



Procedura Whistleblowing

GRUPPO CERVED



Approvata dal CdA
in data 27 06 2023



INDICE

1. Obiettivo	3
2. Ambito di applicazione.....	4
2.1. Riferimenti esterni.....	4
3. Definizioni	6
4. Principi generali	10
5. Condotte segnalabili	13
6. Processo di gestione delle segnalazioni	15
6.1. Segnalazioni anonime	15
6.2. canale digitale di segnalazione e invio delle segnalazioni	15
6.3. Presa in carico e valutazione preliminare	16
6.4. Valutazione	17
6.5. Decisione.....	18
6.6. Canali di segnalazione alternativi	19
6.7. Reporting	22
6.8. Flussi informativi in merito alle segnalazioni rilevanti.....	22
6.9. Informativa al segnalato.....	22
6.10. Interesse privato e corresponsabilità del segnalante	23
6.11. Rivelazione dell'identità del segnalante	23
6.12. TRATTAMENTO DEI DATI PERSONALI	24
7. Adozione della Procedura e informazione ai Destinatari	26
8. Supporto e assistenza	27
9. Tracciabilità del processo di gestione delle segnalazioni.....	28
10. Aggiornamento della procedura.....	29
11. Romanian Appendix (Appendice 1)	30
12. Greece Appendix (Appendice 2).....	33

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 ("Whistleblowing")**, 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; 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 che, a partire da tale data, l'hanno adottata tempestivamente¹ tramite deliberazione del proprio Consiglio di Amministrazione.

Gli aggiornamenti della presente procedura sono immediatamente applicabili a tutto il Gruppo Cerved, eventuali specifiche integrazioni o revisioni da parte delle Singole società vengono approvate da parte dei Consigli di Amministrazione di queste ultime.

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 in linea con gli adempimenti ed i requisiti previsti dallo standard UNI ISO 37001 – Sistemi di gestione anticorruzione.

2.1. RIFERIMENTI ESTERNI

La procedura è stata predisposta in linea con il Decreto Legislativo 10 marzo 2023, n. 24 - 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.

Le specificità relative alla normativa delle Società del Gruppo Cerved operanti in Romania e Grecia e di seguito indicate:

¹ Entro 120 giorni dall'approvazione della Procedura da parte del Consiglio di Amministrazione di Cerved Group SpA.

- Legge 361 del 19 dicembre 2022 – Legge di recepimento nell'ordinamento nazionale rumeno della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019;
- Law 4990/2022 (Government Gazette A 210/11.11.2022) - Legge di recepimento nell'ordinamento nazionale greco della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019;

sono riportate all'interno delle Appendici n. 1 e n. 2.

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, in forma orale. Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o su richiesta della persona segnalante, mediante un incontro diretto con il Responsabile di Sistema fissato entro un termine ragionevole².
- **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 seguenti autorità:
 - **per l'Italia:** Autorità Nazionale Anticorruzione (ANAC);
 - **per la Romania:** all'Agenzia Nazionale per l'Integrità ("NIA – National Integrity Authority");
 - **per la Grecia:** National Transparency Authority ("NTA").

e, se del caso, a istituzioni, organi e organismi dell'Unione di volta in volta competenti per la materia oggetto di segnalazione.

I canali esterni possono essere anche le **Divulgazioni Pubbliche** o la **Denuncia all'autorità giudiziaria o contabile**.

ATTENZIONE: in via prioritaria è favorito l'utilizzo del canale interno e, solo al ricorrere di una delle condizioni di cui all'art. 6 D. Lgs. 24/2023 (richiamate al par 6.6.2), è possibile effettuare una segnalazione esterna.

- **CERVED** o **GRUPPO CERVED** o **GRUPPO:** Cerved Group S.p.A. e le società direttamente o indirettamente controllate da Cerved Group S.p.A..
- **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.

² D. Lgs. 24/2023 – Capo II Art. 4 c. 3

- **DIVULGAZIONE PUBBLICA:** rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone³.
- **FACILITATORE:** una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata⁴.
- **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.
- **GESTORE ALTERNATIVO:** soggetto al quale rivolgersi quando il Responsabile del Sistema si trova in una delle situazioni di potenziale "conflitto di interessi" richiamate al par. 6.6.1. Il Gestore Alternativo è identificato nell'**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.
- **INFORMAZIONI SULLE VIOLAZIONI:** informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico nonché gli elementi riguardanti condotte volte ad occultare tali violazioni⁵.
- **MODELLO 231:** il Modello di Organizzazione, Gestione e Controllo adottato da ciascuna società del Gruppo Cerved ai sensi del Decreto Legislativo 231/2001.
- **PERSONA SEGNALANTE O SEGNALANTE (WHISTLEBLOWER):** la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo⁶.
- **PERSONA COINVOLTA o SEGNALATO:** la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente⁷.

³ D. Lgs. 24/2023 – Capo I Art. 1 lett. f

⁴ D. Lgs. 24/2023 – Capo I Art. 1h

⁵ D. Lgs. 24/2023 – Capo I Art. 1 lett. b

⁶ D. Lgs. 24/2023 – Capo I Art. 1 lett. g

⁷ D. Lgs. 24/2023 – Capo I Art. 1 lett. l

- **PERSONE DI CERVED:** azionisti, componenti degli Organi Sociali, le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, tutti i Dipendenti e, più in generale, tutti i soggetti che svolgono in favore di Cerved la propria attività lavorativa (quali ad esempio lavoratori autonomi, collaboratori, liberi professionisti, consulenti, volontari, tirocinanti, ecc.) e ogni altro soggetto, persona fisica o giuridica, con cui Cerved entri in contatto nello svolgimento di relazioni d'affari che vengono a conoscenza, in un contesto lavorativo pubblico o privato, delle condotte indicate nella presente procedura o di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato⁸. A tali soggetti sono equiparati i Facilitatori, le persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado; i colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente; gli enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone⁹.

La tutela si applica PRE – DURANTE e POST rapporto di lavoro / di collaborazione

- **RESPONSABILE DEL SISTEMA:** è identificato nei Responsabili della Funzione Internal Audit, di ciascuna Società italiana del Gruppo, salvo che per le seguenti società:
 - Cerved Rating Agency S.p.A. – identificato nel Responsabile della Funzione Compliance & Risk Management della società;
 - Cerved Master Services S.p.A. – identificato nel Responsabile della Funzione Compliance, AML & Risk Management della società.

Per le società estere del Gruppo è stato individuato altresì un Responsabile del Sistema locale.

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.

⁸ D. Lgs. 24/2023 – Capo I Art. 1 c. 1

⁹ D. Lgs. 24/2023 – Capo I Art. 3 c. 5

- **RISCONTRO:** comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione¹⁰.
- **RITORSIONE:** qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto¹¹.
- **SEGNALAZIONE RILEVANTE (O SEGNALAZIONI RILEVANTI):** segnalazione che coinvolge
 - l'Amministratore Delegato, l'alta dirigenza, gli amministratori o i membri dell'organo di controllo di Cerved Group o di una società del Gruppo;
 - le Persone di Cerved di più strutture aziendali o di più società del Gruppo;e ha ad oggetto atti o fatti di rilevanza penale, violazioni ripetute sistematicamente oppure un comportamento ritorsivo nei confronti del segnalante; 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.
- **SEGUITO:** l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate¹².
- **SISTEMA DI SEGNALAZIONE o SISTEMA:** il sistema multicanale per la ricezione e la gestione delle segnalazioni oggetto della presente Procedura.

¹⁰ D. Lgs. 24/2023 – Capo I Art. 1 lett. o

¹¹ D. Lgs. 24/2023 – Capo I Art. 1 lett. l

¹² D. Lgs. 24/2023 – Capo I Art. 1 lett. n

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 segnalante¹³:** 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, imposizione di obiettivi impossibili da raggiungere, 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. I soggetti che dovessero ritenere di aver subito condotte ritorsive o vessatorie in conseguenza di una segnalazione possono altresì comunicare la circostanza ad ANAC, tramite il sito web dedicato.
- **Divieto di comportamenti volti ad ostacolare le segnalazioni¹⁴:** 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

¹³ D. Lgs. 24/2023 – Capo II Art. 17 e Art. 19

¹⁴ Dir. UE 2019/1937, art. 23, par. 1, lett. dalla a) alla d).

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 qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità senza il consenso espresso della stessa persona segnalante¹⁵. È altresì tutelata 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 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. Qualora la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato della eventuale sanzione disciplinare, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.¹⁶
- **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.

¹⁵ D. Lgs. 24/2023 – Capo II, Art. 12 c. 2

¹⁶ D. Lgs. 24/2023 – Capo II, Art. 12 c. 5.

- **Divieto di rinuncia ai diritti¹⁷**: 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.

¹⁷ Dir. UE 2019/1937, art. 24.

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 (Whistleblowing)** 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. In questo caso, con la piena attuazione di tutte le tutele per il segnalante previste dalla presente Procedura, il fatto oggetto di segnalazione viene riportato anche all'Organismo di Vigilanza della Società di riferimento;
 - ✓ violazioni delle procedure adottate dalle Società del Gruppo, in particolare, tra le altre procedure/normative interne, violazioni del Sistema di Gestione Anticorruzione, della Politica Anticorruzione di Gruppo e/o della Procedura "Due diligence anti-corruzione delle Terze Parti Rilevanti" nonché della procedura in materia di conflitto di interesse e le procedure collegate al programma di compliance antitrust;
 - ✓ tematiche di *business integrity* (ad esempio, condotte scorrette nella gestione degli affari, eventi dannosi che coinvolgono la clientela, conflitti di interesse), che includono anche quanto relativo alle seguenti casistiche:
 - 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 ...);
 - comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:
 - illeciti amministrativi, contabili, civili o penali;
 - illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al presente decreto ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea;
 - atti od omissioni che ledono gli interessi finanziari dell'Unione;

- atti od omissioni riguardanti il mercato interno (a titolo esemplificativo: violazioni in materia di concorrenza e di aiuti di Stato);
 - atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.
- ✓ tematiche di *financial integrity* (ad esempio, violazioni in materia contabile, frodi societarie, furti, utilizzo non corretto delle risorse aziendali), 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. SEGNALAZIONI ANONIME

Cerved prevede la possibilità di effettuare segnalazioni in forma anonima. Queste saranno prese in carico e gestite, al pari delle segnalazioni nominative.

Qualora la segnalazione interna sia presentata ad un soggetto diverso dal Responsabile del Sistema, individuato come competente e autorizzato a trattarla, il ricevente dovrà trasmettere la segnalazione entro 7 giorni dal suo ricevimento al Responsabile del Sistema competente, dando contestualmente notizia della trasmissione alla persona segnalante.

6.2. CANALE DIGITALE DI SEGNALAZIONE E INVIO DELLE SEGNALAZIONI

Il Canale Digitale di Segnalazione (<https://ewhistle.cerved.com>) è liberamente accessibile via web a tutte le Persone di Cerved.

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. È garantito il divieto di tracciamento dei canali di segnalazione.

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.

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.

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.

Il Responsabile del Sistema (o il Gestore Alternativo) invia alla persona segnalante avviso di ricevimento della segnalazione **entro sette giorni dalla data di ricezione**; successivamente mantiene le interlocuzioni con la persona segnalante richiedendo a quest'ultima, se necessario, integrazioni.

Il Responsabile del Sistema (o il Gestore Alternativo) dà diligente seguito alle segnalazioni ricevute e fornisce riscontro alla segnalazione **entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.**

6.3. 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 della Società interessata dalla segnalazione.

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 “cestinate” sono salvate nell’archivio informatico del Canale Digitale di Segnalazione, che non consente alcuna forma di alterazione (cfr. § 0). 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 tempestivamente.

6.4. VALUTAZIONE

Il Responsabile del Sistema verifica, per le segnalazioni che non siano state immediatamente “cestinate”, 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 quanto prima al segnalante.

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.

6.5. DECISIONE

Sulla base di quanto emerso nel corso dell'istruttoria, il Responsabile del Sistema individua la funzione/organo aziendale competente a condurre le opportune valutazioni e 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 collegialmente, con l'astensione dei diretti interessati, dove presente verrà altresì 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 e coerenti con il Sistema sanzionatorio di ciascun Modello organizzativo applicabile al caso di specie.

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.

6.6. CANALI DI SEGNALAZIONE ALTERNATIVI

6.6.1 CANALE 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 seguenti **canali interni alternativi**:

- **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 della Società interessata dalla segnalazione.

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:

- l'oggetto della e-mail contenga la predetta dicitura "riservata/personale"
- la segnalazione venga inserita in una busta chiusa che rechi all'esterno la dicitura "riservata/personale".

- **Segnalazioni in forma orale**, che potrà essere effettuata:

- **attraverso la linea telefonica non registrata messa a disposizione da Cerved (numerazioni disponibili sul sito web)**. Sono previste le seguenti numerazioni differenti:
 - una per segnalazioni riguardanti Cerved Rating Agency SpA;
 - una per segnalazioni riguardanti Cerved Master Services SpA;
 - una per segnalazioni riguardanti le Società del Gruppo con Sede in Grecia (lingua greca);

- una per segnalazioni riguardanti le Società del Gruppo con Sede in Romania (lingua rumena);
- una per le segnalazioni riguardanti tutte le altre Società o paesi del Gruppo Cerved.

Tutte le linee consentono di effettuare una segnalazione in lingua inglese.

In questo caso il Responsabile del Sistema procederà a formalizzare la segnalazione all'interno del canale digitale mediante un resoconto dettagliato della conversazione. Al segnalante verrà comunicato il numero identificativo della segnalazione per consentirgli di accedere alla segnalazione, verificarla e/o chiedere rettifiche e infine approvarla tramite il canale di comunicazione riservato presente all'interno del canale digitale di segnalazione.

- **attraverso un incontro con il Responsabile del Sistema.** In questo caso il Responsabile del Sistema, subordinatamente al consenso della persona segnalante, documenterà la segnalazione, se possibile, all'interno del canale digitale di segnalazione, in presenza del segnalante, chiedendo poi conferma dei contenuti ed acquisendo, laddove possibile, la sottoscrizione di quanto segnalato.

Si precisa che anche le segnalazioni pervenute attraverso i 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,

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.

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. Per inviare direttamente una segnalazione al Gestore Alternativo è sufficiente selezionare, nel menù a tendina, la Società e l’opzione “Gestore Alternativo” (“nome società – Gestore Alternativo”) procedendo poi a completare la segnalazione come indicato in precedenza.

6.6.2 CANALI DI SEGNALAZIONE ESTERNI

È sempre prevista la possibilità per il segnalante di effettuare la segnalazione anche mediante l’utilizzo **dei seguenti canali di segnalazione esterni**:

- presso l’Autorità nazionale anticorruzione (ANAC - www.anticorruzione.it) che attiva un canale di segnalazione esterna che garantisca, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell’identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione;
- tramite Divulgazione Pubblica ovvero rendendo di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone;
- tramite Denuncia all’autorità giudiziaria o contabile.

In via prioritaria è favorito l’utilizzo del canale interno e, solo al ricorrere di una delle seguenti condizioni è possibile effettuare una segnalazione esterna:

- a) non è prevista, nell’ambito del contesto lavorativo del segnalante, l’attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dall’articolo 4 del D. Lgs. 24/2023;
- b) la persona segnalante ha già effettuato una segnalazione interna ai sensi dell’articolo 4 e la stessa non ha avuto seguito;
- c) la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- d) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

6.7. REPORTING

Il Responsabile del Sistema redige almeno annualmente una relazione sull'andamento delle attività svolte da trasmettere agli organi di amministrazione e controllo di volta in volta competenti. Tale relazione deve contenere le informazioni aggregate sulle segnalazioni "cestate" e sulle risultanze delle attività svolte in relazione alle segnalazioni non "cestate". 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 SEGNALANTE¹⁸

Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati¹⁹.

Detto consenso viene acquisito tramite richiesta effettuata dal Responsabile del Sistema (con spiegazione scritta delle ragioni alla base della rivelazione dei dati riservati in questione) attraverso il canale di comunicazione previsto all'interno dell'applicativo affinché siano sempre garantiti la riservatezza delle informazioni e l'anonimato fino al rilascio del consenso. Nel caso di segnalazioni effettuate mediante i canali interni alternativi verranno informati i segnalanti che le segnalazioni saranno riportate all'interno del canale digitale di segnalazione e gestite attraverso tale canale in modo da poter interagire con il segnalante, anche per acquisire il consenso alla rivelazione della sua identità, in maniera riservata e tutelando la sua identità.

Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione

¹⁸ Nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità della persona segnalante non può essere rivelata fino alla chiusura della fase istruttoria

¹⁹ D. Lgs. 24/2023 – Capo II Art. 12 c. 2: ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità. Detto consenso verrà acquisito secondo le modalità sopra indicate.

È dato avviso alla persona segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati anche quando la rivelazione della identità della persona segnalante è indispensabile anche ai fini della difesa della persona coinvolta.

La tutela dell'identità delle persone coinvolte e delle persone menzionate nella segnalazione deve essere garantita fino alla conclusione dei procedimenti avviati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante.

La Persona Coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

6.12. TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali (intesi come dati relativi a persone fisiche identificate o identificabili, nello specifico il segnalante, nel caso di segnalazioni nominative, ed il segnalato o le persone coinvolte) acquisiti in occasione della gestione di una segnalazione ai sensi della presente procedura è effettuato nel rispetto delle normative in materia di Privacy, segnatamente del Reg. UE 679/2016 ("GDPR") e del D. Lgs. 196/2003 e successive modificazioni e integrazioni ("Codice Privacy").

Per i dettagli sul trattamento dei dati relativo alle Società del Gruppo Cerved con sede in Grecia e in Romania si vedano le rispettive appendici n. 1 e n. 2

Agli interessati, ovvero sia alle persone segnalanti che alle persone coinvolte, sono fornite idonee informazioni ai sensi degli articoli 13 e 14 del GDPR attraverso anche l'Informativa Privacy disponibile all'indirizzo web del canale digitale di segnalazione e, per dipendenti e collaboratori Cerved, nella intranet aziendale.

È garantito agli interessati l'esercizio dei diritti di cui agli artt. dal 15 al 22 "GDPR", nei limiti di quanto previsto dall'art. 2-undecies, comma 1, lett. f), del Codice Privacy.

I dati personali saranno trattati nel rispetto dei principi di correttezza e del trattamento e di minimizzazione dei dati, in virtù dei quali i dati che risultino non utili al trattamento di una specifica segnalazione o non adeguati, non pertinenti o non limitati rispetto alle finalità del trattamento oggetto dalla presente procedura saranno immediatamente cancellati.

Ulteriori dettagli sono comunque 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 possa impattare in modo rilevante sui diritti degli interessati, nonché in tutti i casi in cui vi sia una elevata probabilità di rischio dei loro diritti.

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 e-mail alla casella email del Responsabile del Sistema di cui al precedente § 6.1 oppure attraverso la linea telefonica dedicata.

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.

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.

Le segnalazioni, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza.

10. Aggiornamento della procedura

Il Responsabile del Sistema 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 vengono coinvolte 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.

11. Romanian Appendix (Appendice 1)

Law no. 361/2022 provides the general framework on the protection of persons who report violations of the law, which have occurred or are likely to occur within the authorities, public institutions, other legal persons governed by public law, as well as within legal persons governed by private law, providing the procedure for receiving, examining and resolving reports, as well as the rights and obligations of persons submitting reports or publicly disclosing information on violations of the law, their protection measures, the obligations of authorities, public institutions and other legal persons governed by public law, as well as those of legal persons governed by private law, the rights of the persons concerned and the responsibilities of the competent authorities.

The appendix is applicable to Cerved Romanian companies: Re Collection S.R.L., Cerved Credit Collection S.p.A. (the offices in Romania) and Cerved Property Services S.A.

Whistleblower System Manager

Re Collection S.R.L., Cerved Credit Collection S.p.A. (the offices in Romania) and Cerved Property Services S.A. named a person operating in Romania, member of the *Compliance and Quality Assurance* function, that will act as Whistleblowing System Manager in coordination with Cerved Group Whistleblowing System Manager as part of the activities related to the whistleblowing reporting management process.

If you are based in Romania and wish to raise a concern, these country specific provisions apply to you in addition to the main Whistleblowing Procedure of Cerved Group.

WHO THIS PROCEDURE APPLIES TO

Whistleblowers can be:

I. Persons who have obtained in the framework of their work with Re Collection S.R.L., Cerved Credit Collection S.p.A. (the offices in Romania) and Cerved Property Services S.A. information regarding the breaches they report, importantly:

- a. workers;
- b. persons having self-employed status, within the meaning of Article 49 TFEU;
- c. shareholders and persons belonging in the administrative, management or supervisory bodies of the company, including non-executive members, as well as volunteers and paid or unpaid trainees;
- d. any person working under the supervision and direction of contractors, subcontractors, and suppliers.

II. Persons who wish to report information on breaches obtained in the framework of their employment with Re Collection S.R.L., Cerved Credit Collection S.p.A. (the offices in Romania) and Cerved Property Services S.A. which has ended (for any reason, including retirement), as well as persons whose employment relationship with Re Collection S.R.L., Cerved Credit Collection S.p.A. (the offices in Romania) and Cerved Property Services S.A. has not yet begun, where information on breaches has been acquired during the recruitment process or during other precontractual obligations.

WHAT VIOLATIONS THIS PROCEDURE APPLIES TO

This Procedure is applicable to violation reports concerning:

- a. breaches falling within the scope of EU law that concern the following areas: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; and (x) protection of privacy and personal data, and security of network and information systems;
- b. breaches affecting the financial interests of the EU as referred to in Article 325 TFEU and as further specified in relevant EU measures; and
- c. breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of EU competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law, which represent disciplinary violations, misdemeanors or offenses, or which are contrary to the object or purpose of the law;

ANONYMOUS VIOLATION REPORTS

Our companies provide the option of filing a violation report anonymously and shall be examined and resolved to the extent that it contains indications of violations of the law.

ACCEPTANCE OF A VIOLATION REPORT AND ASSESSMENT

- a. Step one: The Whistleblowing System Manager will acknowledge your violation report within 7 days.**

The Whistleblowing System Manager will acknowledge the receipt of the violation report within seven (7) days of receipt.

- b. Step two: Whistleblowing System Manager's actions.**

Once a violation report has been made, the Whistleblowing System Manager will either forward the violation report to the competent team of the company or the competent entity (e.g., competent authorities) for further actions, or will terminate the procedure, in case the report is unintelligible, or abusive, or does not include facts constituting a breach of EU law, or there are no serious indications of such breach.

Please note that the Whistleblowing System Manager may contact you for any further information which might be needed regarding your report. The whistleblower has 15 days to submit the requested information.

- c. Step three: Whistleblowing System Manager will provide you with feedback.**

The Whistleblowing System Manager will provide you with information regarding the actions taken within a reasonable timeframe, which shall not exceed three (3) months from the receipt of the violation report or from the deadline for acknowledging the receipt.

PROCESSING OF PERSONAL DATA

Any processing of personal data carried out pursuant to this law, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Law no. 363/2018, as well as the provisions of Regulation (EU) 2018/1.725.

Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

EXTERNAL REPORTING

External reports can be submitted directly to the National Integrity Agency ("NIA"), which is the competent authority to receive, manage and follow up on them.

Reports can be made in writing, orally by telephone or request a face-to-face meeting with the person appointed by the NIA, or through the electronic platform of the NIA.

If you submit a report to the NIA, the NIA will acknowledge the receipt of the report within seven (7) days of receipt, unless you specifically require otherwise or in case the NIA considers that such receipt will put at risk the confidentiality of your identity.

12. Greece Appendix (Appendice 2)

With Law 4990/2022 (Government Gazette A' 210/11.11.2022) (hereinafter, the "Law"), the major issue of the protection of the persons who report breaches of Union law is addressed. Specifically, persons who work for a public or private organization or are in contact with such an organization in the context of their work-related activities are often the first to know about threats or harm to the public interest which arise in that context. The purpose of this Law is the establishment of a unified protection framework for persons reporting breaches of Union law, as well as the transposition of the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (L 305).

If you are based in Greece and wish to report violations, these country specific provisions apply to you in addition to the main Whistleblowing Procedure of Cerved Group.

WHO THIS PROCEDURE APPLIES TO

Whistleblowers can be:

I. Persons who have obtained in the framework of their work with Cerved Greece information regarding the breaches they report, importantly:

- a. employees (full or part-time, indefinite or fixed term, posted, etc.);
- b. self-employed persons, consultants and home workers;
- c. shareholders and persons belonging in the administrative, management or supervisory bodies of the company, including non-executive members, as well as volunteers and paid or unpaid trainees;
- d. any person working under the supervision and direction of contractors, subcontractors, and suppliers.

II. Persons who wish to report information on breaches obtained in the framework of their employment with Cerved Greece which has ended (for any reason, including retirement), as well as persons whose employment relationship with Cerved Greece has not yet begun, where information on breaches has been acquired during the recruitment process or during other precontractual obligations.

WHAT VIOLATIONS THIS PROCEDURE APPLIES TO

This Procedure is applicable to violation reports concerning:

- a. breaches falling within the scope of EU law that concern the following areas: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; and (x) protection of privacy and personal data, and security of network and information systems;
- b. breaches affecting the financial interests of the EU as referred to in Article 325 TFEU and as further specified in relevant EU measures; and
- c. breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of EU competition and State aid rules, as well as breaches relating to the internal market in

relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

ANONYMOUS VIOLATION REPORTS

Cerved provides the option of filing a violation report anonymously, but the whistleblower should note that in case of an anonymous report if they are not identified at a later stage, they could not be protected under Greek legislation.

ACCEPTANCE OF A VIOLATION REPORT AND ASSESSMENT

a. Step one: The Whistleblowing System Manager will acknowledge your violation report within 7 days.

The Whistleblowing System Manager will acknowledge the receipt of the violation report within seven (7) working days of receipt.

b. Step two: Whistleblowing System Manager's actions.

Once a violation report has been made, the Whistleblowing System Manager will either forward the violation report to the competent team of Cerved or the competent entity (e.g., competent authorities) for further actions, or will terminate the procedure, in case the report is unintelligible, or abusive, or does not include facts constituting a breach of EU law, or there are no serious indications of such breach.

Please note that the Whistleblowing System Manager may contact you for any further information which might be needed regarding your report.

c. Step three: Whistleblowing System Manager will provide you with feedback.

The Whistleblowing System Manager will provide you with information regarding the actions taken within a reasonable timeframe, which shall not exceed three (3) months from the receipt of the violation report or from the deadline for acknowledging the receipt.

PROCESSING OF PERSONAL DATA

The personal data processed in the context of a violation report pursuant to this Procedure shall be processed in compliance with the EU Reg. 679/2016 ("GDPR"), Greek law 4624/2019, the regulatory acts and decisions of the Greek Personal Data Protection Authority and any additional legislation, at whatever level, including the opinions and guidelines produced by the WP29 and EDPB.

As a matter of exception from the general GDPR rules, according to Greek Whistleblowing Law 4990/2022 ("Local Law"), Cerved will not inform the subject party or any third party mentioned in the violation report regarding their personal data processing and may not satisfy their relevant rights (right to access, rectification, erasure, etc.), for as long as necessary, in order to ensure that the whistleblowing process is carried out in accordance with Local Law and the provisions of this Procedure.

Cerved adopts all necessary technical and organizational measures to ensure the protection of the rights and freedoms of persons involved in a violation report.

EXTERNAL REPORTING

External reports can be submitted directly to the National Transparency Authority ("NTA"), which is the competent authority to receive, manage and follow up on them.

You may also report a breach externally if you reasonably believe that your report cannot be managed properly by the Whistleblowing System Manager or if risk of retaliation exists.

Reports can be made in writing, orally by telephone or request a face-to-face meeting with the person appointed by the NTA, or through the electronic platform of the NTA, accessible to persons with disabilities too.

If you submit a report to the NTA, the NTA will acknowledge the receipt of the report within seven (7) working days of receipt, unless you specifically require otherwise or in case the NTA considers that such receipt will put at risk the confidentiality of your identity.