



SYNLAB

Speak-Up Policy per soggetti terzi

1. Ambito di applicazione della Speak-Up Policy per soggetti terzi

La presente Speak-Up Policy per soggetti terzi ("**Policy**") ha lo scopo di incoraggiare e consentire ai partner commerciali¹ e ai loro rispettivi dipendenti, nonché ad altri soggetti terzi, di segnalare violazioni accertate o sospette del Supply Chain Due Diligence Act tedesco (*Lieferkettensorgfaltspflichtengesetz*) e del Codice di condotta per i fornitori di SYNLAB ("**Segnalanti**").

2. Principi generali

A prescindere dalle circostanze in cui viene effettuata una segnalazione, SYNLAB aderisce ai seguenti principi e intende applicarli in qualsiasi situazione e per tutte le misure intraprese.

2.1. Protezione dei Segnalanti

SYNLAB ritiene che la possibilità, per i soggetti terzi, di effettuare segnalazioni di violazioni possa avvenire solo sulla base di un sistema trasparente e affidabile, nell'ambito del quale i Segnalanti abbiano la certezza di agire in un'atmosfera sicura e protetta. SYNLAB si impegna pertanto a rispettare i seguenti principi:

Non ritorsione: i Segnalanti non devono temere alcuna conseguenza negativa di natura discriminatoria o disciplinare per aver effettuato una segnalazione in buona fede o per aver sollevato domande, dubbi e preoccupazioni.

Processo equo: tutti i casi saranno soggetti a una rigorosa imparzialità, si applica la presunzione di innocenza e si garantisce il diritto all'ascolto.

SYNLAB si impegna inoltre a compiere ogni ragionevole sforzo per preservare il più possibile la **riservatezza** delle segnalazioni legittime e delle informazioni in esse contenute. Pertanto, le segnalazioni possono essere presentate anche in forma anonima².

SYNLAB si riserva tuttavia il diritto di divulgare eventuali informazioni qualora:

- Il segnalante abbia fornito il proprio consenso;
- La divulgazione sia necessaria per indagare efficacemente in merito alla segnalazione e per adottare le relative misure opportune;
- La divulgazione sia necessaria per adempiere a un obbligo legale;
- La divulgazione sia obbligatoria ai sensi della legge vigente (ad esempio, autorità di contrasto).

2.2. Eccezione per uso improprio

È severamente vietato utilizzare intenzionalmente in modo improprio, a scopo di abuso, il sistema di segnalazione previsto dalla presente Policy (ad esempio, per presentare segnalazioni in malafede o a scopo di vendetta). I Segnalanti che ricorrono al sistema di segnalazione in modo improprio non sono tutelati dai principi sopra enunciati e possono incorrere in sanzioni ai sensi del diritto del lavoro, penale e civile.

Inoltre, non sono tollerati alcun tipo di minaccia, comportamento lesivo o atto di ritorsione. Tali comportamenti costituiscono una violazione dei nostri valori e possono comportare un'azione disciplinare.

¹ Un partner commerciale con cui SYNLAB ha stipulato un contratto per la fornitura di beni o la prestazione di servizi.

² Si prega di notare che lo svolgimento delle indagini risulterà più agevole qualora le segnalazioni non venissero effettuate in forma anonima, in modo da consentire eventuali domande e richieste di chiarimenti successivi.

2.3. Comunicazione ai soggetti interessati

SYNLAB informerà ragionevolmente le persone oggetto di una segnalazione.

Sulla base delle circostanze del singolo caso, SYNLAB può astenersi dal comunicare tale informazione per non compromettere l'efficacia dell'indagine, la protezione delle prove o la procedura di segnalazione.

2.4. Protezione dei dati

Nella gestione delle segnalazioni, SYNLAB si attiene alle leggi vigenti in materia di protezione dei dati e agli standard di sicurezza dei dati.

Le registrazioni delle segnalazioni e i relativi materiali d'indagine saranno conservati in conformità alle leggi vigenti e nella misura in cui ciò sia necessario per il conseguimento degli interessi legittimi di SYNLAB, in particolare per il funzionamento dei canali di segnalazione interni e per un'efficace gestione della conformità. Altri interessi legittimi includono l'istituzione, l'esercizio o la difesa di rivendicazioni legali o la garanzia di conformità agli obblighi di legge vigenti a cui SYNLAB è soggetta. Generalmente, trascorsi tre anni dal momento in cui l'ulteriore conservazione non è più legalmente richiesta, le registrazioni saranno cancellate in conformità alle leggi vigenti in materia di protezione dei dati.

Le segnalazioni ritenute infondate o le informazioni per altri motivi considerate al di fuori dell'ambito di applicazione della presente Policy saranno cancellate immediatamente in conformità alle leggi e ai regolamenti vigenti.

3. Procedura di segnalazione e gestione dei casi

La procedura di segnalazione prevista dalla presente Policy mira a consentire una gestione efficiente, sicura e trasparente delle segnalazioni.

I Segnalanti possono contribuire a tale obiettivo fornendo informazioni in modo conciso e sufficientemente dettagliato, nonché allegando prove a supporto della segnalazione, se disponibili.

3.1. Procedura di segnalazione e follow-up

Le segnalazioni possono essere presentate a SYNLAB tramite uno dei seguenti canali:

I segnalanti possono utilizzare lo strumento elettronico di segnalazione di SYNLAB al seguente link: <https://synlab.integrityline.app>. Questo sistema di comunicazione elettronica è gestito da EQS Group AG.

Le segnalazioni possono inoltre essere presentate anche direttamente tramite il proprio referente presso SYNLAB o tramite il Chief Human Rights Officer (CHRO) di SYNLAB.³

Il Segnalante riceverà una conferma di ricezione della segnalazione entro sette (7) giorni; le informazioni sullo stato di avanzamento della segnalazione saranno fornite in conformità alle leggi vigenti. Le persone competenti per la revisione della segnalazione potrebbero contattare il Segnalante per domande di follow-up ed eventuali chiarimenti.

³ Si prega di notare che in questi casi, anche per motivi tecnici, l'anonimato non può essere garantito.

3.2. Verifica della plausibilità e indagini approfondite

Attraverso una prima **verifica della plausibilità** con il coinvolgimento dei servizi competenti di SYNLAB, i casi ritenuti non plausibili saranno eliminati e chiusi. Il Segnalante verrà informato di conseguenza.

I casi ritenuti plausibili saranno oggetto di indagini approfondite. Tale valutazione approfondita del caso terrà conto di tutti i fatti noti e sarà effettuata con il coinvolgimento dei servizi più appropriati di SYNLAB (ad esempio, i reparti responsabili delle Risorse Umane, della Conformità o degli Audit interni), in base alla natura del caso. I potenziali conflitti di interesse (ad esempio, della persona accusata o delle parti coinvolte nell'indagine) vengono debitamente presi in considerazione.

La valutazione dei fatti avviene senza ritardi ingiustificati e in tempi ragionevoli, tenendo conto delle circostanze di fatto del caso (ad esempio, la gravità, la complessità, le informazioni e le prove presentate, ecc.). Se richiesto dalle specificità di ciascun caso, per la valutazione possono essere coinvolte risorse esterne. SYNLAB coinvolgerà e collaborerà con autorità pubbliche e altre istanze (comitato aziendale, responsabile della protezione dei dati (DPO), ecc.) nella misura in cui ciò sia richiesto dalle leggi vigenti e in conformità con esse.

A seguito dell'indagine, i casi saranno classificati e gestiti come segue:

- Le segnalazioni di violazioni che non possono essere provate saranno chiuse come **casi ritenuti infondati**. La decisione di chiusura del caso viene documentata.
- Le violazioni accertate sono classificate come casi ritenuti fondati. A questi casi si risponderà con **misure correttive** adeguate.

3.3. Misure correttive

Sulla base di una valutazione caso per caso, SYNLAB deciderà come rispondere nel modo più appropriato ed efficace ai casi ritenuti fondati, tenendo conto, tra l'altro, dei seguenti criteri:

- **Gravità della violazione:** valutazione del grado di compromissione (intensità o gravità di una violazione) e del numero di persone coinvolte;
- **Probabilità della violazione:** probabilità che un rischio di violazione si concretizzi in una violazione effettiva;
- **Urgenza:** rischio imminente di violazione o violazione già esistente;
- **Categoria della violazione:** classificazione dei casi (ad esempio, casi o reati penali) e delle circostanze (negligenza, dolo);
- **Reversibilità della violazione:** considerazioni relative alla possibilità di eliminare gli effetti negativi della violazione e valutazione delle eventuali risorse necessarie a tal fine;
- **Ambito della violazione:** violazione interna all'azienda SYNLAB o violazione da parte di un fornitore.

Le potenziali misure correttive comprendono, tra l'altro:

- Comunicazioni, avvisi, richieste di certificazioni o di audit ai partner aziendali;
- Esercizio di una pressione dal punto di vista commerciale per contrastare una violazione;
- Misure per annullare di fatto o risarcire i danni relativi a una violazione.

I programmi correttivi di base vengono stabiliti all'interno dei reparti coinvolti e sono soggetti all'approvazione del Chief Human Rights Officer.

Le misure correttive saranno attuate sotto la supervisione dei servizi competenti di SYNLAB, come previsto dal programma correttivo.

3.4. Chiusura e documentazione

Dopo aver applicato con successo le misure correttive e previa conferma da parte del Chief Human Rights Officer, i casi saranno considerati chiusi. La decisione di chiudere i casi verrà documentata. Inoltre, i servizi competenti di SYNLAB saranno informati della chiusura del caso in questione, in modo da determinare la necessità di un adeguamento o dell'adozione di nuove misure preventive.

3.5. Verifica dell'efficacia

L'efficacia della presente Policy e delle misure correttive sarà verificata su base regolare e, se necessario, appositamente per un caso specifico sotto la supervisione del Chief Human Rights Officer. Il Chief Human Rights Officer fornirà periodicamente alla direzione di SYNLAB informazioni sintetiche sullo stato di avanzamento delle procedure previste dalla presente Policy.