caso, il Responsabile del Sistema definisce uno specifico "piano di investigazione", in cui sono individuate:

- le modalità di svolgimento dell'investigazione (richieste di integrazioni/chiarimenti al segnalante, svolgimento degli accertamenti ritenuti necessari, etc.);
- le possibili società del Gruppo e/o funzioni aziendali competenti sulla materia ed eventualmente per territorio; e
- le tempistiche entro cui concludere l'investigazione.

Gli organi delle società del Gruppo e/o le funzioni aziendali coinvolte nel "piano di investigazione" devono garantire piena collaborazione al Responsabile del Sistema per quanto necessario allo svolgimento dell'istruttoria, nel rispetto dei principi e delle garanzie previsti da questa procedura.

Al termine della fase istruttoria, il Responsabile del Sistema predispone una relazione sugli esiti delle indagini effettuate.

In ogni caso, la fase di valutazione è completata entro 40 giorni lavorativi dalla ricezione della segnalazione - fatti salvi i casi in cui segnalazioni relative a situazioni di particolare complessità richiedano tempi di valutazione più lunghi e comunque non superiori a 60 giorni lavorativi - nel rispetto dei principi di imparzialità, competenza e diligenza professionale.

6.6. DECISIONE

Sulla base di quanto emerso nel corso dell'istruttoria, il Responsabile del Sistema individua la funzione/organo aziendale competente ad esprimere la decisione in merito a ciascuna segnalazione nonché ad individuare le possibili azioni correttive idonee a porre rimedio alle conseguenze della violazione e a prevenire il rischio di violazioni analoghe a quella oggetto della segnalazione e trasmette a tale organo/funzione la relazione predisposta al termine della fase istruttoria.

L'organo/funzione aziendale competente - esaminata la relazione del Responsabile del Sistema - decide le possibili azioni correttive valutando di proporre eventuali misure disciplinari.

Le misure disciplinari sono definite e approvate dalla funzione Human Resources del Gruppo Cerved e devono essere condivise con la società del Gruppo (Consiglio di Amministrazione; Amministratore Delegato; altri ruoli / funzioni di volta in volta competenti).

In caso di accertate violazioni rilevanti ai fini della presente Procedura, le azioni correttive e le misure disciplinari saranno proposte alle funzioni / organi aziendali di volta in volta competenti.

Nell'ipotesi in cui le violazioni riguardino atti o comportamenti posti in essere da componenti del Consiglio di Amministrazione le opportune decisioni verranno adottate dal Consiglio di Amministrazione, sentito il Collegio Sindacale.

Le misure decise vengono comunicate al Responsabile del Sistema e al responsabile della violazione e quindi definitivamente adottate dalla funzione Human Resources di Gruppo o dall'organo sociale competente, nel rispetto della normativa giuslavoristica nazionale applicabile. L'adozione delle misure deve essere comunicata al Responsabile del Sistema dall'organo/funzione aziendale competente.

Le misure disciplinari devono essere adeguate e proporzionate alla violazione accertata, anche tenuto conto dell'eventuale rilevanza penale dei comportamenti posti in essere, e devono essere conformi a quanto previsto dalla normativa giuslavoristica nazionale applicabile.

Il Responsabile del Sistema verifica periodicamente l'effettiva adozione delle misure correttive decise in relazione alle segnalazioni pervenute e riflette l'esito di tali verifiche in una relazione indirizzata agli organi/funzioni aziendali competenti.

6.7. REPORTING

Il Responsabile del Sistema redige almeno annualmente una relazione sull'andamento delle attività da trasmettere agli organi di amministrazione e controllo di volta in volta competenti. Tale relazione deve contenere le informazioni aggregate sulle segnalazioni "cestinate" e sulle risultanze delle attività svolte in relazione alle segnalazioni non "cestinate". La relazione viene approvata dagli organi aziendali competenti e messa a disposizione delle Persone di Cerved mediante pubblicazione sulla rete intranet aziendale.

6.8. FLUSSI INFORMATIVI IN MERITO ALLE SEGNALAZIONI RILEVANTI

Il Responsabile del Sistema procede senza indugio a informare gli organi sociali e di controllo delle società del Gruppo interessate dalla segnalazione:

- 1) qualora nell'ambito delle fasi sopra descritte venga a conoscenza di una Segnalazione Rilevante;

- 2) quando il Responsabile del Sistema medesimo è gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato, è esso stesso il presunto responsabile della violazione ovvero ha un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio e che, pertanto, occorre affidare la gestione delle segnalazioni al gestore alternativo di cui al precedente § 6.1.1.

6.9. INFORMATIVA AL SEGNALATO

Nell'ambito di tutte le fasi di gestione delle segnalazioni, il Responsabile del Sistema valuta le modalità con cui informare il soggetto segnalato in merito alla trasmissione di una segnalazione a suo carico, alla violazione contestata, allo svolgimento del relativo procedimento e all'esito dello stesso.

In particolare, il momento in cui il segnalato viene messo al corrente della segnalazione a suo carico deve essere valutato caso per caso, verificando se l'invio di tale informativa possa pregiudicare lo svolgimento delle indagini necessarie all'accertamento dei fatti oggetto di segnalazione o se, invece, il coinvolgimento del segnalato sia necessario per lo sviluppo dell'indagine.

Cerved garantisce, ad ogni modo, il diritto del segnalato a potersi difendere e ad essere informato (entro tempi ragionevoli) delle accuse e delle eventuali misure disciplinari a suo carico.

6.10. INTERESSE PRIVATO E CORRESPONSABILITÀ DEL SEGNALANTE

Il soggetto segnalante è tenuto a dichiarare la sussistenza di un proprio interesse privato collegato alla segnalazione.

Qualora il segnalante sia corresponsabile delle violazioni oggetto di segnalazione, nei confronti dello stesso potrà essere applicata una attenuazione delle misure disciplinari proporzionata al contributo fornito dalla segnalazione alla scoperta e/o alla prevenzione delle suddette violazioni.

Il Canale Digitale di Segnalazione è pertanto configurato in modo tale da consentire al segnalante di rendere nota (i) la sussistenza di un interesse privato in relazione alla segnalazione nonché (ii) la propria eventuale corresponsabilità in relazione agli atti o fatti oggetto della segnalazione.

6.11. RIVELAZIONE DELL'IDENTITÀ DEL SEGNALANTE

Il Responsabile del Sistema ha il compito di verificare le esigenze di difesa e/o di indagine e di assumere le opportune decisioni in merito alla rivelazione dell'identità del segnalante in conformità alle norme di legge applicabili.

La rivelazione dell'identità del segnalante è ammessa solo qualora essa rappresenti un obbligo necessario e proporzionato imposto dal diritto dell'Unione o dal diritto nazionale nel contesto di indagini da parte delle autorità nazionali o di procedimenti giudiziari, anche al fine di salvaguardare i diritti della difesa del segnalato¹³. In tal caso, la rivelazione dell'identità del segnalante è oggetto di adeguate garanzie ai sensi delle norme europee e nazionali applicabili. In particolare, il segnalante è informato prima della rivelazione della sua identità, a meno che ciò non pregiudichi le relative indagini o procedimenti giudiziari. Quando informa le persone segnalanti, il Responsabile del Sistema invia al segnalante una spiegazione scritta delle ragioni alla base della rivelazione dei dati riservati in questione¹⁴.

6.12. TRATTAMENTO DEI DATI PERSONALI

I dati personali (intesi come dati relativi a persone fisiche identificate o identificabili, nello specifico il segnalante, nel caso di segnalazioni nominative, ed il segnalato) trattati in occasione di una segnalazione ai sensi della presente procedura saranno trattati nel rispetto delle più recenti normative in materia di Privacy, segnatamente del D. Lgs. 196/2003 e successive modificazioni e integrazioni ("Codice Privacy"), del Reg. UE 679/2016 ("GDPR"), e l'ulteriore normativa applicabile, di qualunque rango, inclusi i pareri e le linee guida elaborati dal WP29).

È garantito agli interessati l'esercizio dei diritti di cui agli artt. dal 15 al 22 "GDPR", sia per quanto riguarda il segnalante, sia per quanto riguarda il segnalato, fatta eccezione, laddove applicabili, per le limitazioni previste dagli artt. 2-undecies e 2-terdecies del Codice Privacy.

I dati personali saranno trattati nel rispetto del principio di proporzionalità del trattamento e di minimizzazione, in virtù dei quali i dati che risultino non adeguati, non pertinenti o eccedenti lo scopo previsto dalla presente procedura (ad es. dati particolari eventualmente comunicati in fase di segnalazione da parte del segnalante, nonostante apposito divieto previsto nell'informativa privacy rivolta al segnalante), saranno immediatamente cancellati.

Ulteriori dettagli sono indicati nell'Informativa Privacy disponibile all'indirizzo web del canale digitale di segnalazione.

Cerved ha previsto l'interazione con il DPO nel disegno della presente procedura, nell'eventuale supporto alla gestione dei diritti degli interessati in materia, ed in tutti i casi in cui venga in considerazione, nell'applicazione della presente procedura, un trattamento di dati personali che

¹³ Art. 16, par. 2, dir. UE 2019/1937.

¹⁴ *Ivi*, art. 16, par. 3.

possa impattare notevolmente sulle libertà personali e sui diritti degli interessati, nonché in tutti i casi in cui vi sia fondato motivo di sospettare una compromissione di diritti o una violazione dei dati.

7. Adozione della Procedura e informazione ai Destinatari

La presente Procedura ha la massima diffusione possibile. A tal fine, la stessa:

- è stata approvata dal Consiglio di Amministrazione di Cerved Group S.p.A. e viene adottata da ciascuna società del Gruppo tramite deliberazione del proprio Consiglio di Amministrazione (o del corrispondente organo/funzione/ruolo);
- è pubblicata sul sito internet e sulla rete intranet aziendale; e
- è resa nota ai soggetti segnalanti tramite il Canale Digitale di Segnalazione.

I soggetti suindicati assicurano, per quanto di competenza, l'aggiornamento della consegna o dell'invio della presente Procedura in occasione di avvicendamenti di personale e/o di variazione degli assetti societari partecipativi.

La funzione Human Resources del Gruppo Cerved assicura, per quanto di competenza, che le modalità di accesso alla presente Procedura siano rese note a tutti i dipendenti all'atto dell'assunzione.

8. Supporto e assistenza

Per qualsiasi dubbio, chiarimento o consiglio relativo a questa Procedura le Persone di Cerved devono sempre rivolgersi al Responsabile del Sistema o alla Funzione Anticorruzione (per le società del Gruppo nelle quali queste figure non coincidono) che sono a loro disposizione per fornire ogni supporto necessario.

Ogni richiesta di assistenza può essere inoltrata tramite il Canale Digitale di Segnalazione o via email alla casella email del Responsabile del Sistema di cui al precedente § 6.1.

9. Tracciabilità del processo di gestione delle segnalazioni

Le segnalazioni ricevute (unitamente alla relativa documentazione eventualmente allegata) sono salvate nell'archivio informatico del Canale Digitale di Segnalazione, che non consente alcuna forma di cancellazione e/o alterazione.

In generale, nel caso di utilizzo di canali alternativi interni, tutta la documentazione prodotta e raccolta nell'ambito della segnalazione verrà archiviata all'interno di apposite aree dedicate, con accesso ristretto al solo Responsabile del Sistema; l'accesso a tali aree non è consentito ad altro personale aziendale.

Tale documentazione deve essere conservata nel rispetto degli obblighi di riservatezza per un periodo di tempo adeguato, ritenuto necessario e proporzionato per confermarsi agli obblighi imposti dalle normative nazionali o comunitarie (tra cui segnatamente la direttiva UE 2019/1937), e comunque non inferiore a 10 anni.

10. Aggiornamento della procedura

La funzione Internal Audit riesamina periodicamente la presente procedura per assicurarne l'efficacia nel tempo e l'aderenza alle best practices raccomandando eventuali miglioramenti o integrazione laddove ne ravvisi la necessità. Nell'ambito del processo di revisione viene coinvolta la funzione Legal e la funzione Human Resources al fine di allineare sempre il contenuto del documento ai più aggiornati dettati normativi, ivi inclusi gli aspetti di tipo giuslavoristico.