

# Sistema di segnalazione delle violazioni (“Whistleblowing”)

Il dispositivo Whistleblowing, descritto di seguito, è un sistema interno di segnalazione con il quale si ha la possibilità di segnalare una particolare situazione di cui si è a conoscenza, in cui non sono rispettate le norme interne (locali e di Gruppo) che disciplinano lo svolgimento delle attività e/o gli standard e i principi etici di Gruppo e/o le normative esterne di riferimento.

## CHI PUÒ ESSERE AUTORE DI UNA SEGNALAZIONE?

L'autore di una segnalazione può essere qualsiasi dipendente<sup>1</sup>, collaboratore esterno o saltuario<sup>2</sup>, un membro degli organi societari, uno dei direttori e degli azionisti, nell'ambito del dovere di diligenza, qualsiasi prestatore di servizi con cui si intrattiene una relazione commerciale (subappaltatori o fornitori). Chi segnala può essere aiutato da terzi, detti "facilitatori", senza che ciò pregiudichi l'ammissibilità della segnalazione. Lo status di whistleblower può estendersi a questi facilitatori terzi, alle persone fisiche in relazione con il whistleblower e alle entità giuridiche controllate dal whistleblower per le quali il whistleblower lavora o con le quali è associato in un contesto professionale.

Un individuo sarà considerato un "whistleblower" e godrà dello status di protezione riservato agli autori di segnalazioni, se come persona fisica segnalante, agisce in buona fede e responsabilmente, non si aspetta di avere una ricompensa per la segnalazione<sup>3</sup> e segnala fatti rientranti nell'ambito di applicazione della normativa di riferimento.

Sono ricomprese dalla predetta normativa anche le segnalazioni effettuate nell'ambito di un rapporto di lavoro poi terminato, se le informazioni sono state acquisite durante il suo svolgimento, nonché qualora il rapporto non sia ancora iniziato e le informazioni sulle violazioni siano state acquisite durante la selezione o in altre fasi precontrattuali.

---

*1 Compresi coloro il cui rapporto di lavoro è terminato, se le informazioni sono state ottenute nel contesto di tale rapporto, e tutti coloro che hanno fatto richiesta di lavoro presso l'entità interessata, se le informazioni sono state ottenute nel contesto di tale domanda.*

*2 Personale esterno e temporaneo (lavoratori temporanei, apprendisti, tirocinanti, volontari aziendali internazionali (VIE), fornitori di servizi, dipendenti di subappaltatori, gestori di fornitori di servizi e subappaltatori).*

*3 In alcuni ordinamenti è prevista una ricompensa a fronte della segnalazione.*

## **QUALI FATTI POSSONO ESSERE OGGETTO DI SEGNALAZIONE?**

Le violazioni che possono essere segnalate ai sensi del Decreto Whistleblowing sono quelle di cui il segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo (con cui il segnalante intrattiene un dato rapporto giuridico) e che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o della Società e consistono in:

- Violazioni o tentativi di violazione del diritto nazionale
  - Illeciti penali, civili, amministrativi o contabili;
  - Condotte illecite rilevanti ai sensi del Decreto Legislativo 231/2001 o violazioni del Modello di Organizzazione e gestione 231 (tra cui violazioni dei relativi codici di condotta, violazione di principi e procedure previste dal Modello 231);
  
- Violazioni o tentativi di violazione del diritto comunitario
  - Atti /omissioni che ledono il mercato interno e la libera circolazione di merci, persone, servizi e capitali (quali ad esempio violazioni di diritto UE in materia di concorrenza e di aiuti di stato di imposta sulle società);
  - Violazioni del diritto dell'UE in specifici settori (ad esempio appalti pubblici, servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, reati ambientali, protezione dei consumatori, tutela della vita privata e protezione dei dati personali - da intendersi come violazione della normativa in materia di privacy-e sicurezza delle reti e dei sistemi informativi adozione di pratiche commerciali sleali);
  - Atti/omissioni che ledono gli interessi finanziari dell'UE (ad es. frode, corruzione, qualsiasi altra attività illegale connessa alle spese UE);
  - Atti/comportamenti che vanificano oggetto e finalità di disposizioni UE nei settori di cui si è detto.
  
- Ritorsioni contro la persona che segnala o contro qualsiasi altra persona fisica o giuridica protetta dalla normativa whistleblowing.

## COME EFFETTUARE LA SEGNALAZIONE?

### 1) Canali interni

Per SGSS S.p.A. sono presenti i seguenti strumenti, qui di seguito dettagliati

➤ Forma scritta

Il Gruppo SG ha messo a disposizione di SGSS S.p.A. un canale interno autonomo fornito dal provider esterno Whistleb By Navex attraverso una piattaforma<sup>4</sup> dedicata e sicura, che permette di garantire i livelli di riservatezza richiesti dalla normativa, disponibile sul sito web. La procedura di segnalazione è cifrata e protetta da password.

Il canale Whistleb interno di SGSS S.p.A. è raggiungibile al seguente indirizzo:

[https://report.whistleb.com/it/sgss\\_spa](https://report.whistleb.com/it/sgss_spa)

La gestione degli alert è a cura del whistleblowing team di SGSS S.p.A. I dati sono visibili anche al *whistleblowing referent team* di SG.

È possibile inoltrare una segnalazione al tool di SG.

Il link alla piattaforma di segnalazione è:

<https://report.whistleb.com/societegenerale>

ed è disponibile nella homepage del sito del gruppo Societe Generale.

➤ Forma orale

Un sistema di messaggistica vocale con relativa registrazione è disponibile al seguente numero:



**+ 39 347 8179 321**

---

<sup>4</sup> <https://report.whistleb.com/it/message/societegenerale>

Il segnalante può inoltre richiedere, per il tramite del canale orale sopra indicato un incontro finalizzato ad effettuare la segnalazione. L'incontro sarà fissato entro un termine ragionevole (entro 15 giorni salvo cause di forza maggiore) con almeno un componente del whistleblowing team.

## 2) Canali esterni

In via prioritaria, i segnalanti sono incoraggiati a utilizzare i canali interni e, al ricorrere di determinate condizioni, possono effettuare una segnalazione esterna direttamente alle Autorità competenti.

È possibile effettuare una segnalazione esterna, per l'Italia, all'**Autorità Nazionale AntiCorruzione (ANAC)**.

Le condizioni per ricorrere al canale esterno presso ANAC sono le seguenti:

1. se il canale interno obbligatorio:

- non è attivo;
- è attivo ma non è conforme a quanto previsto dal legislatore in merito ai soggetti, alle modalità di presentazione delle segnalazioni.

2. la persona ha già fatto la segnalazione interna ma non ha avuto seguito;

*Si fa riferimento ai casi in cui il canale interno sia stato utilizzato ma il team cui è affidata la gestione del canale non abbia intrapreso entro i termini previsti alcune attività circa l'ammissibilità della segnalazione, la verifica della sussistenza dei fatti segnalati o la comunicazione dell'esito dell'istruttoria svolta.*

3. la persona segnalante ha fondati motivi di ritenere che se effettuasse una segnalazione interna;

- alla stessa non sarebbe dato efficace seguito (è il caso ad es. del conflitto di interesse con il team che riceve la segnalazione<sup>5</sup>);
- questa potrebbe determinare rischio di ritorsione.

---

<sup>5</sup> Si ricorda la possibilità di usufruire del canale interno di Gruppo.

*I fondati motivi che legittimano il ricorso alla segnalazione esterna per il timore di ritorsioni o di trattamento inadeguato della segnalazione devono essere fondati sulla base di circostanze concrete che devono essere allegate alla segnalazione e su informazioni effettivamente acquisibili.*

4. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire il pericolo imminente o palese per il pubblico interesse.

Le segnalazioni esterne all'ANAC possono essere effettuate secondo le modalità previste sul sito istituzionale dell'ente.

#### **ASPETTI CONNESSI ALLA PRIVACY**

Nell'ambito del framework per le segnalazioni, Societe Generale SA (di seguito "SG") e Societe Generale Securities Services S.p.A. (di seguito "SGSS"), in quanto Titolari del trattamento dei dati personal, raccolgono ed elaborano dati e informazioni personali (dati personali o informazioni personali) relativi all'utente. Tali attività di elaborazione dei dati personali sono svolte nel pieno rispetto del Regolamento UE 679/2016 ("GDPR") e conseguente normativa nazionale nonché in base agli obblighi legali a cui SG e SGSS sono soggette oppure nell'interesse legittimo delle citate società.

Le informazioni personali raccolte in questo ambito possono essere divulgate al Direttore della Conformità del Gruppo, a esperti interni ed esterni preventivamente individuati ed autorizzati per l'analisi, l'elaborazione e il risultato della segnalazione, incluse le finalità legali e/o regolamentari. SG e SGSS possono inoltre divulgare le informazioni personali alle autorità competenti, incluse quelle giudiziarie, al fine di rispettare ogni obbligo legale o regolamentare.

Per soddisfare le finalità sopra riportate, SG e SGSS possono dover trasferire i dati personali a soggetti terzi con sede all'interno o all'esterno dello Spazio Economico Europeo. Tali trasferimenti di dati avverranno nel rispetto delle condizioni e garanzie previste dal GDPR e che assicurino la protezione dei dati personali (autorizzazione dell'autorità preposta in materia di protezione dei dati, laddove necessaria, vincolo contrattuale con i fornitori dei servizi interessati e/o Binding Corporate Rules del Gruppo Societe Generale).

Le informazioni personali raccolte ed elaborate si riferiscono a quanto segue

- Identità, ruolo e dati di contatto del segnalatore;

- Identità, ruolo e dati di contatto dei singoli cui si fa riferimento nella segnalazione;
- Identità, ruolo e dati di contatto dei singoli coinvolti nella raccolta e nell'elaborazione della segnalazione;
- I fatti oggetto della segnalazione;
- Gli elementi raccolti nell'ambito della verifica dei fatti oggetto della segnalazione;
- Il rapporto scritto delle attività di verifica;
- Le conseguenze della segnalazione.

I dati personali relativi a una segnalazione considerata da SG e/o SGSS non rientrante nello schema di segnalazione vengono distrutti o resi anonimi nei due mesi successivi alla decisione di escludere l'incidente dal sistema.

In assenza di follow-up su un incidente rientrante nello schema di segnalazione, i dati personali correlati a tale segnalazione vengono distrutti e resi anonimi da SG e/o SGSS entro 12 mesi dalla chiusura delle attività di verifica (conclusione del processo di segnalazione). Con l'espressione "follow-up" si intende ogni decisione dei predetti soggetti finalizzata a trarre le conclusioni in merito alla segnalazione.

In caso di follow-up di una segnalazione (e in particolare nel caso di procedura disciplinare o di causa giudiziaria contro una persona coinvolta o contro il segnalatore di un incidente illegittimo), i dati personali correlati alla segnalazione possono essere conservati da SG e SGSS fino alla conclusione della procedura oppure del periodo di appello contro la decisione.

I dati personali possono essere conservati per periodi più lunghi qualora sussista un obbligo legale e/o regolamentare in merito in capo a SG e SGSS. Pertanto, in conformità ai sistemi legislativi locali, i periodi di conservazione possono essere più lunghi.

Gli interessati possono esercitare i diritti previsti dal GDPR mediante trasmissione di una comunicazione scritta all'indirizzo: [IT-SGSS-SegnalazioniPrivacy@socgen.com](mailto:IT-SGSS-SegnalazioniPrivacy@socgen.com); inoltre potranno esercitare i diritti di accesso, rettifica, cancellazione e limitazione e opporsi al trattamento ai sensi delle condizioni indicate nel regolamento creando una nuova richiesta nello strumento (nella categoria "Protezione dei dati personali") e riceveranno risposta tramite il canale di comunicazione protetto.

Per qualsiasi questione relativa alla protezione dei dati personali, è possibile rivolgersi al Responsabile della Protezione dei Dati presso SGSS al seguente indirizzo e-mail: [IT-DPO-SGSS@socgen.com](mailto:IT-DPO-SGSS@socgen.com)

Inoltre, è possibile sporgere reclamo presso le autorità competenti in materia di protezione dei dati nelle giurisdizioni dove la procedura di reclamo è ammessa.