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

Società :
Tutte le società del Gruppo Esprinet

Sede :
Tutte le sedi

Sottosistema
D.Lgs. 231/01, Codigo Penal, L. 179/2017

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	G.Monina	A.Cattani
			CRO	RIA	AD
01	15/10/18	Aggiornamento Whistleblowing, estensione al Gruppo Esprinet	P.Aglianò	G.Monina	A.Cattani
			CRO	RIA	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 del Gruppo Esprinet (d'ora in avanti semplicemente Gruppo Esprinet).

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.

2. DESTINATARI

La presente *policy* si applica a tutti i dipendenti e collaboratori[1] del Gruppo Esprinet e per quel che attiene la parte relativa alle segnalazioni in materia di *Whistleblowing* a tutti i Destinatari del Codice Etico e del Modello Organizzativo.

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

[1] Si intendono per collaboratori, i dipendenti di fornitori, i collaboratori a progetto, gli agenti e chiunque stabilmente operi con il Gruppo Esprinet Italia.

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.
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 di Esprinet, commessa da soggetti esterni all'organizzazione (clienti, fornitori, terzi)
FRODE INTERNA	Frode ai danni di 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)
ILLECITO AZIENDALE	Qualunque evento di natura umana (condotta ed elemento soggettivo) che cagioni o che sia potenzialmente atto a cagionare un danno all'azienda
ILLECITI (rilevanti anche ai fini delle segnalazioni Whistleblowing)	Si intende la commissione – o possibile commissione – di un reato per cui è applicabile la responsabilità degli enti ex D.Lgs. 231/01. Tali reati sono elencati nel medesimo D.Lgs. 231/01. Per le società spagnole si veda art. 13 del Código Penal.

IRREGOLARITA'	Sono considerate tali le violazioni delle procedure e delle regole previste dal Codice Etico e/o dal Modello di Organizzazione, Gestione e Controllo di Esprinet.
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)
RED FLAG	indicatori rilevanti di potenziali frodi o abusi, che costituiscono spunti per l'avvio di una verifica
WHISTLEBLOWING	Sistema di segnalazioni mediante il quale il lavoratore che, durante l'attività lavorativa all'interno di un'azienda, rileva una possibile frode, 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
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.

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 Italia;
- 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 Italia 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)
PROCEDURE E DOCUMENTI INTERNI	Codice etico
	Sistema disciplinare interno
	Modello "231" adottato dal Gruppo Esprinet Italia
	Regole per l'utilizzo degli 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 Esprinet
	Mansionario Incarichi Privacy Celly
	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 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 dal Presidente dell'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 dal Presidente dell'Organismo di Vigilanza nelleipotesi 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 su segnalazioni da parte del Presidente dell'Organismo di Vigilanza;
- 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 al Presidente dell'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 del Presidente 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 al Presidente dell'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;
- 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 *Chief Risk Officer* e del RIA, mettendo a disposizione i dati e le informazioni necessari e la loro più approfondita conoscenza dei processi aziendali.

8. CANALI DI SEGNALAZIONE E TUTELA DEI SEGNALANTI

La rilevazione di casi di potenziali frodi può avvalersi del leale contributo di tutti i dipendenti e destinatari della presente *policy*.

Tutti sono tenuti a segnalare al Presidente dell'Organismo di Vigilanza qualunque caso di sospetta frode o violazione al Codice Etico e del Modello Organizzativo di cui dovessero venire a conoscenza, secondo le disposizioni che seguono.

8.1. WHISTLEBLOWING

Per *whistleblowing* si intende la possibilità di segnalare casi di eventuali illeciti, irregolarità, di sospette frodi e/o violazioni al Codice Etico e al Modello Organizzativo, di cui i Destinatari del Codice Etico e del Modello Organizzativo 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.

In ogni caso, è dovere precipuo del destinatario della segnalazione (Presidente dell'Organismo di Vigilanza 231, o in alternativa RIA e CRO, nel caso di segnalazione *Whistleblowing*) di adottare ogni misura volta ad assicurare la riservatezza dell'identità del segnalante.

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

- tramite lettera al Presidente dell'ORGANISMO DI VIGILANZA - Esprinet S.p.A. c/o Energy Park 20871 Vimercate (MB)
- piattaforma di *Whistleblowing* accessibile da qualsiasi *browser* (anche accedendo da dispositivi mobili) avente il seguente indirizzo https://esprinet.eticainsieme.it. Quest'ultimo strumento offre le più ampie garanzie di riservatezza per il segnalante.

8.2. 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 attuale o trascorso all'interno dell'azienda.
- 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 irregolarità;
- 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.

8.3. 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 8.2.
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.

8.4. Gestione delle segnalazioni

Ricevuta la segnalazione, il destinatario della stessa – dopo aver dato evidenza al segnalante della presa in carico - provvederà ad analizzarla entro il temine di 15 giorni, 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.

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.

Saranno effettuate le opportune verifiche, comprensive dell'eventuale audizione del segnalante qualora ne presti il consenso, 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 60 giorni i destinatari della segnalazione dovranno concludere l'istruttoria e informare dell'esito il soggetto segnalante.

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 irregolarità;
- 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.

8.5. 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.

9. ALTRI SISTEMI DI RILEVAZIONE

9.1. Segnalazioni all'Organismo di Vigilanza

L'Organismo di Vigilanza (OdV), 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 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, il Presidente dell'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. 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 al Presidente dell'Organismo di Vigilanza.
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.

Nel corso del procedimento disciplinare, l'identità del segnalante può essere rivelata alla funzione Risorse Umane e all'incolpato esclusivamente nei seguenti casi:

- quando vi sia stato il consenso espresso del segnalante;
- 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.

11. CONTROLLI AMMESSI E CONTROLLI VIETATI

11.1. CONTROLLI INDIRETTI SUGLI STRUMENTI DI LAVORO E VIDEOSORVEGLIANZA

In relazione al contenuto del Decreto attuativo del *Jobs Act* (D.Lgs. n. 151/2015), 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 anche utilizzato per finalità di accertamento di presunti comportamenti fraudolenti o contrari al Codice Etico (es. utilizzo non autorizzato di credenziali di accesso altrui).

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

Sono sempre vietati controlli che assumano carattere vessatorio.

Tali strumenti, in nessun caso, potranno essere utilizzati come forma di monitoraggio continuo dell'attività lavorativa dei dipendenti, anche quando tale monitoraggio dovesse essere finalizzato alla rilevazione di eventuali illeciti. Solo a seguito di una segnalazione o di altri fondati elementi, potranno essere estratti dati utilizzabili quali evidenze di condotte disciplinarmente o penalmente rilevanti.

11.2. ALTRE ATTIVITÀ DI CONTROLLO VIETATE

È severamente vietato:

- installare sistemi di videosorveglianza che includano anche registrazioni audio;
- installare sistemi di videosorveglianza in luoghi deputati ad attività ricreative (es. mensa, *toilette* etc…);
- attivare sistemi che consentano da remoto l'ascolto delle telefonate o di altre forme di comunicazione;
- attivare il sistema di viva-voce, nel corso di una conversazione telefonica, consentendone l'ascolto a terzi presenti, senza autorizzazione dell'interlocutore;
- qualunque ulteriore forma di controllo occulto, remoto e non autorizzato.

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 di far, a tal fine, rispettare le 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 e i collaboratori delle società del Gruppo Esprinet sono tenuti al rispetto di quanto previsto dalle regole in tema di utilizzo degli strumenti degli strumenti tecnologici, degli applicativi e dei programmi informatici.

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 dalle procedure e policy interne.

13. MODALITÀ DI ESECUZIONE E DI DOCUMENTAZIONE DELLE INTERVISTE

Nel corso di una verifica condotta dalla funzione di *Internal Audit* e/o dal Presidente dell'O.d.V. con riguardo alle segnalazioni in materia di *Whistleblowing*, finalizzata ad accertare presunte condotte fraudolente o in violazione al Codice Etico, potranno essere espletate delle attività di intervista di dipendenti e collaboratori in grado di riferire circostanze utili.

Chiunque, convocato per un'audizione dal RIA o dal Presidente dell'Organismo di Vigilanza, 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.

La funzione di *Internal Audit* e il Presidente dell'Organismo di Vigilanza 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, per non incorrere nel divieto *ex* art. 24, comma 1, lett. f) D.Lgs. n. 196/2003;

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 email, 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 (*email, 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, il Presidente dell'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 il Presidente dell'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.

In relazione alla presente *policy*, pur non costituendo un elenco tassativo, sono sempre fonte di responsabilità disciplinare le seguenti infrazioni:

- violazione dell'obbligo di tutela della riservatezza dell'identità del segnalante;
- esecuzione di forme di ritorsione o discriminazione attuate nei confronti del segnalante;
- effettuazione di segnalazioni false e ingiuriose;
- distruzione/cancellazione di *email*, *file* o documenti inerenti l'attività lavorativa, senza la necessaria autorizzazione;
- rifiuto di presentarsi per l'audizione a seguito della convocazione da parte della funzione *Internal Audit* o del Presidente dell'Organismo di Vigilanza;
- rifiuto di collaborare con le funzioni di cui al punto precedente, non rispondendo alle domande poste o fornendo informazioni non veritiere.

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.