



Standard Operating Procedure

Titolo: Procedura Whistleblowing

KK-QD-105319

VERSIONE ITALIANAPAG. 2

ENGLISH VERSIONPAG. 15



Standard Operating Procedure

1. **SCOPO:**

La presente procedura è adottata dalla Società Kyowa Kirin S.r.l ("la Società") in ottemperanza a quanto stabilito dal Decreto Legislativo 10 marzo 2023, n. 24 (nel testo: Decreto o D. Lgs. 24/2023) in vigore dal 30 marzo 2023 che recepisce la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea (c.d. direttiva whistleblowing) di cui si è venuti a conoscenza nel contesto lavorativo, lesive dell'interesse pubblico o dell'integrità dell'amministrazione pubblica o dell'ente privato.

La procedura inoltre è predisposta in coerenza con la KKI Regional Policy Speaking-Up (Whistleblowing) KK-QD-058101 ed ai protocolli di comportamento di cui al Modello Organizzativo adottato dalla Società ai sensi del D.Lgs. 231/2001.

La presente procedura è stata approvata dal Consiglio di Amministrazione della Società in data 25.03.2024, unitamente all'identificazione dei ruoli organizzativi coinvolti nel processo di gestione delle segnalazioni di whistleblowing e alle relative responsabilità.

2. **CAMPO DI APPLICAZIONE:**

La presente procedura si applica a qualsiasi segnalazione di comportamenti consistenti in violazioni (effettive o presunte) del Codice di Condotta del Gruppo, di procedure e policy aziendali, del Modello Organizzativo adottato ai sensi del D. Lgs. 231/2001 e di leggi e regolamenti applicabili, acquisite all'interno del contesto lavorativo, effettuata attraverso gli appositi canali di segnalazione messi a disposizione dalla Società.

Sono escluse dall'ambito di applicazione della presente procedura:

- le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale che attengano esclusivamente ai rapporti individuali di lavoro, ovvero ai rapporti di lavoro con le figure gerarchicamente sovraordinate;
- le violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale;
- violazioni disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali che garantiscono già apposite procedure di segnalazione.

3. **DEFINIZIONI E ABBREVIAZIONI:**

3.1. Definizioni

- **"segnalazioni"**: qualsiasi comunicazione, scritta o orale, anche in forma anonima, contenente informazioni sulle violazioni;
- **"violazioni"**: violazioni del Codice di Condotta del Gruppo, di procedure e policy aziendali, del Modello Organizzativo adottato ai sensi del D. Lgs. 231/2001, e di leggi o regolamenti applicabili;



Standard Operating Procedure

- **“informazioni sulle violazioni”**: tutte le informazioni, tra le quali i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell’organizzazione con cui la persona segnalante intrattiene un rapporto giuridico ed anche gli elementi informativi riguardanti condotte volte ad occultare tali violazioni;
- **“segnalazione interna”**: comunicazione delle “segnalazioni” attraverso il predisposto canale interno di segnalazione;
- **“segnalante”**: persona fisica che effettua la segnalazione di informazioni sulle violazioni acquisite nell’ambito del proprio contesto lavorativo;
- **“facilitatore”**: persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all’interno dello stesso contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- **“contesto lavorativo”**: attività lavorative o professionali, presenti o passate attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all’autorità giudiziaria o contabile;
- **“persona coinvolta”**: persona fisica o giuridica menzionata nella segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata;
- **“responsabile del canale”**: soggetto individuato dalla Società responsabile della gestione del canale e della segnalazione dotato di autonomia organizzativa e funzionale;
- **“referente interno”**: Dipartimento Legal & Compliance; qualora il referente interno sia la persona coinvolta nella segnalazione, il ruolo di referente interno verrà svolto dall’organo amministrativo;
- **“ritorsione”**: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione e strettamente legato alla stessa, 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 ingiusto;
- **“seguito”**: l’azione ovvero le azioni avviata dal soggetto cui è affidata la gestione del canale di segnalazione;
- **“riscontro”**: comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione comprendendo le misure previste o adottate o da adottare e dei motivi della scelta effettuata;
- **“piattaforma”**: canale di segnalazione interna adottato dalla Società (come meglio specificato al paragrafo 5.3 e ss) per trasmettere le informazioni sulle violazioni;
- **“Organismo di Vigilanza (“OdV”)**: Organismo di Vigilanza ai sensi del D. Lgs. n. 231/2001 di Kyowa Kirin S.r.l.;
- **“Modello 231”**: Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. n. 231/2001 di Kyowa Kirin S.r.l.



Standard Operating Procedure

4. RESPONSABILITÀ:

4.1. Il responsabile del canale, anche attraverso l'utilizzo della piattaforma:

- rende disponibili, anche attraverso la presente procedura e le informazioni pubblicate sulla piattaforma, chiare informazioni sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne;
- rilascia alla persona segnalante il riscontro di ricevimento della segnalazione nei termini previsti;
- valuta i criteri di processabilità della segnalazione;
- condivide con il referente interno, definito nell'ambito della presente procedura, e l'OdV (quando applicabile), la segnalazione, l'avvio di eventuali indagini, il loro esito e il riscontro da fornire al segnalante;
- trasmette al segnalante il riscontro circa la chiusura dell'iter di gestione della segnalazione;
- mantiene le interlocuzioni con la persona segnalante e, se del caso, gestisce la richiesta di integrazioni e l'esecuzione di eventuali colloqui di approfondimento con la persona segnalante, se richiesti;
- archivia e conserva la documentazione sulla segnalazione nei tempi normativamente previsti;
- garantisce il rispetto del principio di riservatezza.

4.2 Il referente interno:

- identifica, all'interno della Società, i soggetti da coinvolgere e condivide con questi quanto emerso dall'analisi effettuata dal responsabile del canale;
- è delegato a fornire al responsabile del canale riscontro in merito alle decisioni prese dalla Società per l'approfondimento di quanto oggetto di segnalazione;
- attua le raccomandazioni espresse dal responsabile del canale per approfondire quanto oggetto di segnalazione;
- coordina e monitora la fase delle eventuali indagini con le funzioni interne/team esterni incaricati;
- condivide con il responsabile del canale l'avvio di eventuali indagini, il loro esito e il riscontro da fornire al segnalante;
- individua piani di miglioramento per evitare il ripetersi di eventi oggetto di segnalazione;
- assicura che tutte le informazioni previste sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, siano rese disponibili sui canali aziendali;
- gestisce, con il supporto delle funzioni aziendali competenti, le attività conseguenti ad eventuali divulgazioni pubbliche nei casi previsti;
- garantisce il rispetto del principio di riservatezza.

4.3 Il segnalante:

CONFIDENTIAL

Page 4 of 28



Standard Operating Procedure

- trasmette le segnalazioni nel rispetto della presente procedura;
- è tenuto a fornire informazioni circostanziate relative a quanto oggetto di segnalazione;
- indica eventuali soggetti destinatari di forme di tutela e protezione (es. facilitatori).

4.4 L' OdV:

- in caso la segnalazione sia relativa a condotte illecite ai sensi del D.Lgs. n. 231/2001, o violazioni del Modello Organizzativo, coordina e monitora la fase delle indagini con le funzioni interne/team esterni incaricati, valuta l'esito delle indagini e gli eventuali provvedimenti conseguenti;
- garantisce il rispetto del principio di riservatezza.

4.5 Il rappresentante legale:

- interloquisce con ANAC in caso di attivazione di attività ispettive.

4.6 Il CDA:

- approva la presente procedura unitamente alla struttura dei ruoli organizzativi connessi;
- garantisce il rispetto delle misure per la protezione della persona segnalante;
- garantisce che siano adottati gli eventuali provvedimenti in conformità a quanto previsto dal sistema sanzionatorio contemplato nel Modello Organizzativo 231/2001, ove applicabile.

5. **PROCEDURA:**

5.1 Soggetti che possono effettuare una segnalazione (c.d. "segnalante")

Possono procedere alla segnalazione:

- i dipendenti;
- i lavoratori autonomi e collaboratori che svolgono la propria attività presso soggetti pubblici e privati;
- i liberi professionisti;
- i volontari;
- i consulenti;
- gli azionisti;
- gli amministratori;
- i fornitori di prestazioni a favore di terzi a qualsiasi titolo (a prescindere dalla natura di tali attività) anche in assenza di corrispettivo;
- i tirocinanti anche non retribuiti;
- i soggetti che esercitano funzioni di amministrazione, di direzione, di controllo, di vigilanza ovvero di rappresentanza, anche se le relative attività sono svolte a titolo di fatto e non di diritto;
- Sono, altresì, compresi nella categoria in oggetto tutti quei soggetti che, a qualsiasi titolo, vengono a conoscenza di illeciti nell'ambito del contesto lavorativo della Società ovvero:
 - o quando il rapporto di lavoro non sia ancora iniziato;
 - o durante il periodo di prova;



Standard Operating Procedure

- allo scioglimento del rapporto.

5.2 Referente interno

La Società ha affidato il ruolo di referente interno ai sensi della presente procedura, ai membri del Dipartimento Legal & Compliance della società.

5.3 Canale di segnalazione interna

La Società ha previsto un canale di segnalazione interna che il segnalante deve utilizzare per la trasmissione delle informazioni sulle violazioni. L'istituzione di tale canale permette una più efficace prevenzione e accertamento delle violazioni. Tale scelta risponde al principio di favorire una cultura della buona comunicazione e della responsabilità sociale d'impresa nonché di miglioramento della propria organizzazione.

Il canale di segnalazione interna è rappresentato dalla "KKI Speak-up line" accessibile attraverso la sezione Speak Up nella pagina della intranet aziendale dedicata alla Compliance, al link <https://secure.ethicspoint.eu/domain/media/en/gui/105727/index.html>.

Il canale di segnalazione interna garantisce la riservatezza dell'identità del segnalante, del facilitatore (ove presente), delle persone coinvolte e comunque menzionate nella segnalazione nonché del contenuto della stessa e della relativa documentazione inoltrata o integrabile.

Il canale è utilizzabile anche da soggetti esterni alla Società, tramite accesso al sito internet.

5.4 Soggetto responsabile della gestione del canale (c.d. "responsabile del canale")

La gestione del canale interno è affidata al Regional Compliance team di casa madre, i cui membri sono in possesso dei requisiti di autonomia, indipendenza e specificamente formati.

5.5 Caratteristiche del canale di segnalazione interna

Il canale di segnalazione della Società "Speak-up line" è gestito da un fornitore esterno e consente ai dipendenti di effettuare segnalazioni tramite un portale web o tramite telefono. Il sistema consente segnalazioni anonime, nonché la possibilità di interagire direttamente con il segnalante, in modo anonimo.

Il trattamento dei dati personali deve sempre tener conto ed essere conforme agli obblighi previsti dal GDPR e dal D. Lgs. 196/2003 e ss.mm.ii. La Società, in qualità di titolare del trattamento attraverso il canale di segnalazione interna è tenuta ad effettuare una previa analisi del disegno organizzativo comprensivo della fondamentale valutazione del possibile impatto sulla protezione dei dati (art. 35 del GDPR).

5.6 Caratteristiche della segnalazione e segnalazioni anonime



Standard Operating Procedure

È necessario che la segnalazione sia il più possibile circostanziata al fine di consentire l'analisi dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni. In particolare, è necessario risultino chiare:

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- la descrizione del fatto;
- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Le informazioni sulle violazioni segnalate devono essere veritiere. Non si considerano tali semplici supposizioni, indiscrezioni scarsamente attendibili (c.d. voci di corridoio), così come notizie di pubblico dominio, informazioni errate (ad eccezione di errore genuino), palesemente prive di fondamento o fuorvianti ovvero se meramente dannose o offensive. Non è invece necessario che il segnalante sia certo dell'effettivo accadimento dei fatti segnalati e dell'identità dell'autore degli stessi.

È utile anche che il segnalante fornisca documenti che possano dare elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Le segnalazioni anonime, ove circostanziate, sono equiparate a segnalazioni ordinarie e in tal caso considerate nell'ambito della presente procedura anche in riferimento alle tutele del segnalante, qualora successivamente identificato, ed agli obblighi di conservazione.

5.7 Iter operativo di gestione della segnalazione

Il segnalante trasmette la segnalazione tramite il canale interno dedicato.

Il segnalante attiva la segnalazione attraverso il link sopra indicato in modalità scritta, mediante la compilazione di un form guidato.

Qualora il segnalante preferisca effettuare una segnalazione oralmente, potrà richiedere un incontro con il proprio Line Manager o con il Referente interno o con l'HR Director. In caso di incontro diretto, lo svolgimento dell'incontro deve essere assicurato entro un tempo ragionevole (10-15 giorni), preferendo che l'audizione avvenga in locali diversi da quelli aziendali. Se il segnalante effettua la segnalazione oralmente mediante un incontro fissato, la stessa, previo consenso del segnalante stesso, è documentata a cura del Line Manager/Referente interno/HR Director con la registrazione su un dispositivo idoneo alla conservazione e alla riproduzione vocale ovvero tramite la redazione di un verbale. In questa ultima ipotesi, il segnalante può verificare, rettificare e/o confermare il verbale dell'incontro mediante relativa sottoscrizione.

La ricezione della segnalazione da parte del soggetto responsabile del canale avvia il processo di gestione delle segnalazioni. Il responsabile del canale procede quindi alla sua "lavorazione".

Alla ricezione della segnalazione, il soggetto responsabile del canale provvede a comunicare una conferma di ricezione al segnalante entro 7 giorni dal ricevimento della segnalazione e la presa in carico della segnalazione.



Standard Operating Procedure

Il soggetto responsabile del canale procede con una prima verifica del contenuto della segnalazione anche in riferimento alla sua verificabilità in base alle informazioni fornite. Il responsabile del canale informa tempestivamente il referente interno, garantendo il rispetto del principio di riservatezza.

Qualora sia necessario acquisire elementi integrativi, il responsabile del canale contatterà il segnalante tramite la piattaforma. Se il segnalante non fornisce, entro 3 mesi dalla richiesta di integrazione, informazioni aggiuntive il responsabile del canale procede con l'archiviazione della segnalazione dandone comunicazione al segnalante e informando il referente interno.

Qualora la segnalazione sia relativa a condotte illecite ai sensi del D.Lgs. n. 231/2001, o violazioni del Modello Organizzativo il referente interno informa, nel rispetto del principio di riservatezza, l'Organismo di Vigilanza al fine di valutare la modalità di avvio della fase di indagine, fatto salvo il rispetto del principio di autonomia e indipendenza dell'OdV rispetto al modo con cui gestire la segnalazione ai fini e per gli effetti del D. Lgs. n. 231/01.

Il referente interno, a chiusura dell'indagine, predispone un report finale e ne condivide gli esiti con il responsabile del canale e l'Organismo di Vigilanza ove applicabile, al fine di procedere con il riscontro al segnalante. Il riscontro al segnalante deve essere trasmesso dal responsabile del canale entro tre mesi dalla data di conferma di ricezione della segnalazione ovvero, in mancanza di tale conferma, dalla scadenza del termine di sette giorni dalla presentazione della segnalazione. Solo in casi eccezionali, qualora la complessità della segnalazione lo richiedesse, o in considerazione dei tempi di risposta del segnalante, il responsabile del canale, informato prontamente il segnalante prima della scadenza, con opportuna motivazione, potrà continuare la fase di indagine per il tempo necessario e dando al segnalante periodici aggiornamenti.

Ove applicabile, l'OdV, nell'ambito della sua autonomia operativa, valuta l'esito ricevuto e, qualora la segnalazione sia fondata, gli eventuali provvedimenti conseguenti valutando l'adozione di eventuali misure ritenute necessarie ai fini dell'adeguamento del Modello dando corso alle comunicazioni necessarie per l'applicazione delle eventuali sanzioni. Gli eventuali provvedimenti conseguenti sono applicati in conformità a quanto previsto dal sistema sanzionatorio previsto nel Modello Organizzativo 231.

In caso di diffamazione o di calunnia, accertata con condanna anche di primo grado, la Società procede con un procedimento sanzionatorio nei confronti del segnalante.

Si specifica che, dalla ricezione della segnalazione fino alla sua chiusura, ogni soggetto che si trovasse in una situazione di conflitto di interesse deve astenersi dall'assumere decisioni al fine di garantire il rispetto del principio di imparzialità.

5.8 Trasmissione delle segnalazioni con erroneo destinatario

Qualora la segnalazione sia trasmessa a un soggetto diverso da quello preposto a riceverla, chi la riceve ha l'obbligo di trasmetterla entro sette giorni al soggetto competente dando notizia della trasmissione alla persona segnalante e garantendo una gestione conforme agli obblighi di riservatezza. La Società adotta sanzioni a livello disciplinare in caso di mancato rispetto dell'obbligo di trasmissione.



Standard Operating Procedure

Nel caso di involontaria trasmissione della segnalazione a soggetto diverso da quello legittimato a riceverla, il segnalante deve dimostrare la mera negligenza e l'assenza di un interesse personale nella erronea trasmissione.

5.9 Conservazione della documentazione sulla segnalazione interna

Le segnalazioni interne e tutta la relativa documentazione allegata ovvero integrata sono conservate dal responsabile del canale e dal Referente Interno, curando che venga rispettata la riservatezza, per il tempo necessario al trattamento della segnalazione stessa.

In ogni caso, la documentazione è conservata soltanto per un periodo temporale individuato nel massimo di cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

In tutti i casi citati, è necessario che la conservazione delle segnalazioni interne e della relativa documentazione, sia conforme alle garanzie comunitarie e nazionali sul trattamento dei dati personali nonché alle predisposte misure sul diritto alla riservatezza.

5.10 Obblighi di informazione

Le informazioni sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni sono disponibili nell'apposita sezione Speak Up nella pagina della intranet aziendale dedicata alla Compliance, all'interno di Veeva Quality, sistema certificato dedicato alla registrazione di procedure e training e all'interno delle cartelle comuni.

Inoltre, tali informazioni sono pubblicate sul sito internet della Società per renderle accessibili a terzi.

La Società ha inoltre provveduto a dare informativa della presente procedura alle organizzazioni sindacali.

5.11 Obbligo di riservatezza

Tutte le segnalazioni ed i relativi allegati non sono utilizzati oltre il tempo necessario per darne seguito.

È previsto che l'identità del segnalante unitamente a qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non siano rivelate senza il consenso espresso del segnalante stesso a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli artt. 29 e 32, paragrafo 4 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del codice in materia di protezione dei dati personali di cui al D. Lgs. 30 giugno 2003, n. 196.

La Società tutela l'identità delle persone coinvolte, dei facilitatori e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione stessa, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

Le circostanze di mitigazione della tutela del diritto alla riservatezza comprendono:

- nell'ambito di un procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'art. 329 c.p.p.: è imposto l'obbligo di segretezza degli atti delle



Standard Operating Procedure

indagini preliminari sino al momento in cui l'indagato non abbia il diritto ad averne conoscenza e, comunque, non oltre la chiusura di tale fase;

- nell'ambito del procedimento stabilito presso la Corte dei Conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria;
- nell'ambito del procedimento disciplinare, l'identità del 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 del segnalante a rivelare la propria identità;
- nei casi di procedimento disciplinare avviato nei confronti del presunto autore della condotta segnalata, sarà dato avviso in forma scritta al segnalante delle ragioni della rivelazione dei dati riservati quando la rivelazione sarà indispensabile anche ai fini della difesa della persona coinvolta.

Poste la vigenza delle mitigazioni appena elencate, il soggetto coinvolto, su sua istanza, è sentito anche attraverso un procedimento cartolare mediante l'acquisizione di osservazioni scritte e di documenti.

Tra gli obblighi di riservatezza si comprendono:

- la sottrazione della segnalazione e della documentazione ad essa allegata al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e ss. della l. n. 241/1990 e all'accesso civico generalizzato di cui agli artt. 5 e ss. del d.lgs. n. 33/2013;
- le amministrazioni ed enti coinvolti nella gestione delle segnalazioni garantiscono la riservatezza durante tutte le fasi del procedimento di segnalazione, ivi compreso l'eventuale trasferimento delle segnalazioni ad altre autorità competenti.

5.12 Tutela dei dati personali

Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, è effettuato a norma:

- del Regolamento (UE) 2016/679;
- del D. Lgs. 30 giugno 2003, n. 196 e ss.mm.ii.

La comunicazione dei dati personali da parte di istituzioni, di organi o degli organismi dell'Unione Europea è effettuata in conformità del Regolamento (UE) 2018/1725.

Il trattamento dei dati personali relativi alla ricezione e alla gestione delle segnalazioni è effettuato dal titolare, nel rispetto dei principi di cui agli artt. 5 e 25 del regolamento (UE) 2016/679, fornendo preliminarmente le idonee informazioni ai soggetti segnalanti e alle persone coinvolte nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

L'informativa agli interessati, riepilogativa anche dei loro diritti e delle modalità per esercitarli, è reperibile sul sito internet della Società.

5.13 Misure di protezione e di sostegno



Standard Operating Procedure

Sono previste adeguate misure per proteggere i segnalanti dalle ritorsioni dirette e dalle ritorsioni indirette.

Le misure di protezione si applicano se al momento della segnalazione la persona segnalante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate fossero vere, rientrassero nell'ambito oggettivo e sia stata rispettata la procedura di segnalazione.

In caso di diffamazione o di calunnia, accertata con condanna anche di primo grado, le tutele non sono garantite.

Le misure di protezione si applicano anche:

- a) ai facilitatori;
- b) alle persone del medesimo contesto lavorativo della persona segnalante/denunciante che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- c) ai colleghi di lavoro della persona segnalante/denunciante che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- d) agli enti di proprietà della persona segnalante/denunciante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

5.13.1 Divieto di ritorsione

I soggetti enumerati nel paragrafo 5.1 non possono subire alcuna ritorsione. A titolo informativo e non esaustivo si considerano "ritorsioni":

- il licenziamento, la sospensione o misure equipollenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni;
- il cambiamento del luogo di lavoro;
- la riduzione dello stipendio;
- la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione di accesso alla stessa;
- le note di merito negative o le referenze negative non adeguatamente motivate;
- l'adozione di misure disciplinari o di altre sanzioni (anche pecuniarie);
- la coercizione;
- l'intimidazione;
- le molestie;
- l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole immotivato;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- i danni, anche alla reputazione della persona, in particolare sui social media,
- i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;



Standard Operating Procedure

- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento di un contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici ovvero medici.

Gli atti assunti in violazione del divieto di ritorsione sono nulli.

Nell'ambito di procedimenti giudiziari o amministrativi ovvero in caso di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati nei confronti dei soli soggetti segnalanti, si presume che gli stessi siano stati posti in essere a causa della segnalazione. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione è del soggetto che ha posto in essere gli atti ritorsivi.

I segnalanti possono comunicare all'ANAC le ritorsioni che ritengono di avere subito, sia quelle tentate o prospettate.

L'ANAC informa l'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza.

5.13.2 Misure di sostegno

Il segnalante potrà rivolgersi a enti del Terzo settore presenti nell'elenco pubblicato sul sito ANAC. Si tratta di enti che esercitano attività di interesse generale per il perseguimento, senza scopo di lucro, di finalità civiche, solidaristiche e di utilità sociale ("promozione della cultura della legalità, della pace tra i popoli, della nonviolenza e della difesa non armata; promozione e tutela dei diritti umani, civili, sociali e politici, nonché dei diritti dei consumatori e degli utenti delle attività di interesse generale, promozione delle pari opportunità e delle iniziative di aiuto reciproco, incluse le banche dei tempi e i gruppi di acquisto solidale") e che hanno stipulato convenzioni con ANAC.

Le misure di sostegno fornite consistono in informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni offerta dalle disposizioni normative nazionali e da quelle dell'Unione europea, sui diritti della persona coinvolta, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato.

5.13.3 Limitazione di responsabilità del segnalante

E' prevista l'assenza di responsabilità (anche di natura civile o amministrativa) per chi riveli o diffonda informazioni collegate ad una violazione:

- coperte dall'obbligo di segreto,
- relative alla tutela del diritto d'autore,
- delle disposizioni relative alla protezione dei dati personali,
- che offendono la reputazione della persona coinvolta o denunciata,

se, al momento della rivelazione o diffusione, vi fossero fondati motivi per ritenere che la rivelazione o diffusione delle stesse informazioni fosse necessaria per svelare la violazione e la segnalazione è stata effettuata in coerenza con le condizioni per la protezione.



Standard Operating Procedure

Inoltre, tra le misure di protezione, si evidenziano:

- i diritti a effettuare una segnalazione e le relative tutele non possono essere limitati in modo pattizio a livello contrattuale;
- l'esclusione di ogni altra responsabilità, anche civile e amministrativa, per l'acquisizione o l'accesso alle informazioni sulle violazioni, salva l'ipotesi in cui la condotta costituisca reato;
- l'esclusione di ogni altra responsabilità con riguardo a comportamenti, atti, omissioni posti in essere se collegati alla segnalazione e strettamente necessari a rivelare la violazione o, comunque, non collegate alla segnalazione.

5.14 Regime sanzionatorio

Il sistema disciplinare adottato dalla Società ai sensi dell'art. 6, comma 2, lettera e), del D. Lgs. 231/2001, e richiamato nella Parte Generale del Modello 231, prevede sanzioni da applicare nei confronti di coloro che la Società accerta essere responsabili degli illeciti riferiti a:

- commissione di ritorsioni o proposta di adozione, ostacolo alla segnalazione (anche tentato) o violazione degli obblighi di riservatezza,
- mancate istituzione dei canali di segnalazione, mandata adozione di procedure per la gestione delle stesse, ovvero procedure non conformi alle prescrizioni del decreto ovvero assenza di attività di verifica e analisi delle segnalazioni,
- responsabilità civile della persona segnalante, anche con sentenza di primo grado, per diffamazione o calunnia nei casi di dolo o colpa grave, salvo che la medesima sia stata già condannata, anche in primo grado, per i reati di diffamazione o di calunnia;

nonché nei confronti di chiunque violi la presente procedura.

Per gli stessi illeciti, ANAC può intervenire con l'applicazione di sanzioni amministrative pecuniarie (da € 500 fino a € 50.000) in caso di accertamento degli stessi illeciti.

6. ALLEGATI:

N/A

7. RIFERIMENTI:

- Decreto Legislativo 10 marzo 2023, n. 24;
- Direttiva (UE) 2019/1937;
- Codice di Condotta di Gruppo
- Modello di organizzazione, gestione e controllo ex D.Lgs. 231/01 e codice Etico;
- Regolamento Europeo 2016/679 (GDPR);
- Codice Privacy (D. Lgs. 196/2003 e ss.mm.ii.);



Standard Operating Procedure

- Linee guida ANAC in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne.
- KKI Regional Policy Speaking-Up (Whistleblowing) KK-QD-058101

8. **STORIA DELLA VERSIONE:**

Versione	Data di Approvazione	Descrizione delle Modifiche
1.0	Data della firma dell'Approvatore	Nuovo documento



Standard Operating Procedure

Titolo: Procedura Whistleblowing

KK-QD-105319

1. **OBJECTIVE:**

This procedure is adopted by the Company Kyowa Kirin S.r.l ("the Company") in compliance with the provisions of Legislative Decree no. 24 of 10 March 2023 (in the text: Decree or Legislative Decree 24/2023) in force since 30 March 2023 which implements Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, on the protection of persons who report violations of national or European Union regulatory provisions (so-called whistleblowing directive) of which they became aware in the context, detrimental to the public interest or the integrity of the public administration or private entity.

The procedure is also prepared in accordance with the KKI Regional Policy Speaking-Up (Whistleblowing) KK-QD-058101 and the behavioural protocols referred to in the Organizational Model adopted by the Company pursuant to Legislative Decree 231/2001.

This procedure was approved by the Board of Directors of the Company on March 25th, 2024, together with the identification of the organisational roles involved in the whistleblowing reporting management process and the related responsibilities.

2. **SCOPE:**

This procedure applies to any report of information on relevant unlawful conduct consisting of violations (actual or presumed) of the Group's Code of Conduct, of company procedures and policies, of the Organizational Model adopted pursuant to Legislative Decree 231/2001 and of applicable laws and regulations, acquired within the work context, carried out through the appropriate reporting channels made available by the Company.

The following are excluded from the scope of this procedure:

1. disputes, claims or requests related to a personal interest that relate exclusively to individual employment relationships, or to employment relationships with hierarchically superior figures;
2. violations of national security, as well as of procurement relating to defence or national security aspects;
3. infringements that are compulsorily regulated by European Union or national acts that already provide for appropriate reporting procedures.

3. **DEFINITION AND ABBREVIATIONS:**

3.1. Definitions

- **"Reports"** means any communication, whether written or oral, whether or not anonymous, containing information about violations;
- **"violations"**: violations of the Group's Code of Conduct, of company procedures and policies, of the Organizational Model adopted pursuant to Legislative Decree 231/2001, and of applicable laws or regulations;

CONFIDENTIAL

Pag. 1 di 28



Standard Operating Procedure

- **'information on violations'** means all information, including well-founded suspicions, concerning violations committed or which, on the basis of concrete evidence, could be committed in the organisation with which the reporting person has a legal relationship, as well as information on conduct aimed at concealing such violations;
- **"internal reporting"**: communication of "reports" through the internal reporting channel;
- **"whistleblower"**: a natural person who reports information on violations acquired in the context of his or her work context;
- **"facilitator"** means a natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
- **'work context'** means actual or past employment or professional activities through which, regardless of the nature of such activities, a person acquires information about violations and in the context of which he or she may risk retaliation in the event of a report or public disclosure or complaint to a judicial or accounting authority;
- **"Person Involved"** means a natural or legal person named in the report as a person to whom the infringement is attributed or as a person otherwise implicated in the reported infringement;
- **"channel manager"**: a subject identified by the Company responsible for managing the channel and the reporting with organisational and functional autonomy;
- **"internal contact person"**: Legal & Compliance Department; if the internal contact person is the person involved in the report, the role of internal contact person will be performed by the administrative body;
- **"retaliation"** means any behaviour, act or omission, even if only attempted or threatened, carried out as a result of the report and closely linked to the same, the complaint to the judicial or accounting authority or the public disclosure and which causes or may cause unjust damage to the reporting person or to the person who filed the complaint, directly or indirectly;
- **"follow-up"**: the action(s) initiated by the entity entrusted with the management of the reporting channel;
- **"response"** means communication to the reporting person of information relating to the follow-up that is given or intended to be given to the report, including the measures envisaged or adopted or to be adopted and the reasons for the choice made;
- **"platform"**: internal reporting channel adopted by the Company (as further specified at paragraph 5.3 and ff) to transmit information on violations;
- **"Supervisory Body ("SB")"**: Supervisory Body pursuant to D. Legislative Decree 231/2001 of Kyowa Kirin S.r.l.;
- **"Model 231"**: Organizational, management and control model pursuant to D. Legislative decree. 231/2001 of Kyowa Kirin S.r.l.

4. RESPONSABILITIES:

4.1 The Channel manager, also through the use of the platform:



Standard Operating Procedure

- makes available, also through this procedure and the information published on the platform, clear information on the channel, procedures and conditions for making internal reports;
- issues to the reporting person the acknowledgment of receipt of the report within the established deadlines;
- evaluates the criteria for the processability of the report;
- shares with the internal contact person, defined in the context of this procedure, and the SB (if applicable), the report, the initiation of any investigations, their outcome and the feedback to be provided to the whistleblower;
- transmits to the whistleblower the feedback on the closure of the report management process;
- maintains dialogue with the reporting person and, if necessary, manages the request for additions and the execution of any in-depth interviews with the reporting person, if requested;
- archives and maintains the documentation on the report within the time limits provided for by law;
- ensures compliance with the principle of confidentiality.

4.2 The internal contact person:

- identifies, within the Company, the subjects to be involved and shares with them what emerged from the analysis carried out by the channel manager;
- is delegated to provide the channel manager with feedback on the decisions taken by the Company for the in-depth analysis of what is the subject of the report;
- implements the recommendations made by the channel manager to investigate what is being reported;
- coordinates and monitors the phase of any investigations with the internal functions/external teams in charge;
- shares with the channel manager the launch of any investigations, their outcome and the feedback to be provided to the whistleblower;
- identifies improvement plans to avoid the recurrence of reported events;
- ensures that all the information required on the channel, procedures and assumptions for making internal reports is made available on the company channels;
- manages, with the support of the competent corporate departments, the activities resulting from any public disclosures in the cases envisaged;
- ensures compliance with the principle of confidentiality.

4.3 The whistleblower:

- submits the reports in accordance with this procedure;



Standard Operating Procedure

- is required to provide detailed information relating to what is being reported;
- indicates subjects for which protection can be requested (e.g. facilitators).

4.4 The SB:

- if the report relates to illicit conduct pursuant to Legislative Decree no. 231/2001, or violations of the Organizational Model, coordinates and monitors the investigation phase with the internal functions/external teams in charge, evaluates the outcome of the investigations and any consequent measures;
- ensures compliance with the principle of confidentiality.

4.5 The legal representative:

- liaises with ANAC in the event of the activation of inspection activities.

4.6 The Board of Directors:

- approves this procedure together with the structure of the related organisational roles;
- ensures compliance with the measures for the protection of the reporting person.
- ensures that any measures are taken in accordance with the provisions of the sanctioning system provided for in the 231/2001 Organisational Model, if applicable.

5. **PROCEDURE**

5.1 **Subjects who can make a report (so-called "whistleblower")**

The following can make a report:

- employees;
- self-employed workers and collaborators who carry out their activities in public and private entities;
- freelancers;
- volunteers;
- consultants;
- shareholders;
- Administrators;
- providers of services to third parties for any reason (regardless of the nature of such activities) even in the absence of consideration;
- trainees, even if not paid;
- persons who exercise administrative, managerial, control, supervisory or representative functions, even if the related activities are carried out in fact and not in law.
- The category in question also includes all those persons who, for any reason, become aware of offences within the Company's working context, namely:
 - o when the employment relationship has not yet begun;
 - o during the probation period;



Standard Operating Procedure

- o upon the termination of the relationship.

5.2. Internal contact person

The Company has identified the members of the company's Legal & Compliance Department as the internal contact person pursuant to this procedure.

5.3. Internal Reporting Channel

The Company has provided an internal reporting channel that the whistleblower must use for the transmission of information on violations. The establishment of such a channel allows for more effective prevention and detection of violations. This choice responds to the principle of fostering a culture of good communication and corporate social responsibility as well as improving one's own organization.

The internal reporting channel is represented by the "KKI Speak-up line" accessible through the Speak Up section on the company intranet page dedicated to Compliance, at the link <https://secure.ethicspoint.eu/domain/media/en/gui/105727/index.html>.

The internal reporting channel guarantees the confidentiality of the identity of the whistleblower, the facilitator (if any), the persons involved and, in any case, mentioned in the report as well as the content of the report and the related documentation forwarded or integrated.

The channel can also be used by third parties external to the Company, by accessing the website.

5.4 Person responsible for the management of the channel (so-called "channel manager")

The management of the internal channel is entrusted to the HQ Regional Compliance team, whose members meet the requirements of autonomy, independence and are specifically trained.

5.5 Characteristics of the internal reporting channel

The Company's internal reporting channel "Speak-up line" is managed from an external vendor and allows employees to report via a web portal or by telephone. The system allows anonymous reporting, as well as the possibility of interacting directly with the Reporter, anonymously.

The processing of personal data must always take into account and comply with the obligations set out in the GDPR and Legislative Decree 196/2003 and subsequent amendments. The Company, as data controller through the internal reporting channel, is required to carry out a prior analysis of the



Standard Operating Procedure

organizational design, including the fundamental assessment of the possible impact on data protection (Article 35 of the GDPR).

5.6 Characteristics of reporting and anonymous reporting

It is necessary that the report is as detailed as possible in order to allow the analysis of the facts by the parties competent to receive and manage the reports. In particular, it is necessary that are clear:

- the circumstances of time and place in which the event that is the subject of the report occurred;
- a description of the fact;
- personal details or other elements that make it possible to identify the person to whom the reported facts can be attributed.

Information about reported violations must be truthful. Such simple assumptions, unreliable rumors (so-called rumors), as well as news in the public domain, incorrect information (with the exception of genuine error), manifestly unfounded or misleading or if merely harmful or offensive, are not considered. On the other hand, it is not necessary for the whistleblower to be certain of the actual occurrence of the reported facts and the identity of the perpetrator of the same.

It is also useful for the whistleblower to provide documents that can give evidence of the facts being reported, as well as the indication of other persons potentially aware of the facts.

Anonymous reports, where substantiated, are equated to ordinary reports and in this case considered in the context of this procedure also with reference to the protection of the whistleblower, if subsequently identified, and to the retention obligations.

5.7 Operational process for the management of the report

The whistleblower transmits the report through the dedicated internal channel.

The whistleblower activates the report through the link indicated above in written form, by filling out a guided form. If the reporter prefers to make a report orally, he or she can request a meeting with his or her Line Manager or with the internal contact person or with the HR Director. In the case of a face-to-face meeting, it has to be guaranteed that the meeting takes place within a reasonable time (10-15 days), preferring that the hearing takes place in premises other than the company premises.

If the whistleblower makes the report orally through a meeting scheduled with the channel manager, the same, with the consent of the whistleblower himself, is documented by the Line Manager/internal contact person/HR Director with the recording on a device suitable for storage and voice reproduction or through



Standard Operating Procedure

the drafting of a report. In the latter case, the whistleblower may verify, rectify and/or confirm the minutes of the meeting by signing it.

With the receipt of the report by the channel manager, the process of managing the reports starts. The channel manager proceeds then to "process" it.

Upon receipt of the report, the channel manager communicates an acknowledgement of receipt to the whistleblower within 7 days of receipt of the report and taking charge of the report.

The channel manager proceeds with an initial verification of the content of the report also with reference to its verifiability based on the information provided. The channel manager promptly informs the internal contact person, ensuring compliance with the principle of confidentiality, who shares the information with the Company.

If it is necessary to acquire additional elements, the channel manager will contact the whistleblower via the platform. If the whistleblower does not provide, within 3 months of the request for integration, additional information, the channel manager proceeds with the archiving of the report, notifying the whistleblower and informing the internal contact person.

If the report concerns illicit conduct pursuant to Legislative Decree no. 231/2001, or violations of the Organizational Model, the internal contact person informs, in compliance with the principle of confidentiality, the Supervisory Body in order to assess the method of starting the investigation phase, without prejudice to compliance with the principle of autonomy and independence of the SB with respect to the way in which to manage the report for the purposes and for the purposes of Legislative Decree 231/01.

At the end of the investigation, the internal contact person prepares a final report and shares the results the channel manager and the Supervisory Body if applicable, in order to proceed with the feedback to the whistleblower. The response to the whistleblower must be sent by the channel manager within three months from the date of acknowledgment of receipt or, in the absence of such acknowledgment, from the expiry of the period of seven days from the submission of the report. Only in exceptional cases, if the complexity of the report requires it, or in consideration of the whistleblower's response time, the channel manager, having promptly informed the whistleblower before the deadline, with appropriate motivation, may continue the investigation phase for the necessary time and giving the whistleblower periodic updates.

If applicable, the SB, within the scope of its operational autonomy, assesses the outcome received and, if the report is well-founded, any consequent measures, evaluating the adoption of any measures deemed necessary for the purpose of adapting the Model, initiating the communications necessary for the application of any sanctions. Any consequent measures are applied in accordance with the provisions of the sanctioning system provided for in the 231 Organizational Model.



Standard Operating Procedure

In the event of defamation or slander, ascertained with a conviction also in the first instance, the Company proceeds with sanctioning proceedings against the whistleblower.

It is specified that, from the receipt of the report until its closure, any person who finds himself in a situation of conflict of interest must refrain from taking decisions in order to ensure compliance with the principle of impartiality.

5.8 Transmission of reports with the wrong recipient

If the report is transmitted to a person other than the person responsible for receiving it, the recipient shall be obliged to transmit it within seven days to the competent entity by giving notice of the transmission to the reporting person and ensuring a management of the information in accordance with the confidentiality obligations. The Company adopts disciplinary sanctions in the event of non-compliance with the obligation to transmit.

In the event of involuntary transmission of the report to a person other than the person entitled to receive it, the whistleblower must demonstrate mere negligence and the absence of a personal interest in the erroneous transmission.

5.9 Keeping records of internal reporting

Internal reports and all related attached or integrated documentation are stored, by the channel manager and by the internal contact person, taking care of confidentiality, for the time necessary to process the report itself.

In any case, the documentation shall be kept only for a maximum period of five years from the date of communication of the final outcome of the reporting procedure.

In all the cases mentioned, it is necessary that the procedure for storing internal reports and related documentation complies with EU and national guarantees on the processing of personal data as well as with the measures in place on the right to confidentiality.

5.10 Information obligation

Information on the channel, procedures and requirements for reporting are available in the specific Speak Up section on the company intranet page dedicated to Compliance, within Veeva Quality, a certified system



Standard Operating Procedure

dedicated to recording procedures and their training and within the common folders. In addition, this information is published on the Company's website to be available to third parties.

The Company has also provided information on this procedure to the trade unions.

5.11 Duty of confidentiality

All reports and their attachments shall not be used beyond the time necessary to follow them up.

It is envisaged that the identity of the whistleblower together with any other information from which such identity can be deduced, directly or indirectly, shall not be revealed without the express consent of the whistleblower to persons other than those competent to receive or follow up on the reports, expressly authorised to process such data pursuant to art. 29 and 32, paragraph 4 of Regulation (EU) 2016/679 and art. 2-quaterdecies of the code regarding the protection of personal data pursuant to Legislative Decree no. 196 of 30 June 2003.

The Company protects the identity of the persons involved, the facilitators and the persons mentioned in the report until the conclusion of the proceedings initiated by reason of the report itself, in compliance with the same guarantees provided for the reporting person.

Circumstances that mitigate the protection of the right to privacy include:

- In the context of criminal proceedings, the identity of the whistleblower is covered by secrecy in the manner and within the limits provided for by Article 329 of the Code of Criminal Procedure: the obligation of secrecy of the acts of the preliminary investigations is imposed until the suspect has the right to know them and, in any case, no later than the end of this phase;
- in the context of the procedure established at the Court of Auditors, the identity of the whistleblower cannot be revealed until the conclusion of the investigation phase;
- in the context of disciplinary proceedings, the identity of the whistleblower cannot be revealed if the objection to the disciplinary charge is based on separate and additional investigations with respect to the report, even if they are consequent to the same;
- if the complaint is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defence of the accused, the report will be used for the purposes of disciplinary proceedings only in the presence of the whistleblower's express consent to reveal his or her identity;
- In cases of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, the whistleblower will be notified in writing of the reasons for the disclosure of confidential data when the disclosure will also be indispensable for the purposes of defending the person involved.



Standard Operating Procedure

Given the validity of the mitigations listed above, the party involved, at his request, is also heard through a paper-based procedure through the acquisition of written observations and documents.

Confidentiality obligations include:

- the removal of the report and the documentation attached to it from the right of access to administrative documents provided for by art. 22 et seq. of Law no. 241/1990 and generalized civic access pursuant to art. 5 et seq. of Legislative Decree no. No 33/2013;
- The administrations and bodies involved in the management of reports guarantee confidentiality during all phases of the reporting process, including the possible transfer of reports to other competent authorities.

5.12 Protection of personal data

Any processing of personal data, including communication between competent authorities, shall be carried out in accordance with:

- Regulation (EU) 2016/679;
- Legislative Decree no. 196 of 30 June 2003 and subsequent amendments.

The communication of personal data by institutions, bodies, offices or agencies of the European Union is carried out in accordance with Regulation (EU) 2018/1725.

The processing of personal data relating to the channel manager is carried out by the Data Controller, in compliance with the principles set forth in art. 5 and 25 of Regulation (EU) 2016/679, providing the appropriate information in advance to reporting entities and persons involved and adopting appropriate measures to protect the rights and freedoms of data subjects.

The information to the data subjects, also summarizing their rights and how to exercise them, can be found on the Company website.

5.13 Protective and support measures

Appropriate measures shall be in place to protect whistleblowers from direct and indirect retaliation.

The safeguards apply if, at the time of the report, the reporting person had reasonable grounds to believe that the information on the reported breaches was true, fell within the objective scope and the reporting procedure was complied with.

In the event of defamation or slander, ascertained by conviction even in the first instance, the protections are not guaranteed.

The protective measures also apply to:

- (a) facilitators;



Standard Operating Procedure

b) to persons in the same working context as the reporting person who are linked to them by a stable emotional or family bond within the fourth degree;

(c) to the reporting person's work colleagues who work in the same working environment as the reporting person and who have a habitual and ongoing relationship with that person;

d) entities owned by the reporting person/complainant or for which the same persons work, as well as entities operating in the same working environment as the aforementioned persons.

5.13.1 Prohibition of retaliation

The persons listed in paragraph 5.1 may not be subject to any retaliation. For information and non-exhaustive reasons, the following are considered "retaliations":

- dismissal, suspension or equivalent measures;
- relegation or non-promotion;
- change of functions;
- the change of workplace;
- salary reduction;
- the modification of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references that are not adequately substantiated;
- the adoption of disciplinary measures or other sanctions (including pecuniary sanctions);
- coercion;
- intimidation;
- harassment;
- ostracism;
- discrimination or unjustified unfavourable treatment;
- the failure to convert a fixed-term employment contract into an employment contract of indefinite duration where the worker had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, in particular on social media,
- economic or financial harm, including loss of economic opportunities and loss of income;
- improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person not being able to find employment in the sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the cancellation of a licence or permit;
- the request to undergo psychiatric or medical examinations.

Acts taken in violation of the prohibition of retaliation shall be null and void.

In the context of judicial or administrative proceedings or in the event of out-of-court disputes concerning the ascertainment of prohibited conduct, acts or omissions only with regard to reporting parties, it is presumed that they have been carried out as a result of the report. The burden of proving that such conduct or acts are motivated by reasons unrelated to the report lies with the person who carried out the retaliatory acts.

Whistleblowers can notify ANAC of the retaliation they believe they have suffered, whether attempted or proposed.



Standard Operating Procedure

ANAC informs the National Labour Inspectorate for the measures within its competence.

5.13.2 Support measures

The whistleblower may contact Third Sector entities on the list published on the ANAC website. These are entities that carry out activities of general interest for the pursuit, on a non-profit basis, of civic, solidarity and socially useful purposes ("promotion of the culture of legality, peace among peoples, nonviolence and unarmed defense; promotion and protection of human, civil, social and political rights, as well as the rights of consumers and users of activities of general interest, promotion of equal opportunities and mutual aid initiatives, including time banks and solidarity purchasing groups") and which have entered into agreements with ANAC.

The support measures provided consist of information, assistance and advice free of charge on how to report and on the protection from retaliation offered by national and EU legal provisions, on the rights of the person concerned, as well as on the terms and conditions of access to legal aid.

5.13.3 Limitation of Whistleblower Liability

There is no liability (including civil or administrative liability) for those who reveal or disseminate information related to a violation, if their disclosure or dissemination was necessary to reveal the violation:

- covered by the obligation of secrecy,
- relating to the protection of copyright,
- the provisions relating to the protection of personal data,
- that offend the reputation of the person involved or charged,

if, at the time of disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to uncover the breach and the report was made in accordance with the conditions for protection.

In addition, among the protection measures, the following are highlighted:

- the rights to report and the associated safeguards cannot be contractually restricted;
- the exclusion of any other liability, including civil and administrative liability, for the acquisition of or access to information on violations, except in the event that the conduct constitutes a crime;
- the exclusion of any other liability with regard to conduct, acts, omissions put in place if related to the report and strictly necessary to reveal the violation or, in any case, not related to the report.



Standard Operating Procedure

5.14 Sanctioning regime

The disciplinary system adopted by the Company pursuant to art. 6, paragraph 2, letter e) of Legislative Decree no. 231/2001, and referred to in the General Part of Model 231, provides for sanctions to be applied to those whom the Company ascertains to be responsible for offences relating to:

- retaliation committee or proposed adoption, obstruction of reporting (even attempted) or breach of confidentiality obligations,
- failure to establish reporting channels, adoption of procedures for the management of the same, or procedures that do not comply with the requirements of the decree or absence of verification and analysis of reports,
- civil liability of the reporting person, even with a judgment of first instance, for defamation or slander in cases of wilful misconduct or gross negligence, unless the same has already been convicted, even in the first instance, for the crimes of defamation or slander;

as well as against anyone who violates this procedure.

For the same offences, ANAC may intervene with the application of administrative fines (from € 500 up to € 50,000) in the event of ascertainment of the same offences.

6. **ANNEXES:**

N/A

7. **RIFERENCES:**

- Legislative Decree no. 24 of 10 March 2023;
- Directive (EU) 2019/1937;
- Group Code of Conduct
- Organization, management and control model pursuant to Legislative Decree 231/01 and Code of Ethics;
- European Regulation 2016/679 (GDPR);
- Privacy Code (Legislative Decree 196/2003 and subsequent amendments);
- ANAC Guidelines on the protection of persons reporting breaches of Union law and protection of persons reporting breaches of national regulatory provisions – procedures for the submission and management of external reports.
- KKI Regional Policy Speaking-Up (Whistleblowing) KK-QD-058101

8. **HISTORY:**



Standard Operating Procedure

Version	Date of Approval	Descriptions of the changes
1.0	Date of the Approver signature	New document

Document Approvals
Approved Date: 26 Mar 2024

Final Approval Task Verdict: Approve	Claudia Coscia, (Claudia.coscia@kyowakirin.com) Document Approver 26-Mar-2024 11:17:57 GMT+0000
---	--