POLICY PER LA PREVENZIONE DI FRODI E VIOLAZIONI AL CODICE ETICO E PER LA GESTIONE DELLE SEGNALAZIONI IN MATERIA DI "*WHISTLEBLOWING*"

Società:
Esprinet S.p.A., V-Valley S.r.l., Dacom S.p.A.

Sede:
Tutte le sedi

Sottosistema:
D.Lgs. 231/01, Regolamento 2016/679, D.Lgs. 24/23

Nome file:
DIS01001 *Policy* per la prevenzione di frodi e violazioni al Codice Etico e per la gestione delle segnalazioni in materia di *"Whistleblowing"*

Responsabilità per Il documento:

Rev.	Data	Nota di Revisione	Redatto	Controllato	Approvato
00	01/03/16	Prima emissione	P.Aglianò CRO	G.Monina RIA	A.Cattani AD
01	15/10/18	Aggiornamento Whistleblowing	P.Aglianò CRO	G.Monina RIA	A.Cattani AD
02	29/06/21	Aggiornamento	P.Aglianò CRO	G.Monina RIA	A.Cattani AD
03	16/03/22	Estensione a V-Valley Advanced Solutions España	P.Aglianò CRO	G.Monina RIA	A.Cattani AD
04	08/06/22	Estensione a Dacom S.p.A.	P.Aglianò CRO	G.Monina RIA	A.Cattani AD
05	03/07/23	Aggiornamento del documento finalizzato a recepire le novità normative introdotte dal D.Lgs. 24/2023	P.Aglianò CRO	G.Monina RIA	A.Cattani AD

INDICE

1. SCOPO ED AMBITO DI APPLICAZIONE

La presente *policy* riassume i principi dettati dalla Società allo scopo di prevenire e contrastare efficacemente comportamenti fraudolenti e illegittimi e comunque contrari al Codice Etico, al Modello Organizzativo ex D.Lgs. 231/01, alle leggi ed ai Regolamenti, da parte di tutti i dipendenti delle società italiane del Gruppo Esprinet.
Inoltre, la presente *policy* ha ad oggetto le segnalazioni, di comportamenti che ledono l'interesse pubblico o l'integrità dell'ente privato, relative a:

- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al D.Lgs. 24/2023;
- atti od omissioni che ledono gli interessi finanziari dell'Unione o il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei suddetti settori.

La rigorosa applicazione di tali principi non può prescindere dalla sentita partecipazione di tutti e a tutti i livelli nel presupposto che il controllo interno possa avere efficacia solo attraverso il contributo di tutte le funzioni aziendali, di tutti i dipendenti e collaboratori, oltre che delle funzioni di controllo e di supporto.
Il suo contenuto si ispira alle principali *best practices* internazionali in materia di controllo interno, primo tra tutti, il sistema CoSo-ERM.
La presente procedura controlla il comportamento dei destinatari, come di seguito definiti, al fine di prevenire la commissione di illeciti e atti come sopra indicati o di uno o più reati previsti dal D.Lgs. 231/01 e dal Codice Penale e di rispettare la normativa in materia di protezione dei dati personali. In particolare, questa procedura ha lo scopo di:

- identificare i compiti e le responsabilità della direzione/dei dipartimenti/unità organizzative coinvolti;
- regolare e identificare la tracciabilità dei controlli effettuati;
- minimizzare il rischio di commettere reati ai sensi del D.Lgs. 231/01 e del Codice Penale;
- garantire il rispetto della normativa vigente e del sistema di procedure aziendali;
- rispettare il principio della privacy *by default* e *by design* previsto dal Regolamento (UE) 2016/679 del 17 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati;
- garantire il rispetto del principio di riservatezza, integrità, disponibilità e tracciabilità delle informazioni.

2. DESTINATARI

La presente *policy* si applica a tutti i *i)* lavoratori subordinati, lavoratori autonomi e collaboratori che svolgono la propria attività presso (non per forza per conto) le società italiane del Gruppo Esprinet, *ii)* volontari e tirocinanti, retribuiti e non retribuiti, *iii)* liberi professionisti e consulenti che svolgono la loro attività presso (non per forza per conto) le società italiane del Gruppo Esprinet, *iv)* azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto delle società italiane del Gruppo Esprinet.

Sarà cura e dovere di ogni responsabile di funzioni divulgarne i principi anche tra fornitori, consulenti e collaboratori occasionali.

La tutela delle persone segnalanti si applica anche qualora la segnalazione avvenga nei seguenti casi:

- quando il rapporto giuridico (ad es. rapporto di lavoro subordinato, di collaborazione, di consulenza, di fornitura etc.) non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- durante il periodo di prova:
- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

3. TERMINI E DEFINIZIONI

ABUSO	Qualunque condotta che produca o che sia potenzialmente atta a produrre un danno all'azienda, con altrui vantaggio o profitto diretto o indiretto, caratterizzata dall'uso distorto della fiducia accordata e dall'elusione di norme aziendali.
COSO ERM	Il COSO ERM è definito come un processo posto in essere dal Vertice aziendale, finalizzato ad identificare quei fattori potenziali che possono esercitare un'influenza rilevante sull'organizzazione, a gestire il rischio entro i livelli "appetiti" dall'organizzazione e a fornire ragionevole garanzia riguardo il conseguimento degli obiettivi aziendali.
DIVULGAZIONE PUBBLICA	Rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.
ENTE GESTORE DELLA SEGNALAZIONE	La gestione e la verifica della fondatezza delle circostanze rappresentate nella segnalazione sono affidate al RIA e al Presidente/Componente monocratico dell'Organismo di Vigilanza, che vi provvedono nel rispetto dei principi di imparzialità e riservatezza, effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati, con l'adozione delle necessarie cautele.
FACILITATORE	Persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.
FATTORE DI RISCHIO	Elemento che può determinare un innalzamento della probabilità di diffusione di comportamenti fraudolenti ed infedeli che agisce su una delle componenti del triangolo della frode.
FRAUD RISK ASSESSMENT	È la valutazione dei rischi di frode che permette non solo di determinare «cosa» potrebbe causare una frode ed il suo impatto sulla società, ma di capire l'efficacia delle misure.
FRODE	Qualunque evento derivante da una condotta umana, caratterizzata dalla *fraudolenza,* ossia da una falsa rappresentazione della realtà, ovvero dall'uso distorto della fiducia accordata o dall'elusione di norme aziendali che cagioni o che sia potenzialmente atto a cagionare un danno all'azienda, finalizzato al conseguimento di un vantaggio o profitto diretto o indiretto per l'autore o per altri.
FRODE ESTERNA	Frode ai danni delle società del Gruppo Esprinet, commessa da soggetti esterni all'organizzazione (clienti, fornitori, terzi).
FRODE INTERNA	Frode ai danni delle società del Gruppo Esprinet, commessa da soggetti interni all'organizzazione (dipendenti).
FRODE MISTA	Frode ai danni di un'azienda, commessa grazie alla complicità tra soggetti esterni ed interni ad Esprinet (es. accordo tra Ufficio Acquisti e fornitori).
INDICATORE DI RISCHIO	Elemento la cui variazione è sintomatica di un innalzamento del livello di rischio (es. aumento delle operazioni «fuori procedura»).
INDICATORI DI ANOMALIA	Segnale di una potenziale frode che richiede approfondimento. (es. rimborsi spese anomali, consumi anomali di carburante etc.….).
KPI ANTIFRODE	Indicatore di *performance* riferito ad uno o più controlli antifrode (es. diminuzione delle differenze inventariali).
PERSONA COINVOLTA	Persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.
RED FLAG	Indicatori rilevanti di potenziali frodi o abusi, che costituiscono spunti per l'avvio di una verifica.
RITORSIONE	Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità

	giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare al segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto. A titolo esemplificativo, sono forme di ritorsione: • il licenziamento o la sospensione; • 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; • l'imposizione o amministrazione di misure disciplinari, la nota di biasimo o altra sanzione, anche pecuniaria; • la coercizione, l'intimidazione, le molestie o l'ostracismo; • il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; • la discriminazione, il trattamento svantaggioso o iniquo; • la pretesa di risultati impossibili da raggiungere nei modi e nei tempi indicati; • una valutazione della *performance* artatamente negativa; • una revoca ingiustificata di incarichi; • un ingiustificato mancato conferimento di incarichi con contestuale attribuzione ad altro soggetto; • il reiterato rigetto di richieste (ad es. ferie, congedi); • la sospensione ingiustificata di brevetti, licenze, etc.
SEGNALANTE/I	Soggetto che effettua una segnalazione o una divulgazione pubblica, appartenente ad una delle seguenti categorie: • lavoratori dipendenti del Gruppo Esprinet e coloro che operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato; • azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza membri degli Organi sociali del Gruppo Esprinet; • lavoratori non dipendenti (es. liberi professionisti e consulenti) che forniscono beni o servizi a favore del Gruppo Esprinet.
VIOLAZIONE/ ILLECITI	Comportamento riconducibile a: • illeciti rilevanti ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, o inadempimento dei modelli di organizzazione e gestione; • illeciti che rientrano nell'ambito del diritto dell'Unione, relativamente a specifici settori (a titolo esemplificativo: servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; tutela dell'ambiente; tutela della vita privata e protezione dei dati personali; sicurezza delle reti e dei sistemi informativi); • atti od omissioni che ledono gli interessi finanziari dell'Unione Europea; • atti od omissioni riguardanti (art. 26 par 2 TFUE) la libera circolazione delle merci, delle persone, dei servizi e dei capitali nel mercato interno, comprese violazioni delle norme dell'Unione Europea in materia di concorrenza; aiuti di Stato; imposte sulle società; • atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea.
WHISTLEBLOWING	Sistema di segnalazioni mediante il quale il lavoratore che, durante l'attività lavorativa all'interno di un'azienda, rileva una possibile frode, una violazione, un illecito, una irregolarità, un pericolo o un altro serio rischio che possa danneggiare clienti, colleghi, azionisti, il pubblico o la stessa integrità e reputazione dell'impresa/ente pubblico/fondazione, decide di effettuare la segnalazione.
Per le definizioni che seguono si veda anche la "relazione sul governo societario e gli assetti proprietari" ai sensi dell'art.123-bis TUF disponibile per la consultazione sul sito istituzionale Esprinet – *Area Investor Relations*	
CCR	Comitato Controllo e Rischi

CdA	Consiglio di Amministrazione
AD	Amministratore Delegato
AI	Amministratore Incaricato del sistema di controllo interno
ANAC	Autorità Italiana Anti Corruzione
RIA	Responsabile *Internal Audit*
CdS	Collegio Sindacale
CRO	*Risk Manager*
SCIGR	Acronimo di Sistema di Controllo Interno e di Gestione dei Rischi. Esso è definito come l'insieme di regole, comportamenti, politiche, procedure e strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione ed il monitoraggio dei principali rischi gestionali contribuendo ad assicurare la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità dell'informazione finanziaria, il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne.
O.d.V.	Organismo di Vigilanza

4. AZIONI COSTITUENTI UNA FRODE

Per condotte fraudolente e comportamenti contrari al Codice Etico devono intendersi tutte quelle azioni intenzionali poste in essere in aggiramento di norme aziendali o abusando della fiducia accordata, finalizzate all'ottenimento di un ingiusto vantaggio. La frode è definita come la falsa rappresentazione di un fatto materiale (o dell'uso distorto della fiducia accordata) per procurare, direttamente o indirettamente, un vantaggio al soggetto agente o ad un terzo.

A titolo esemplificativo e non esaustivo, integrano una frode aziendale le seguenti attività illecite:

- furto di beni di proprietà del Gruppo Esprinet;
- falsificazione o alterazione di documenti;
- falsificazione o manipolazione dei conti ed omissione intenzionale di registrazioni, eventi o dati;
- distruzione, occultamento o uso inappropriato di documenti, archivi, mobili, installazioni e attrezzature;
- appropriazione indebita di denaro, valori, forniture o altri beni appartenenti al Gruppo Esprinet;
- dazione di una somma di danaro o concessione di altra utilità ad un pubblico ufficiale come contropartita di un atto di ufficio (es. snellimento di pratiche doganali) o dell'omissione di un atto di ufficio (es. mancata elevazione di un verbale di contestazione per irregolarità fiscali);
- accettazione di danaro, beni, servizi o altro beneficio come incentivi per favorire fornitori/aziende;
- falsificazione di note spese (es. rimborsi "gonfiati" o per false trasferte);
- falsificazione delle presenze a lavoro;
- rivelazione di informazioni confidenziali e di proprietà del Gruppo Esprinet a parti esterne (es. *competitor*);
- utilizzo delle risorse e dei beni dell'organizzazione per uso personale, senza autorizzazione.

5. RIFERIMENTI

LEGGI E REGOLAMENTI	D.lgs. n. 231/01
	D.Lgs. n. 196/2003
	D.Lgs. n. 151/2015
	CCNL Commercio
	Legge n. 300/1970 (Statuto dei Lavoratori)
	GDPR (Regolamento 2016/679 del 17 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trasferimento dei dati personali, nonché alla libera circolazione di tali dati).
	Codice etico
	D.Lgs. 24/2023
PROCEDURE E DOCUMENTI INTERNI	Sistema disciplinare interno
	Modello "231" adottato dal Gruppo Esprinet Italia
	Disciplinare Interno Utilizzo Strumenti Informatici
	Procedura Omaggi Merce
	Procedura per la gestione ed approvazione delle Operazioni con Parti Correlate
	Gestione Omaggi, Liberalità e Sponsorizzazioni
	Gestione delle Visite Ispettive
	Procedura di Gestione Sistemi di Rilevazione Immagine Gruppo Esprinet
	Procedura nota spese
	Linee di indirizzo per il Sistema di Controllo Interno e di Gestione dei Rischi
	Procedura in tema di acquisizione e gestione Gare
	Mansionario Incarichi *Privacy* Gruppo Esprinet
	Regolamento Interno di *Internal Dealing*
	Regolamento Interno Informazioni Privilegiate

6. RUOLI E RESPONSABILITÀ

6.1. AMMINISTRATORI DELEGATI

Gli Amministratori Delegati (o le funzioni corrispondenti nelle diverse società italiane del Gruppo) conferiscono ampio *committment* alle funzioni operative delegate alla gestione del sistema di prevenzione frodi e alla verifica di segnalazioni di casi sospetti e prendono atto delle attività svolte, delle misure implementate e dei casi accertati nelle relazioni semestrali redatte dal RIA.

Inoltre:

- vengono tempestivamente informati dall'Organismo di Vigilanza nei casi di maggior gravità che coinvolgano alti dirigenti, membri dell'Organo di Controllo o gli altri componenti dell'Organismo di Vigilanza o che comunque possano determinare impatti gravi o riguardare la corretta gestione dell'azienda;
- assumono provvedimenti nei casi di cui al punto precedente.

6.2. CHIEF RISK OFFICER

Il CRO definisce le linee guida della presente *policy*, individuando i rischi di frode in fase di *fraud risk assessment*, con gli altri rischi operativi, di *compliance* e connessi al *financial report*, e presenta la stessa ed eventuali aggiornamenti o modifiche al Comitato Controllo e Rischi.

Particolare attenzione dovrà essere posta alla valutazione degli impatti fiscali di fatti di frode.

Inoltre, verifica la coerenza dei criteri specifici di valutazione dei rischi di frode rispetto alle più generali metodologie di analisi del rischio ed alla propensione al rischio dell'azienda (RAF – *Risk Appetite Framework*).

6.3. COMITATO CONTROLLO E RISCHI

Il CCR esamina la *policy* presentata dal CRO e propone eventuali modifiche e integrazioni della stessa. Prende inoltre atto delle attività svolte, delle misure implementate e dei casi accertati nel corso delle riunioni del comitato a cui è chiamato a partecipare il RIA.

Relativamente ai casi di segnalazioni di fatti rilevanti in materia di *Whistleblowing*, il CCR viene tempestivamente informato dall'Organismo di Vigilanza nelle ipotesi di maggior gravità che coinvolgano alti dirigenti, membri dell'Organo di Controllo o gli altri componenti dell'Organismo di Vigilanza o che comunque possano determinare impatti gravi o riguardare la corretta gestione dell'azienda.

6.4. INTERNAL AUDIT

L'*Internal Audit*:

- esegue gli approfondimenti sulle segnalazioni;
- se durante lo svolgimento delle attività di audit viene a conoscenza di presunte frodi o violazioni al Codice Etico, provvede alla loro valutazione preliminare ed alla loro comunicazione all'Organismo di Vigilanza.
- Integra la propria relazione periodica al Consiglio di Amministrazione con l'andamento del sistema di prevenzione frodi e con le eventuali misure intraprese.

6.5. RISORSE UMANE

Il Responsabile delle Risorse Umane:

- procede senza indugio alla elaborazione della contestazione disciplinare ed alla istruzione del relativo procedimento in caso di ricezione da parte dell'Organismo di Vigilanza, e degli Amministratori Delegati di evidenze circa fatti rilevanti disciplinarmente a carico di un dipendente. Nel caso di fatti penalmente rilevanti ai quali sia seguita la presentazione di una denuncia o una querela, e non si configurino autonome violazioni disciplinari, procede alla contestazione immediata, valutando caso per caso se sospendere o meno il procedimento disciplinare sino a definizione di quello penale.

6.6. UFFICIO LEGALE

Il Legale interno:

- esprime valutazioni circa la configurabilità penale di quanto emerso in fase di esame ed approfondimento di segnalazioni di presunte frodi o violazioni al Modello Organizzativo o al Codice Etico, verificando, avvalendosi di legali esterni, se trattasi di reato perseguibile d'ufficio o a querela di parte. In quest'ultima ipotesi, sottopone alla firma dell'Amministratore Delegato eventuali formali querele e provvede al loro deposito presso organi di Polizia Giudiziaria o presso competenti Uffici Giudiziari a mezzo di legali esterni.

6.7. RESPONSABILI DI FUNZIONE

I Responsabili di Funzione rappresentano il controllo di primo livello e devono costantemente ricordare che con il loro esempio possono contribuire efficacemente alla diffusione di comportamenti virtuosi e rispettosi dei valori e delle regole aziendali, in relazione ai quali non mancheranno di sensibilizzare i propri collaboratori ad ogni favorevole occasione.

Essi sono tenuti:

- a comunicare all'O.d.V. qualunque sospetta violazione del Modello Organizzativo o del Codice Etico, alle regole e procedure aziendali o comportamenti che possano configurare frodi e illeciti, intervenendo tempestivamente per impedire il protrarsi di condotte dannose per l'azienda e, se tali condotte rientrano nell'ambito di applicazione di violazioni/illeciti, a formalizzare tale segnalazione tramite i canali *whistleblowing* di seguito indicati;
- a mantenere riservata l'identità del collaboratore che dovesse segnalare loro alcuno dei fatti di cui al punto precedente;
- ad evitare comportamenti discriminatori o vessatori nei confronti di coloro che dovessero segnalare fatti di cui ai punti precedenti;
- a comunicare tempestivamente situazioni di conflitto di interesse personali o di propri collaboratori, ivi comprese quelle riguardanti i propri familiari, astenendosi dall'assumere decisioni o dall'intervenire in ogni caso in processi decisionali che possano integrare tali situazioni;
- a non utilizzare informazioni aziendali per fini privati;

- ad assumere comportamenti equi ed imparziali;
- a ripartire equamente il carico di lavoro tra i propri collaboratori, sulla base delle capacità, delle attitudini, della professionalità e nel rispetto delle mansioni;
- ad esprimere valutazioni imparziali sul personale;
- a diffondere la coscienza di buone prassi e buoni esempi, rafforzando il senso di fiducia e di appartenenza nei confronti dell'azienda.

7. VALUTAZIONE DEL RISCHIO

Il rischio di frode e di comportamenti contrari al Codice Etico è di natura trasversale, in quanto può avere impatti oltre che su perdite patrimoniali anche sull'immagine aziendale e sulla fisiologica conduzione delle operazioni.

Per un'efficace valutazione del rischio, pertanto, si dovrà tener conto:

- del danno diretto (valore materiale del bene aziendale colpito e/o sanzione in caso di implicazione legale dell'azienda), del danno indiretto (costo delle misure necessarie per il ripristino della normale operatività – *business as usual*) e del danno consequenziale (danno di immagine o reputazionale con potenziali ricadute su perdita di quote di mercato);
- dell'analisi di casi verificatisi in altre realtà aziendali (*fraud business case*) e di cui si sia presa conoscenza attraverso i *media*.

I Responsabili di Funzione dovranno contribuire ad un'efficace analisi e valutazione del rischio attraverso un comportamento di aperta e leale collaborazione nei confronti del Presidente/Componente monocratico dell'O.d.V. e del RIA, mettendo a disposizione i dati e le informazioni necessari e la loro più approfondita conoscenza dei processi aziendali.

8. SEGNALAZIONI WHISTLEBLOWING

Per *whistleblowing* si intende la possibilità di segnalare casi di eventuali illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al D.Lgs. 24/2023, di condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o sospette frodi e/o violazioni al Codice Etico e al Modello Organizzativo, di cui i Destinatari della presente *policy* siano venuti a conoscenza per ragioni di lavoro, con la garanzia di un'assoluta tutela dell'identità del segnalante finalizzata ad evitare qualunque forma di discriminazione nei confronti del medesimo.

Inoltre, si intende la possibilità di segnalare le seguenti situazioni:

- atti od omissioni che ledono gli interessi finanziari dell'Unione o il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei suddetti settori.

In ogni caso, è dovere precipuo dell'ente gestore della segnalazione composto da Presidente/Componente monocratico dell'Organismo di Vigilanza e dal RIA di adottare ogni misura volta ad assicurare la riservatezza

dell'identità del segnalante, del facilitatore, della persona coinvolta o comunque dei soggetti menzionati nella segnalazione e del contenuto della segnalazione e della relativa documentazione.

In particolare, i soggetti che compongono l'ente gestore:

- ricevono formale incarico come componenti dell'ente gestore dei canali interni che comprende anche la lettera di designazione ad autorizzato *ex* artt. 29 Reg. UE 679/2016 (anche "GDPR") e 2-*quaterdecies* D.Lgs. n. 196/2003 (anche "Codice *Privacy*"). La lettera prevede specifiche istruzioni per il corretto trattamento dei dati personali di cui alla segnalazione, di cui le Società sono Titolari del trattamento *ex* art. 4 par. 1 n. 7) GDPR.
- assicurano indipendenza e imparzialità;
- ricevono un'adeguata formazione professionale sulla disciplina del *whistleblowing*, anche con riferimento a casi concreti.

Qualora la segnalazione interna sia presentata ad un soggetto diverso da quello individuato e autorizzato, la segnalazione deve essere trasmessa, entro sette giorni dal suo ricevimento, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante.

Si precisa che il D.P.R. n. 62 del 2013 prevede che la segnalazione possa essere presentata al superiore gerarchico, ma tale segnalazione non può essere considerata di *whistleblowing* e quindi il segnalante non potrà beneficiare della protezione disposta dal D.Lgs. n. 24/2023.

A tal fine, l'azienda pone a disposizione i seguenti canali di ricezione della segnalazione:

- piattaforma di *Whistleblowing,* che consente di inviare segnalazioni per iscritto, accessibile da qualsiasi *browser* (anche accedendo da dispositivi mobili) avente il seguente indirizzo **https://esprinet.eticainsieme.it.** Questo strumento offre le più ampie garanzie di riservatezza per il segnalante;

- chiamando il numero telefonico **+393427755190** (non sottoposto a procedura di registrazione) presidiato da RIA, il quale riscontra la richiesta, proponendo la fissazione di un appuntamento e, nei casi di particolare urgenza, riceve contestualmente la segnalazione. Di tale conversazione, viene stilato un verbale riassuntivo, il quale viene portato a conoscenza – nel rispetto della riservatezza del segnalante – dell'altro componente dell'ente gestore della segnalazione (Presidente/Componente monocratico dell'O.d.V.) e, entro sette giorni dalla telefonata/dal messaggio, quest'ultimo lo trasmette al segnalante tramite *e-mail* all'indirizzo da esso comunicato in modo che possa verificarne, rettificarne, confermarne il contenuto e sottoscriverlo. Successivamente alla conferma del contenuto, RIA può censire la segnalazione all'interno di un'apposita sezione della piattaforma di *Whistleblowing*, includendo il riferimento *e-mail* fornito dal segnalante al fine di consentire l'invio automatico di un codice univoco necessario per monitorare lo stato di avanzamento della lavorazione della stessa.

Successivamente all'invio della segnalazione, tramite la Piattaforma o tramite chiamata telefonica è poi possibile prenotare un incontro da svolgersi di persona.

8.1. CONTENUTO DELLE SEGNALAZIONI

Il segnalante è tenuto a fornire tutti gli elementi a lui noti utili a riscontrare, con le dovute verifiche, i fatti riportati. In particolare, la segnalazione deve essere circostanziata e completa al fine di consentire l'accertamento del fatto segnalato e deve contenere i seguenti elementi essenziali:

- le generalità del soggetto che effettua la segnalazione con indicazione dell'eventuale ruolo all'interno dell'azienda ovvero la società o l'ente presso cui si svolge la propria attività lavorativa, nonché il consenso - o meno - ad utilizzare, fin da subito o in un momento successivo, l'identità dello stesso nelle attività di verifica e quindi rivelare l'identità dello stesso a soggetti diversi dai gestori della segnalazione e/o all'ufficio del personale competente nella gestione del procedimento disciplinare;
- una chiara e completa descrizione dei fatti oggetto della segnalazione;
- le circostanze di tempo e di luogo in cui sono stati commessi i fatti segnalati;
- le generalità del soggetto che ha posto in essere i fatti oggetto di segnalazione;
- l'indicazione dei beneficiari e dei danneggiati dall'illecito o dalla violazione;
- l'indicazione di eventuali altri soggetti che possano riferire in merito ai fatti oggetto della segnalazione;
- l'allegazione di eventuali documenti che possano confermare la fondatezza dei fatti riportati;
- ogni altra informazione che possa fornire un utile riscontro in merito alla sussistenza dei fatti segnalati.

La segnalazione prevede altresì la necessità da parte del segnalante di dichiarare l'impegno a riferire di quanto a sua conoscenza secondo verità.

8.2. PIATTAFORMA DI SEGNALAZIONE

La piattaforma di segnalazione adottata, residente sul *server* di un soggetto terzo, prevede una registrazione riservata, l'utilizzo della crittografia e un percorso guidato per il segnalante che consentirà allo stesso di inserire le informazioni necessarie elencate al paragrafo 8.1.

Le società del Gruppo Esprinet italiane hanno adottato un'unica piattaforma di segnalazione (eticainsieme) che permette al segnalante di indicare a quale delle Società la segnalazione si riferisce; nella pagina iniziale, infatti, è visualizzata una schermata che presenta indicazione di tutte le Società. Si precisa che sono adottate misure organizzative e di sicurezza che consentono a ciascuna Società di accedere alle segnalazioni di propria competenza.

Il fornitore della piattaforma ha sottoscritto l'accordo sulla protezione dei dati *ex* art. 28 GDPR con il quale si impegna al rispetto delle istruzioni fornite dalle Società Titolari del trattamento, anche in caso di sub-affidamenti.

Il segnalante dovrà compilare una serie di domande, aperte e chiuse, che permetteranno al destinatario della segnalazione di approfondire l'oggetto della stessa in prima battuta anche senza creare un contatto diretto con il segnalante stesso.

Al termine della procedura di segnalazione la piattaforma fornirà al segnalante un codice che permetterà allo stesso di accedere al sistema e, pertanto, alla propria segnalazione per:

- monitorarne lo stato di avanzamento;
- integrare la propria segnalazione con ulteriori elementi fattuali o altra documentazione;
- avere un contatto diretto con i destinatari della segnalazione avviando anche un eventuale scambio di richieste e informazioni.

La piattaforma consente, altresì, di effettuare l'*upload* della documentazione che il segnalante ritiene opportuno portare all'attenzione dei gestori del canale a supporto della propria segnalazione.

8.3. GESTIONE DELLE SEGNALAZIONI

Ricevuta la segnalazione, l'ente gestore della stessa – dopo aver dato evidenza al segnalante della presa in carico entro il termine di sette giorni - provvederà ad analizzarla, con la possibilità di coinvolgere le altre figure e funzioni individuate nei paragrafi precedenti sulla base di una preliminare valutazione della gravità dell'oggetto della segnalazione e dei possibili soggetti e funzioni coinvolti nei fatti segnalati.
Nell'ambito dell'istruttoria i gestori della segnalazione:

- mantengono le interlocuzioni con il soggetto segnalante e possono richiedere a questo, se necessario, integrazioni. Attraverso l'utilizzo della piattaforma, è prevista la possibilità di scambi di richieste tra il segnalante e il destinatario della segnalazione al fine di approfondire i temi oggetto di comunicazione
- svolgono le opportune verifiche coinvolgendo, se necessario, soggetti terzi (interni o esterni alle Società) che abbiano le competenze necessarie per gestire la segnalazione ricevuta;
- sentono la persona coinvolta, anche su sua richiesta, oralmente o mediante procedimento cartolare, attraverso l'acquisizione di osservazioni scritte e documenti.

In ogni caso le generalità del segnalante e qualsiasi altra informazione da cui può evincersi direttamente o indirettamente tale identità, non verranno rivelate a soggetti terzi dai destinatari delle segnalazioni senza il consenso del segnalante al fine di proteggerlo da possibili ritorsioni o discriminazioni. Si precisa che, pur in assenza di consenso ma resosi necessario per ragioni istruttorie, qualora anche altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata, i gestori provvedono ad oscurare i dati personali del Segnalante, nonché degli altri soggetti la cui identità deve rimanere riservata (il facilitatore, il segnalato, le altre persone menzionate nella segnalazione).

Attraverso l'utilizzo della piattaforma, è prevista la possibilità di scambi di richieste tra il segnalante e il destinatario della segnalazione al fine di approfondire i temi oggetto di comunicazione o per organizzare l'incontro previsto per la gestione del canale orale.
Saranno effettuate le opportune verifiche, comprensive dell'eventuale audizione del segnalante qualora ne presti il consenso o lo richieda, e nel caso in cui la segnalazione risultasse fondata verranno informate le

funzioni aziendali competenti affinché siano intraprese le opportune azioni disciplinari interessando altresì gli organi gestionali e di controllo della Società.

Entro il termine di 3 mesi dal ricevimento della segnalazione, i destinatari della segnalazione dovranno dare diligente seguito alla segnalazione e fornire riscontro.

In ogni momento successivo alla ricezione della segnalazione, i destinatari potranno archiviare la stessa qualora la ritengano non rilevante ai sensi della presente procedura.

All'esito dell'istruttoria, i destinatari stileranno una relazione prendendo uno o più dei seguenti provvedimenti:

- archiviazione della segnalazione per irrilevanza;
- proposta di modifica al Modello di Organizzazione, Gestione e Controllo e/o al Codice Etico;
- proposta di avvio di procedimenti disciplinari o sanzionatori - conformemente a quanto previsto dal Modello di Organizzazione, Gestione e Controllo - nei confronti dei soggetti segnalati e di cui sia stata riconosciuta la commissione di un illecito o violazione;
- proposta di avvio di procedimenti disciplinari o sanzionatori - conformemente a quanto previsto dal Modello di Organizzazione, Gestione e Controllo e dalla presente procedura - nei confronti dei segnalanti che abbiamo effettuato segnalazioni infondate, basate su circostanze fattuali non vere ed effettuate con dolo o colpa grave.

8.4. LA SEGNALAZIONE TRAMITE CANALI ESTERNI

In conformità con la normativa vigente, il segnalante può effettuare una segnalazione esterna da presentare all'ANAC qualora:

- abbia già effettuato una segnalazione interna a cui non è stato dato seguito;
- esistano fondati motivi per ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito o che potrebbe essere oggetto di ritorsione;
- abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le procedure per la segnalazione sono definite dall'ANAC e pubblicate sul proprio sito internet, all'indirizzo https://www.anticorruzione.it/-/whistleblowing.

In caso di ritorsioni commesse nel contesto lavorativo di un soggetto del settore privato, l'ANAC informa l'Ispettorato Nazionale del Lavoro, per i provvedimenti di propria competenza.

8.5. DIVULGAZIONE PUBBLICA

Il segnalante ha infine la possibilità di effettuare la segnalazione tramite la divulgazione pubblica beneficiando della protezione prevista dalla presente *policy,* solo qualora:

- abbia previamente effettuato una segnalazione interna o esterna senza aver ricevuto riscontro nei termini previsti;
- abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;

- abbia 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.

8.6. ARCHIVIAZIONE

La Piattaforma utilizzata dalla Società permette l'archiviazione delle segnalazioni e della documentazione allegata in modalità informatica e crittografata nonché in conformità alla normativa applicabile in materia di protezione dei dati personali.

Eventuale altra documentazione prodotta dai destinatari delle segnalazioni verrà archiviata e conservata nel rispetto della riservatezza nel limite massimo di cinque anni, salvo eventuali richieste provenienti dall'Autorità (ad es., l'instaurarsi di un procedimento penale).

8.7. INFORMAZIONI SUL TRATTAMENTO DEI DATI DERIVATI DALLA GESTIONE DELLE SEGNALAZIONI

In accordo con la normativa vigente sulla protezione dei dati, informiamo gli interessati che i loro dati personali saranno trattati dalla società del Gruppo Esprinet italiana che riceve la segnalazione, Titolare del trattamento, al solo scopo di elaborare tale segnalazione.

Si considerano quali interessati:

- la persona segnalante: la persona fisica che effettua la segnalazione sulle violazioni acquisite nell'ambito del proprio contesto lavorativo;
- il facilitatore: una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- la persona coinvolta: la persona fisica menzionata nella segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata.

Il Titolare tratterà i dati personali degli interessati di seguito descritti:

- dati identificativi e di contatto, quali nome e cognome, indirizzo e-mail o numero di telefono;
- dati relativi al rapporto con il Titolare;
- altri dati che saranno inseriti dalla persona segnalante nella compilazione del form di segnalazione/forniti al telefono o successivamente acquisiti dai gestori delle segnalazioni nell'ambito dell'attività istruttoria.

I dati personali e le altre informazioni fornite possono essere portati all'attenzione delle figure e degli uffici identificati nei paragrafi precedenti per la corretta investigazione e trattamento della segnalazione.

La base giuridica dei trattamenti suindicati è rinvenibile nell'adempimento dell'obbligo legale *ex* art. 6, par. 1, lett. c) del GDPR come descritto nel D.Lgs. n. 24/2023.

La base giuridica è, altresì, rinvenibile, per ciò che riguarda il trattamento di categorie particolari di dati, nell'articolo 9, par. 2, lett. b) del GDPR in quanto il trattamento è necessario per assolvere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nonché nell'articolo 9, par. 2 lett. g) del GDPR in quanto il trattamento è necessario per motivi di interesse pubblico rilevante sulla base dell'art. 2-*sexies* del D.Lgs. n. 196/2003.

Il trattamento dei dati giudiziari resosi eventualmente necessario per la gestione delle segnalazioni *whistleblowing* ricevuta è legittimo sulla base dell'art. 10 GDPR in correlazione con l'art. 2-*octies* del D.Lgs. n. 196/2003

Qualità dei dati

I segnalanti devono aver fondato motivo di ritenere che i dati personali e le informazioni sulle violazioni contenuti nella segnalazione siano veri, esatti e aggiornati.

Quindi, i dati personali forniti nell'ambito delle segnalazioni saranno trattati in conformità con la normativa applicabile in materia di protezione dei dati personali e per le finalità legittime relative alle indagini derivanti dalla segnalazione, non possono essere utilizzati per fini incompatibili con tale scopo, devono essere adeguati e non eccessivi per tali obiettivi.

In particolare, il Titolare tratterà i dati personali degli interessati unicamente per le seguenti finalità:

- presa in carico della segnalazione da parte dei gestori,
- invio di eventuali richieste e/o ricezione di riscontro alle richieste inviate dal segnalante e dai gestori della segnalazione,
- gestione istruttoria: esecuzione di verifiche sulla fondatezza della segnalazione,
- gestione dei provvedimenti conseguenti, anche sotto il profilo disciplinare.

Diritti di accesso, rettifica, cancellazione, opposizione, limitazione del trattamento dei dati o revoca del consenso

Ciascuna delle società che compone il Gruppo Esprinet sarà considerata Titolare del trattamento dei reclami presentati secondo la procedura regolata nella presente Politica quando i reclami riguardino il suo personale.

I diritti di cui agli articoli da 15 a 22 del Regolamento (UE) 2016/679 (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento) possono essere esercitati nei limiti di quanto previsto dall'articolo 2-*undecies* del D.Lgs. n. 196/2003, ovverosia possono essere limitati qualora dalla richiesta possa derivare un pregiudizio effettivo e concreto, ad esempio, alla riservatezza dell'identità del segnalante o allo svolgimento di investigazioni difensive o all'esercizio di un diritto in sede giudiziaria. Per esercitare tali diritti, gli interessati possono inviare una e-mail a dpo@esprinet.com, indicando il diritto specifico che vogliono esercitare.

Comunicazione e trasferimento dati

Inoltre, i dati relativi alle segnalazioni possono essere comunicati alle altre società del Gruppo, i cui nomi e indirizzi compaiono sul sito web www.esprinet.com quando l'organismo interno responsabile della segnalazione ritiene che il loro intervento sia necessario per l'indagine e il chiarimento dei fatti.

Inoltre, i dati ricevuti attraverso il sistema interno di segnalazioni descritto nella presente Politica possono essere comunicati ad altre entità che forniscono servizi di consulenza necessari per la corretta gestione delle segnalazioni, questi agiranno come responsabili del trattamento.

Conservazione dei documenti e periodo di conservazione

I dati trattati nell'ambito delle indagini saranno conservati per un periodo di tempo non superiore a cinque anni dal termine di chiusura dell'istruttoria relativa alla segnalazione, salvo il caso in cui il Titolare abbia documentata necessità di conservare i dati per un periodo superiore a cinque anni ad esempio in caso di procedimento disciplinare, amministrativo o giudiziario.

Saranno adottate misure per garantire un'adeguata sicurezza e riservatezza delle informazioni, con la possibilità di stabilire misure di sicurezza rafforzate e prendere precauzioni estreme per garantire il rispetto del dovere di riservatezza, tenendo conto della natura dei dati raccolti.

Rimane inteso che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

9. ALTRI SISTEMI DI RILEVAZIONE

9.1. SEGNALAZIONI ALL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza, oltre ad ordinari flussi informativi, è tenuto a ricevere segnalazioni relative a presunte violazioni del Modello Organizzativo che possano costituire un rischio "231" diretto o indiretto.

Tali informative si rendono necessarie per consentire all'Organismo interventi tempestivi finalizzati a prevenire la commissione dei reati previsti dal D.Lgs. n. 231/2001 e per vigilare sul rispetto delle regole che sono parte integrante del Modello stesso.

9.2. ORDINARIA ATTIVITÀ DI *AUDIT*

L'*Internal Audit*, nel corso di ordinarie verifiche previste dal Piano di *Audit*, potrebbe rilevare segnali sintomatici di comportamenti fraudolenti o di gravi violazioni al Codice Etico (cd. *red flag*).

Anche in questi casi, effettuata una preliminare valutazione, procede secondo quanto stabilito nel capitolo 13.

9.3. RECLAMI DI CLIENTI

I reclami dei clienti, oltre che richiedere un tempestivo intervento per ragioni di *customer satisfaction*, possono sottendere aspetti fraudolenti o comportamenti comunque contrari al Codice Etico.

Per tale ragione, chiunque dovesse ricevere tali reclami dovrà valutarli con attenzione e informare, soltanto nei casi di maggiore gravità, l'Organismo di Vigilanza.

10. TUTELA DEL SEGNALANTE

Ad eccezione dei casi in cui sia configurabile una responsabilità penale a titolo di calunnia o di diffamazione ai sensi delle disposizioni o dell'art. 2043 c.c. o, l'identità del segnalante viene protetta in ogni fase successiva alla segnalazione stessa.

Pertanto, l'identità del segnalante non può essere rivelata senza il suo espresso consenso e tutti coloro che ricevono o sono coinvolti nella gestione delle segnalazioni sono tenuti a tutelarne la riservatezza.

La violazione dell'obbligo di riservatezza rappresenta una grave violazione disciplinare.

Parimenti, rappresenta una grave violazione disciplinare qualunque forma di ritorsione o discriminazione attuata nei confronti del segnalante, che è tenuto a denunciare tali comportamenti al suo diretto superiore gerarchico o direttamente l'O.d.V. Tra le forme di ritorsione o discriminazione, si segnalano a titolo esemplificativo:

a) il licenziamento, la sospensione o misure equivalenti;
b) la retrocessione di grado o la mancata promozione;
c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
e) le note di merito negative o le referenze negative;
f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
g) la coercizione, l'intimidazione, le molestie o l'ostracismo;
h) la discriminazione o comunque il trattamento sfavorevole;
i) 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;
j) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
k) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
l) 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;
m) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
n) l'annullamento di una licenza o di un permesso;
o) la richiesta di sottoposizione ad accertamenti psichiatrici o medici;
p) la pretesa di risultati impossibili da raggiungere nei modi e nei tempi indicati;
q) una valutazione della performance artatamente negativa;
r) una revoca ingiustificata di incarichi; un ingiustificato mancato conferimento di incarichi con contestuale attribuzione ad altro soggetto;
s) il reiterato rigetto di richieste (ad es. ferie, congedi);
t) la sospensione ingiustificata di brevetti, licenze, etc.

In ogni caso, il licenziamento ritorsivo o discriminatorio del soggetto che segnala i fatti rientranti nella materia del *Whistleblowing* è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'art. 2103 c.c.
Infine, è onere del Datore di Lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari o a demansionamenti, licenziamenti, trasferimenti o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti sulle condizioni di lavoro, dimostrare che tali misure non sono in alcun modo conseguenza della segnalazione stessa.

La protezione del segnalante è estesa anche nel caso di segnalazione anonima, alla quale è poi seguita l'identificazione del segnalante. Inoltre, le segnalazioni anonime ricevute sono considerate alla stregua di segnalazioni ordinarie da trattare secondo i criteri stabiliti nella presente *policy* e nella normativa locale.
Si specifica anche che la protezione per il segnalante non è garantita nei casi di:

- sentenza primo grado per diffamazione e calunnia;
- casi di dolo o colpa grave.

L'identità del segnalante – mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati – può essere rivelata alla funzione Risorse Umane e all'incolpato esclusivamente nei seguenti casi:

- quando vi sia stato il consenso espresso del segnalante;
- nel procedimento disciplinare, quando la contestazione disciplinare risulti fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante risulti assolutamente indispensabile alla difesa dell'incolpato. In ogni caso, l'attività di verifica dovrà tendere ad acquisire autonome evidenze che non richiedano il riscorso a tale ultima necessità.

10.1. SEGNALAZIONI NON AMMESSE

Le segnalazioni devono sempre avere un contenuto da cui emerga un leale spirito di partecipazione al controllo.
È parimenti vietato:

- il ricorso ad espressioni ingiuriose;
- l'inoltro di segnalazioni con finalità puramente diffamatorie o calunniose;
- l'inoltro di segnalazioni che attengano esclusivamente ad aspetti della vita privata, senza alcun collegamento diretto o indiretto con l'attività aziendale. Tali segnalazioni saranno ritenute ancor più gravi quando riferite ad abitudini e orientamenti sessuali, religiosi e politici;
- l'invio di rivendicazioni, contestazioni, richieste di carattere personale della persona segnalante o della persona che abbia sporto una denuncia all'autorità giudiziaria o contabile, relative esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate;
- alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione Europea o nazionali indicati nella parte II dell'allegato al presente decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione Europea indicati nella parte II dell'allegato alla direttiva

(UE) 2019/1937, seppur non indicati nella parte II dell'allegato al presente decreto;

- alle segnalazioni di violazioni in materia di sicurezza nazionale, nonché' di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione Europea.

11. CONTROLLI AMMESSI E CONTROLLI VIETATI

11.1. CONTROLLI INDIRETTI

Qualunque controllo indiretto sull'attività dei lavoratori operato mediante gli strumenti di lavoro (*email*, *badge*, pc, telefoni cellulari etc…), reso necessario per motivi organizzativi, di sicurezza sui luoghi di lavoro e tutela del patrimonio aziendale, potrà essere utilizzato anche per finalità di accertamento di presunti comportamenti fraudolenti o contrari al Codice Etico (es. utilizzo non autorizzato di credenziali di accesso altrui).

A tal fine viene resa preventivamente al singolo lavoratore adeguata informativa circa le modalità d'uso di tali strumenti nonché circa le modalità di effettuazione dei controlli.

In ogni caso, dovranno essere rispettati i principi *privacy* di proporzionalità, pertinenza e non eccedenza.

Sono sempre vietati controlli che assumano carattere vessatorio.

11.2. CONTROLLI MEDIANTE SISTEMI DI VIDEOSORVEGLIANZA

I controlli mediante impianti audiovisivi e altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere effettuati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

In caso di installazione degli impianti audiovisivi, dovrà preventivamente essere resa al singolo lavoratore adeguata informativa circa le modalità d'uso di tali strumenti nonché circa le modalità di effettuazione dei controlli.

11.3. CONTROLLI DIRETTI

Per controllo diretto si intende qualunque intervento da parte del diretto superiore o delle funzioni di controllo nei confronti del lavoratore. Esso non solo è ammesso, ma è doveroso.

Tale forma di controllo rappresenta l'espressione del dovere-potere direttivo di coloro che hanno una responsabilità del conseguimento degli obiettivi aziendali e del rispetto delle regole.

Il controllo diretto deve mirare alla diffusione di comportamenti virtuosi e rispettosi del Codice Etico e delle procedure aziendali.

Nel caso di sospetto comportamento fraudolento o contrario al Codice Etico, è consentito, al diretto responsabile e al personale della funzione di *Internal Audit*:

- il controllo della postazione di lavoro;
- il controllo diretto sul contenuto del pc aziendale dato in dotazione al singolo dipendente.

Tali controlli dovranno sempre avvenire esclusivamente in presenza del diretto interessato e, solo in casi eccezionali, urgenti e di rilevante gravità, è ammesso il controllo anche in sua assenza, ma alla presenza di un collega da questi indicato o di un rappresentante sindacale.

12. POLITICHE DI SICUREZZA INFORMATICA

Tutti i dipendenti sono tenuti al rispetto di quanto previsto dalla *LIG01001 Politica aziendale relativa all'utilizzo degli strumenti informatici e sicurezza delle informazioni.*

Vale quanto stabilito dal par.11 della presente *policy* in tema di utilizzabilità degli esiti dei monitoraggi necessitati da ragioni di verifica di eventuali comportamenti illeciti.

Si richiama altresì quanto già previsto dalla Politica menzionata.

13. MODALITÀ DI ESECUZIONE E DI DOCUMENTAZIONE DELLE INTERVISTE

Nel corso di una verifica condotta dal RIA e/o dal Presidente/Componente monocratico dell'O.d.V., finalizzata ad accertare la veridicità dell'oggetto della segnalazione, potranno essere espletate delle attività di intervista di dipendenti e/o collaboratori in grado di riferire circostanze utili.

Chiunque, convocato per un'audizione dal RIA e/o dal Presidente/Componente monocratico dell'O.d.V., è obbligato:

- a presentarsi;
- a collaborare lealmente e con la massima trasparenza, riferendo qualunque circostanza a lui nota in relazione ai fatti e alle domande che gli verranno poste;
- a fornire qualunque documentazione integrativa gli venga chiesta, a supporto delle informazioni fornite;
- a sottoscrivere la relazione di intervista che sarà redatta.

il RIA e/o il Presidente/Componente monocratico dell'O.d.V. avranno cura di:

- evitare di assumere atteggiamenti vessatori o inquisitori nei confronti del dipendente/collaboratore intervistato, anche quando dovesse trattarsi del presunto autore della violazione:
- non consentire di assistere alla audizione a qualunque soggetto diverso dall'intervistato;
- non rilasciare copia della relazione di intervista;

L'intervista non costituisce in alcun modo contestazione disciplinare, anche quando dovesse riguardare il presunto autore della violazione oggetto dell'accertamento.

14. MODALITÀ E CRITERI PER LA TRACCIABILITÀ, L'ARCHIVIAZIONE, CONTROLLO E RENDICONTAZIONE DELLE ATTIVITÀ SVOLTE

Le attività di verifica rispondono ai principi generali del SCIGR ed agli *standard* professionali degli *auditor*, anche in tema di tracciabilità, archiviazione e rendicontazione delle attività di verifica.

Tuttavia, stante la particolare natura, anche ai fini *privacy*, dei dati raccolti nel corso di un'attività di verifica, tale documentazione dovrà essere sottoposta a rafforzate misure di sicurezza.

È a tutti vietata la cancellazione o la distruzione di *e-mail*, di file o documenti da conservare in esecuzione di un obbligo di legge, per motivi fiscali e per espresse disposizioni di *policy* aziendali. Inoltre, va tracciato e conservato qualsiasi documento elettronico (*e-mail, file* etc…) riconducibile ad operazioni in deroga rispetto alle *policy* aziendali.

15. GESTIONE DEI RAPPORTI EVENTUALI CON POLIZIA E AUTORITÀ GIUDIZIARIA

Nel caso in cui si rendesse necessario, per fatti di rilevante gravità, richiedere l'intervento delle Forze dell'Ordine, l'Organismo di Vigilanza dovrà informare il Responsabile Sicurezza che provvederà secondo competenze territoriali e funzionali. Eventuali denunce/querele sono elaborate e depositate a cura dell'Ufficio Legale.

Chiunque dovesse essere convocato dalla Polizia Giudiziaria o dall'Autorità Giudiziaria o dal Giudice Penale, in veste di persona informata sui fatti o di testimone per vicende connesse all'attività aziendale o ad accertate frodi o illeciti di cui sia stata presentata querela/denuncia da parte dell'azienda, è tenuto ad informarne l'Organismo di Vigilanza che potrà autorizzare la visione di atti interni o di dichiarazioni precedentemente rese in sede di intervista, quale aiuto alla memoria e per consentire una collaborazione fattiva e trasparente con gli organi di Polizia e Autorità Giudiziaria.

Al di fuori di questi casi, la persona convocata dovrà mantenere l'assoluto riserbo su dettagli e motivi della convocazione ricevuta.

16. SISTEMA SANZIONATORIO

Il sistema sanzionatorio applicato in azienda e prescritto dal CCNL Commercio prevede l'erogazione delle seguenti sanzioni disciplinari:

- biasimo inflitto verbalmente per le mancanze lievi;
- biasimo inflitto per iscritto nei casi di recidiva delle infrazioni di cui al precedente punto;
- multa in misura non eccedente l'importo di 4 ore della normale retribuzione;
- sospensione dalla retribuzione e dal servizio per un massimo di giorni 10;
- licenziamento disciplinare senza preavviso e con le altre conseguenze di ragione e di legge.

La scelta della sanzione da erogare va commisurata, secondo il principio di gradualità, a valle della verifica della gravità dell'infrazione commessa, tenendo presente, in particolare:

- le evidenze raccolte nel procedimento disciplinare;
- la natura volontaria o colposa dell'infrazione commessa;
- la recidività del comportamento illecito;
- il danno, anche potenziale, arrecato all'azienda, intesa sia come struttura fisica, sia popolazione di dipendenti/collaboratori.

Con specifico riferimento alla regolamentazione delle segnalazioni *whistleblowing* di cui alla presente *policy*, pur non costituendo un elenco tassativo, sono sempre fonte di responsabilità disciplinare le seguenti infrazioni:

a. nei confronti di tutti i soggetti che:

- ostacolino o tentino di ostacolare le segnalazioni di cui alla presente *policy*;
- violino l'obbligo di riservatezza dell'identità del segnalante e di qualsiasi altra informazione di cui alle segnalazioni su indicate;
- attuino forme di ritorsione o discriminazione nei confronti del segnalante e dei facilitatori;

b. nei confronti di chi ha adottato la presente *policy*:
   - quando si rilevi che la stessa non è conforme alle previsioni di cui agli artt. 4 e 5 del D.Lgs. 24/2023;

c. nei confronti di chi approfondisce le segnalazioni:
   - quando non è stata svolta l'attività di verifica ed analisi delle segnalazioni ricevute;

d. nei confronti dei soggetti segnalanti:
   - nel caso in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per il reato di diffamazione commesso con la segnalazione o per i reati di calunnia o di diffamazione commessi con la denuncia all'autorità giudiziaria o contabile o qualora sia accertata la responsabilità civile del segnalante per comportamenti riconducibili ai reati sopra indicati in caso di dolo o colpa grave;

e. nei confronti della persona coinvolta che si sia resa colpevole di violazioni/illeciti rilevanti ai sensi della presente policy, nel caso in cui la segnalazione sia risultata fondata.

Infine, ogni altra violazione delle regole procedurali declinate nella presente *policy* costituisce illecito disciplinare.

17. ARCHIVIAZIONE

La copia in originale cartacea della presente *policy* è archiviata presso l'ufficio *Internal Audit*, come evidenza delle firme di redazione, controllo ed approvazione.

Una copia è archiviata all'interno del sistema documentale aziendale.