WHISTLEBLOWING

MISURE ADOTTATE DA CHG-MERIDIAN ITALIA S.P.A. IN RELAZIONE AL SISTEMA DI SEGNALAZIONE DEGLI ILLECITI E DELLE VIOLAZIONI DEL MODELLO DI ORGANIZZAZIONE E GESTIONE EX D.LGS. n. 231/2001

1 - SCOPO E INTRODUZIONE..... pag.2

2 - CANALI DI SEGNALAZIONE INTERNA..... pag.4

2.1 – Segnalazioni Whistleblowing Individuali..... pag.4

2.2 - Segnalazioni Whistleblowing da Portale..... pag.4

2.3 – Ombudsman pag.5

3 – REGISTRAZIONE E GESTIONE E DEFINIZIONE DELLA SEGNALAZIONE WHISTLEBLOWING..... pag.6

4 – PROCEDIMENTO DISCIPLINARE **(art.21 D.Lgs.4/2023)**..... pag.7

5 - SEGNALAZIONI ESTERNE ALL'AZIENDA **(artt.6 e 7 D.Lgs.24/2023)**.. pag.7

6 – SEGNALAZIONI PUBBLICHE **(art.15 D.Lgs.24/2023)**.....pag.8

FAQ..... pag.9

1 –SCOPO E INTRODUZIONE

CHG-MERIDIAN AG e le sue filiali (di seguito CHG-MERIDIAN), in cui si applica il Codice di Condotta del Gruppo CHG-MERIDIAN (e, per l'Italia, il Codice Etico di CHG MERIDIAN Italia S.p.a.), hanno implementato un processo di segnalazione delle violazioni previste dalla 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 e del D.Lgs. n. 24/2023 (whistleblower policy).

CHG-MERIDIAN si aspetta che i suoi dipendenti e partner commerciali segnalino tentativi, sospetti o effettive violazioni di leggi o regolamenti, nonché violazioni di norme interne come il Codice di Condotta e il Codice Etico.

La segnalazione deve essere fatta – per esempio – per le seguenti tipologie di violazioni:

- Sicurezza delle informazioni e dei dati personali (es. accesso non autorizzato, la perdita o il furto di informazioni riservate o dati personali).
- Protezione dei dati personali
- Outsourcing
- Ambiente
- Sostenibilità
- Diritti umani e del lavoro, compresa la discriminazione
- Antiriciclaggio
- Gestione della continuità aziendale, incluse eventi naturali, incendi e pandemie
- Compliance, incluse frodi, corruzione e appropriazione indebita.

Le persone che presentano una segnalazione sono anche chiamate "Whistleblower".

L'Amministratore Unico e la Direzione di CHG-MERIDIAN Italia sono convinti che la discussione aperta e franca di queste questioni e problematiche sia parte integrante della cultura aziendale di CHG, e continuerà a esserlo in futuro.

La cultura della trasparenza e del dialogo dovrebbe avere sempre la precedenza sull'uso di mezzi di comunicazione anonimi, nella misura in cui questo è possibile, senza che ciò

comporti alcun rischio per la propria persona o per la propria posizione all'interno dell'azienda.

Indipendentemente dal canale di comunicazione scelto, CHG-MERIDIAN garantisce al Whistleblower che nessuna informazione sulla sua persona o sui fatti o sulle circostanze della segnalazione sarà divulgata all'infuori delle persone autorizzate alla gestione della segnalazione stessa (es. Ombudsman, Gestore della segnalazione).

Tutte le segnalazioni saranno trattate in modo confidenziale e nel rispetto della riservatezza e il Whistleblower deciderà autonomamente se desidera o meno rivelare la propria identità.

Per questo motivo, deve essere istituito un canale di comunicazione che consenta di segnalare in modo completamente anonimo le questioni relative alla compliance. Inoltre, il Whistleblower può anche decidere di rivelare la propria identità durante il processo di gestione della segnalazione.

Tuttavia, la dichiarazione della propria identità può contribuire a stabilire i fatti della questione, in quanto consente di chiarire meglio e con maggiore precisione i fatti e le questioni che sorgono nell'ambito del trattamento.

Inoltre, le notificazioni e le comunicazioni al Whistleblower relative alla gestione della segnalazione e di eventuali ulteriori misure può essere effettuata soltanto solo se l'identità del Whistleblower è nota.

Il Compliance Officer di CHG-MERIDIAN AG deve sempre garantire che il Whistleblower rimanga anonimo, a meno che non decida rivelare la propria identità.

Le segnalazioni saranno trasmesse a terzi solo in una forma che garantisca l'anonimato del Whistleblower, salvo che questo abbia rivelato la propria identità nell'ambito del procedimento.

I seguenti canali di segnalazione non devono essere utilizzati per richieste o reclami di natura commerciale (ad es problemi tecnici con TESMA o domande/discussioni relative al contratto del cliente), oppure (come evidenziato nelle Linee Guida ANAC Whistleblowing e nell'art. 1 D.lgs. n. 24/2023), per questioni legate a un interesse personale del segnalante, che attengono ai propri rapporti individuali di lavoro, ovvero inerenti ai rapporti di lavoro

con le figure gerarchicamente sovraordinate (es. vertenze di lavoro, discriminazioni, conflitti interpersonali tra colleghi, segnalazioni su trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di una lesione dell'interesse pubblico o dell'integrità dell'ente privato o dell'amministrazione pubblica), a meno che non configurino violazioni del Codice Etico e del Modello di Organizzazione e Gestione adottato da CHG-MERIDIAN Italia in attuazione del D.Lgs. n. 231/2001 (es. lesioni subite con violazione delle norme sulla tutela della salute e sicurezza sul lavoro).

2 – CANALI DI SEGNALAZIONE INTERNA

2.1 – Segnalazioni Whistleblowing Individuali

Le segnalazioni possono essere fatte di persona o via e-mail ai seguenti Responsabili Regulatory Affairs del Gruppo CHG-MERIDIAN, alle seguenti email:

- compliance@chg-meridian.com
- security@chg-meridian.com
- privacy@chg-meridian.com
- bcm@chg-meridian.com
- outsourcing@chg-meridian.com
- aml@chg-meridian.com

O anche per telefono, chiamando direttamente i colleghi o tramite il numero +49 751 503 222.

La segnalazione sarà trattata in modo confidenziale ed elaborata esclusivamente nell'ambiente riservato di ServiceNow denominato "Security Incidents".

2.2 - Segnalazioni Whistleblowing da Portale

Le segnalazioni da parte del personale del Gruppo CHG-MERIDIAN possono essere effettuate online all'interno del portale Regulatory Affairs.

Il portale è accessibile al seguente link: Regulatory Affairs Portal

Tuttavia, in questo caso la segnalazione non è anonima.

La segnalazione sarà, comunque, trattata in modo confidenziale ed elaborata esclusivamente nell'ambiente riservato di ServiceNow denominato "Security Incidents".

2.3 – Ombudsman

La segnalazione **in forma anonima** potrà essere inviata al OMBUDSMAN (vedi il sito di CHG-MERIDIAN AG nella sezione Corporate Governance)

Stefan Fischerkeller (DDSK GmbH: Dr.-Klein-Str. 29 in 88069 Tettnang Germany)

Phone: +49 7542 94921-90

E-Mail: whistleblowing.chg.meridian@ddsk.de (Oggetto: "CHG Ombudsman")

L'Ombudsman è il punto di riferimento centrale e anonimo del sistema di Whistleblower di CHG-MERIDIAN.

La segnalazione iniziale e i fatti corrispondenti vengono trasmessi in forma anonima all'ufficio Regulatory Affairs di CHG-MERIDIAN come Security Incident.

All'Ombudsman è espressamente vietato rivelare l'identità del Whistleblower a CHG-MERIDIAN, a meno che l'informatore non abbia espressamente dato il suo consenso in precedenza o che la divulgazione dell'identità sia stata da questo successivamente espressamente approvata.

L'Ombudsman, se tecnicamente possibile, entro 7 giorni confermerà al Whistleblower il ricevimento della segnalazione, comunicando il numero assegnato.

L'Ombudsman, se tecnicamente possibile, fornirà al Whistleblower il riscontro alla segnalazione entro 3 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).

3 – REGISTRAZIONE, GESTIONE E DEFINIZIONE DELLA SEGNALAZIONE WHISTLEBLOWING

In linea di principio, tutti gli incidenti di sicurezza devono essere gestiti nel rispetto della legislazione applicabile sulla protezione dei dati personali.

Al fine di adempiere agli obblighi nascenti dalle segnalazioni e di garantirne una gestione efficace, tutte le segnalazioni in arrivo vengono protocollate in base al loro contenuto e al numero. La protocollazione serve, inoltre, a garantire che tutte le segnalazioni siano state gestite in forma appropriata e che le relative conclusioni e le conseguenti misure adottate siano appropriate.

La responsabilità della protocollazione e della documentazione spetta al Compliance Officer o ai rispettivi responsabili ai quali è assegnata la segnalazione.

La gestione delle segnalazioni è di competenza di Regulatory Affairs ed è finalizzata al completo chiarimento delle sospette violazioni o dei rischi, al fine di garantire l'adozione di misure adeguate per proteggere l'azienda e/o i suoi dipendenti.

Le persone che agiscono come Regulatory Affairs dispongono dei necessari poteri ed autorizzazioni.

Nel rispetto della massima riservatezza, l’incaricato di Regulatory Affairs può coinvolgere il local Compliance Officer o il management della filiale italiana, per acquisire le informazioni necessarie a chiarire i fatti o per provvedere alla definizione della segnalazione ed all’adozione delle conseguenti ed appropriate misure.

Alle stesse condizioni, l’incaricato da Regulatory Affairs può anche incaricare l'Internal Audit o, se necessario o appropriato, esperti esterni per chiarimenti o supporto nella gestione della segnalazione.

Ove possibile e necessario, Regulatory Affairs consulta il Whistleblower e lo informa dell’andamento e delle conclusioni raggiunte sulla segnalazione.

Gli incaricati da Regulatory Affairs sono responsabili di garantire che tutte le segnalazioni siano protocollate, che la gestione sia documentata in modo esauriente e che le misure definite siano seguite fino alla loro attuazione.

A questo scopo, i Security Incidents generati all'interno dell'applicazione ServiceNow devono essere identificati e numerati in modo univoco, con una numerazione progressiva.

Regulatory Affairs includerà nel report al Consiglio di Gestione (o C.d.A.) di CHG-MERIDIAN AG il numero e il contenuto delle segnalazioni ricevute, la rispettiva area tematica, lo stato dell'istruttoria e le misure adottate a seguito della segnalazione.

Continuano a essere applicati i principi di riservatezza e protezione dei dati.

Se la segnalazione è stata ricevuta dall'Ufficio Compliance della filiale locale, questo dovrà relazionarne Regulatory Affairs, includendo il numero e il contenuto delle segnalazioni ricevute, la rispettiva area tematica, lo stato dell'istruttoria e le misure adottate a seguito della segnalazione.

4 - PROCEDIMENTO DISCIPLINARE (ART. 21 D.LGS. N. 24/2023)

Sono passibili di procedimento disciplinare tutti coloro che:
- abbiano commesso **ritorsioni** in danno del segnalante;
- abbiano ostacolato o tentato di ostacolare la segnalazione;
- abbiano violato l'obbligo di riservatezza sulla segnalazione e sull'identità del segnalante;
- siano stati riconosciuti responsabili dei fatti segnalati;
- siano stati condannati per diffamazione o calunnia per la falsa segnalazione o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero in caso di responsabilità civile, per lo stesso titolo, ovvero di dolo o colpa grave.

E' vietata qualunque ritorsione a carico del segnalante a causa della segnalazione.

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 sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.

5 - SEGNALAZIONI ESTERNE ALL'AZIENDA (artt. 6 e 7 D.Lgs. n. 24/2023)

La persona segnalante può effettuare una segnalazione esterna se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

a) non è prevista, nell'ambito del suo contesto lavorativo, 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 Decreto 24/2023;

b) la persona segnalante ha già effettuato una segnalazione interna ai sensi dell'articolo 4 del Decreto 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.

Maggiori informazioni sui presupposti, sui canali e sulle modalità di segnalazione sono reperibili sui siti dedicati predisposti dall'ANAC: https://www.anticorruzione.it/-/whistleblowing –

6 - SEGNALAZIONI PUBBLICHE (ART. 15 D.LGS. N. 24/2023)

I segnalanti possono effettuare direttamente una divulgazione pubblica (es. denuncia all'Autorità Giudiziaria) quando:

- la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

FAQ

1. CHG-MERIDIAN dispone di un canale di segnalazione Whistleblowing di gruppo?

Sì. CHG-MERIDIAN offre canali di segnalazione a livello di Gruppo. Alcuni di questi canali sono pubblici, trasparenti, privi di barriere e anonimi. Tutte le segnalazioni sono trattate allo stesso modo.

2. Chi può segnalare?

Tutti, poiché sono disponibili canali per tutte le persone. Sia per i dipendenti che per i terzi esterni e gli stakeholder.

3. Cosa posso segnalare?

Ogni attività sospetta di reale, tentata o sospetta violazione e infrazione delle leggi e delle norme interne. Sono compresi anche i tentativi di frode. Questo include anche i sospetti di tentativi di frode.

Le segnalazioni possono riguardare il comportamento dei dipendenti interni, nonché le procedure e le attività relativi all'attività di CHG-MERIDIAN e ai partner commerciali.

Si prega di segnalare solo se si ritiene che la violazione o l'infrazione sia vera.

Non segnalate reclami o richieste di informazioni di carattere commerciale. Ad esempio, richieste su contratti con i clienti o reclami tecnici TESMA.

Non segnalate questioni che attengono ai propri rapporti individuali di lavoro, ovvero inerenti ai rapporti di lavoro con le figure gerarchicamente sovraordinate (es. vertenze di lavoro, conflitti interpersonali tra colleghi, segnalazioni su trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di una lesione dell'interesse pubblico o dell'integrità di CHG-MERIDIAN Italia), a meno che non configurino violazioni del Codice Etico e del Modello di Organizzazione e Gestione adottato da CHG in attuazione del D.Lgs. n. 231/2001 (es. lesioni subite con violazione delle norme sulla tutela della salute e sicurezza sul lavoro).

4. Ci sono diversi modi per fare una segnalazione?

Sì. CHG-MERIDIAN offre diversi canali. È possibile contattare il proprio manager, i Regulatory Affairs individualmente o tramite il portale dei Regulatory Affairs. Potete anche ricorrere all'Ombudsman esterno.

5. Chi è responsabile della gestione della mia segnalazione?

La segnalazione viene solitamente gestita come Security Incident all'interno dai Regulatory Affairs. Se necessario, possono essere coinvolti altri funzionari o dirigenti locali, seguendo un approccio strettamente confidenziale.

6. La mia identità è trattata in modo confidenziale?

Sì. Oltre ai requisiti di protezione dei dati, tutte le segnalazioni ed i Security Incident sono trattati in modo confidenziale. **Se si desidera mantenere l'anonimato è possibile contattare l'Ombudsman.**

7. Sarò informato sullo stato della mia segnalazione?

Sì. Se si utilizzano i canali interni si ha comunque un contatto diretto con Regulatory Affairs.

Se si contatta l'Ombudsman, riceverete una conferma di ricezione entro 7 giorni e una comunicazione dell'esito della segnalazione entro 3 mesi, se tecnicamente possibile.

8. Tutte le segnalazioni verranno gestite?

Sì. Ogni segnalazione ricevuta dai Regulatory Affairs verrà verificata e gestita.

9. Cosa succederà alla mia segnalazione?

Dipende da ogni singola segnalazione, dalla qualità e quantità delle informazioni. In generale, Regulatory Affairs o i rispettivi Incaricati indagano sul caso e adottano misure preventive.

A volte è necessario acquisire informazioni da parte di altri dipartimenti o Paesi (filiali) per chiudere una segnalazione.

10. Che ne è della mia protezione come Whistleblower?

CHG-MERIDIAN non tollera ritorsioni di alcun tipo!

Le persone che presentano reclami o segnalazioni in buona fede non saranno penalizzate per averlo fatto. Se ritenete che voi o altri abbiate subito ritorsioni o che siate stati discriminati in qualche modo per aver presentato una segnalazione, vi invitiamo a segnalarlo immediatamente.

Indagheremo su tutte le accuse plausibili di discriminazione. Le accuse fondate di discriminazione da parte di CHG-MERIDIAN saranno perseguite anche come violazione della Compliance.