

**MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO**  
**ex D.Lgs. 231/01**

**Versione del documento**

<i>Versione</i>	<i>Data</i>	<i>Descrizione</i>
<b>V.2.0</b>	<b>22 marzo 2024</b>	<b>Aggiornamento</b>

## SOMMARIO

PARTE GENERALE .....	4
IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 .....	4
1.1 Il regime di responsabilità amministrativa-penale a carico di persone giuridiche, società ed associazioni anche prive di personalità giuridica .....	4
1.2 Le fattispecie di reato (i c.d. “reati presupposto”).....	5
1.3 Delitti tentati .....	5
1.4 Criteri di imputazione e esclusione della responsabilità 231.....	6
1.5 Le sanzioni.....	7
1.6 Vicende societarie .....	7
1.7 I reati commessi all'estero.....	8
1.8 Gruppi di Società' .....	8
2. L'ADOZIONE DEL MODELLO DA PARTE DI MONEYNET .....	8
2.1 Gli obiettivi perseguiti da Moneynet con l'adozione del Modello .....	8
2.2 Struttura e Componenti del Modello Organizzativo .....	9
2.3 Destinatari.....	9
2.4 Approccio Metodologico .....	9
2.5 Identificazione delle attività a rischio .....	10
2.6 Identificazione e analisi degli attuali presidi al rischio .....	11
2.7 Esiti Risk Assessment.....	11
3. Redazione e diffusione del Modello organizzativo e gestionale.....	11
3.1 La struttura del Modello della Società .....	12
3.2 Linee di condotta.....	13
3.3 Principi generali dei presidi organizzativi.....	16
4 L'Organismo di Vigilanza .....	18
4.1 Struttura e composizione dell'Organismo di Vigilanza .....	18
4.2 Requisiti .....	19
4.3 Revoca.....	20
4.4 Cause di sospensione .....	21
4.5 Temporaneo impedimento .....	21
4.6 Definizione dei compiti e dei poteri dell'Organismo di Vigilanza .....	21
4.7 Reporting dell'Organismo di Vigilanza.....	23
4.8 Flussi informativi nei confronti dell'Organismo di Vigilanza.....	24
5. La diffusione del Modello e la formazione .....	26
5.1 L'attività formativa 231 .....	26
6. Il sistema sanzionatorio .....	27
6.1 Destinatari del sistema sanzionatorio.....	27
6.2 Principi generali relativi alle sanzioni .....	27
6.3 Sanzioni relative al personale dipendente .....	28
6.4 Sanzioni relative al personale dipendente con qualifica di dirigente .....	28
6.5 Sanzioni relative ai componenti dell'organo amministrativo.....	29
6.6 Misure nei confronti delle controparti contrattuali .....	29
7. PROTOCOLLI.....	30
8. FLUSSI INFORMATIVI .....	46

## PARTE GENERALE

### IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

#### 1.1 Il regime di responsabilità amministrativa-penale a carico di persone giuridiche, società ed associazioni anche prive di personalità giuridica.

Con l'emanazione del D. Lgs. 8 giugno 2001, n. 231, il Legislatore ha parzialmente attuato la Legge delega n. 300/2000, che, a sua volta, ha recepito normative sopranazionali, ossia la Convenzione del 26 maggio 1997, relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità Europee o degli Stati membri dell'Unione Europea, e la Convenzione OCSE del 17 dicembre 1997, sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali.

Detto Decreto (come integrato dal D.M. n. 201 del 2003 e da successivi interventi legislativi) ha introdotto per la prima volta nel nostro ordinamento la responsabilità di persone giuridiche, società ed associazioni, anche prive di personalità giuridica (di seguito, per brevità, "enti" o "ente"), per attività illecita derivante dalla commissione di alcuni reati, posti in essere a vantaggio e/o nell'interesse dell'ente, da parte di:

- persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente (i cd soggetti apicali) o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo degli stessi;
- persone sottoposte (i cd soggetti sottoposti) alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a);
- soggetti esterni che, operando in nome e/o per conto dell'ente, compiono atti nei confronti dell'esterno.

Ciò significa che, in caso di commissione di uno o più reati espressamente previsti dalla legge ad opera di un soggetto apicale, ovvero di un sottoposto, o di un soggetto esterno all'ente, si aggiunge, alla responsabilità penale dell'autore materiale del reato, la responsabilità amministrativa dell'ente, se il reato è stato commesso nel suo interesse o la Società ne ha comunque tratto un vantaggio.

L'ente è chiamato a rispondere con il proprio patrimonio e la sua responsabilità è autonoma rispetto a quella dell'autore del reato cui si aggiunge anche quando l'autore del reato non è stato individuato o non è imputabile oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

Ai sensi dell'art. 5, comma 2, del Decreto, "l'ente non risponde se le persone sopra indicate hanno agito nell'interesse esclusivo proprio o di terzi".

Ai fini dell'affermazione della responsabilità dell'ente, oltre all'esistenza dei richiamati requisiti che consentono di collegare oggettivamente il reato all'ente, il legislatore impone l'accertamento della colpevolezza dell'ente. Tale condizione si identifica con una colpa da organizzazione, intesa come violazione di adeguate regole di diligenza autoimposte dall'ente medesimo e volte a prevenire lo specifico rischio da reato.

Ai sensi dell'art. 6 del Decreto, la responsabilità amministrativa è esclusa pertanto se l'ente coinvolto dimostra, prima della commissione del reato, di aver adottato ed efficacemente attuato, fra l'altro, Modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione dei reati previsti dal Decreto sia che il reato sia stato commesso da un soggetto apicale sia che sia stato commesso da un soggetto sottoposto.

## 1.2 Le fattispecie di reato (i c.d. “reati presupposto”)

L'insorgenza della responsabilità in capo all'ente non è conseguente alla commissione di qualsiasi reato, bensì di quelli esclusivamente previsti dalla legge.

I reati da cui può conseguire la responsabilità amministrativa per l'ente sono espressamente indicati nel D.Lgs. 231/2001, nonché in altri provvedimenti di legge che al D.Lgs. 231/2001 fanno rinvio, sono:

- Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24 dlgs. 231/01)
- i delitti informatici, di trattamento illecito di dati, nonché i reati commessi con violazione delle prescrizioni in materia di cyber security (art. 24 bis);
- i delitti di criminalità organizzata (art. 24 ter);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art.25)
- i reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis);
- i delitti contro l'industria e il commercio (art. 25 bis 1);
- i reati societari (art. 25 ter);
- i reati con finalità di terrorismo o di eversione dall'ordine democratico (art. 25 quater);
- i reati commessi nell'effettuazione di pratiche di mutilazione degli organi genitali femminili (art. 25 quater.1);
- i reati contro la personalità individuale (art. 25 quinquies);
- i reati di abuso di informazioni privilegiate e di manipolazione del mercato (art. 25 sexies);
- una serie di reati (dall'associazione a delinquere, al traffico di stupefacenti, a talune fattispecie di ostacolo alla giustizia) a condizione che siano commessi da organizzazioni criminali che operano a livello internazionale (cd. reati transnazionali);
- i reati di omicidio colposo e lesioni colpose gravissime e gravi commessi con violazione delle norme sulla sicurezza del lavoro (art. 25 septies);
- i reati di ricettazione, riciclaggio e di impiego di denaro, beni o utilità di provenienza illecita nonché di autoriciclaggio (art. 25 octies);
- i delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1);
- i reati in materia di violazione del diritto d'autore (art. 25 novies),
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies);
- i reati ambientali (art. 25 undecies);
- il reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25 duodecies);
- i reati di razzismo e xenofobia (art. 25-terdecies);
- i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25- quaterdecies);
- i reati tributari (art. 25 – quinquiesdecies);
- il contrabbando (art. 25-sexiesdecies);
- i delitti contro il patrimonio culturale (art. 25-septiesdecies)
- riciclaggio dei beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies) .

## 1.3 Delitti tentati

La responsabilità della società può conseguire non soltanto allorché si siano verificati tutti gli elementi costitutivi della fattispecie di reato (es. gli atti fraudolenti, l'induzione in errore, il profitto e il danno, nel reato di truffa), ma anche nell'ipotesi in cui il reato non si sia completamente consumato - per mancato

compimento dell'azione, o per mancata verifica dell'evento - rimanendo allo stadio del solo tentativo (ricorrendo tali presupposti la pena inflitta alla persona fisica e le eventuali conseguenze sanzionatorie per la società, in presenza dei criteri di ascrizione della responsabilità subiranno soltanto una riduzione ex art. 26 d.lgs. 231/01).

#### **1.4 Criteri di imputazione e esclusione della responsabilità 231**

La responsabilità dell'ente si configura qualora:

- uno o più Reati Presupposto è stato commesso da un Soggetto Apicale o un Soggetto Subordinato
- e
- il fatto illecito sia stato commesso nell'interesse dell'ente, ovvero per favorire l'ente, indipendentemente dalla circostanza che tale obiettivo sia stato conseguito oppure
- il fatto illecito abbia portato un vantaggio all'ente a prescindere dall'intenzione di chi l'ha commesso

Gli art. 6 e 7 del Decreto prevedono forme specifiche di esonero da responsabilità degli enti.

Qualora il reato venga commesso da un soggetto apicale, il Decreto presuppone la responsabilità dell'ente, salvo che non venga dimostrato che:

- l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione e di gestione idoneo a prevenire reati della specie di quello verificatosi (Modello di Organizzazione, Gestione e Controllo – di seguito anche “Modello Organizzativo” o “Modello 231”)
- il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento è stato affidato a un organismo della società dotato di autonomi poteri di iniziativa e di controllo (Organismo di Vigilanza – di seguito anche “ODV”)
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione
- non vi è stata omessa o insufficiente vigilanza da parte ODV.

Nel caso di reato commesso da un Soggetto Subordinato, l'inosservanza degli obblighi di direzione o vigilanza e, quindi, la responsabilità dell'ente sono escluse se l'ente dimostra di aver adottato ed efficacemente attuato, prima della commissione del fatto, un Modello Organizzativo idoneo a prevenire reati della specie di quello verificatosi.

In altri termini, nei casi di reato commesso tanto da un soggetto apicale come da un soggetto subordinato, l'adozione e l'efficace attuazione del Modello 231 escludono la responsabilità dell'ente.

## 1.5 Le sanzioni

Il Decreto 231 prevede che agli enti possano essere applicate sanzioni pecuniarie e sanzioni interdittive. In particolare, nel settore finanziario è previsto l'intervento della Banca d'Italia sia con un ruolo di collaborazione con il pubblico ministero e con il giudice del procedimento penale, sia con l'incarico di porre in essere l'esecuzione delle eventuali sanzioni interdittive disposte nei confronti di un intermediario finanziario, di cui all'art. 9, comma 2, lettere a) – interdizione dall'esercizio dell'attività e b) – sospensione o revoca dall'autorizzazione.

Il Decreto prevede che le sanzioni pecuniarie siano sempre applicate in caso di accertata responsabilità dell'ente, a seguito di procedimento penale, e che tale applicazione avvenga per "quote", in numero non inferiore a cento e non superiore a mille. L'importo di ciascuna quota va da un minimo di Euro 258,00 ad un massimo di Euro 1.549,00. Il giudice, nel commisurare la sanzione pecuniaria applicabile, fissa l'importo della quota sulla base delle condizioni economiche e patrimoniali dell'ente in modo da rendere efficace la sanzione. L'Ente sarà tenuto a rispondere della sanzione pecuniaria entro i limiti del suo patrimonio.

Le sanzioni interdittive consistono in:

- interdizione dall'esercizio dell'attività
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito
- divieto di contrattare con la pubblica amministrazione
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi
- divieto di pubblicizzare beni o servizi

Mentre la sanzione pecuniaria si applica in ogni caso, la sanzione interdittiva si applica soltanto in relazione ai reati per i quali tale sanzione è espressamente prevista, in presenza di reiterazione dell'illecito o nel caso in cui l'ente abbia tratto un profitto rilevante dal reato la cui commissione è stata agevolata da gravi carenze organizzative dell'Ente.

Le sanzioni interdittive possono essere applicate all'ente sia all'esito del giudizio, sia in via cautelare, qualora vi siano (i) gravi indizi per ritenere la sussistenza della responsabilità dell'Ente per un illecito amministrativo dipendente da reato e (ii) fondati e specifici elementi che facciano ritenere l'esistenza del concreto pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

Con la sentenza di condanna nei confronti dell'ente è sempre disposta la confisca del prezzo o del profitto del reato. Nel caso in cui vengano comminate sanzioni interdittive, può essere disposta, come pena accessoria, anche la pubblicazione della sentenza di condanna.

Con specifico riferimento al settore finanziario, le sanzioni interdittive non possono essere applicate in via cautelare agli intermediari finanziari (SIM, SICAV; SGR). La stessa norma stabilisce, altresì, un flusso informativo tra il Pubblico Ministero che iscrive nel registro delle notizie di reato un illecito amministrativo a carico di un intermediario finanziario e la Banca d'Italia e la Consob, le quali possono essere sentite nel corso del procedimento ed hanno, in ogni caso la facoltà di presentare relazioni scritte.

## 1.6 Vicende societarie

Il D.Lgs. 231/2001 disciplina, inoltre, il regime della responsabilità patrimoniale dell'ente con riferimento a vicende modificative quali la trasformazione, la fusione, la scissione e la cessione d'azienda. In particolare, in caso di trasformazione, l'ente "trasformato" rimane responsabile anche per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto.

## 1.7 I reati commessi all'estero

In forza dell'art. 4 del Decreto, l'ente che abbia la propria sede principale nel territorio dello Stato può essere chiamato a rispondere innanzi al giudice penale italiano anche per reati commessi all'estero sia da soggetti apicali sia da soggetto sottoposti alla direzione di questi ultimi, se ricorrono le seguenti condizioni:

- l'ente ha in Italia la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, (enti dotati di personalità giuridica), ovvero il luogo in cui viene svolta l'attività in modo continuativo (enti privi di personalità giuridica)
- nei confronti dell'ente non stia procedendo lo Stato dove è stato commesso il fatto
- la richiesta del Ministro della giustizia è riferita anche all'ente medesimo.

Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità: "il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione" (art. 6 c.p.).

## 1.8 Gruppi di Società'

Il D.Lgs. 231/2001 non prende in considerazione esplicita i gruppi di società. Secondo l'interpretazione ormai costante della giurisprudenza, oggi fatto proprio anche da Confindustria nell'aggiornamento delle linee guida del 30 giugno 2021, non esiste un interesse di gruppo rilevante ai fini 231. Tuttavia, si ammette che la società controllante (holding) possa essere considerata responsabile per l'attività svolta da una controllata se (i) dalla condotta deriva un vantaggio diretto anche per la controllante e (ii) persone fisiche collegate in via funzionale alla controllante hanno partecipato alla condotta illecita recando un contributo causale dimostrabile.

## 2. L'ADOZIONE DEL MODELLO DA PARTE DI MONEYNET

### 2.1 Gli obiettivi perseguiti da Moneynet con l'adozione del Modello

Attraverso l'azione del Modello Moneynet S.p.A. (di seguito "Moneynet" o la "Società") intende:

- promuovere una cultura aziendale orientata all'eticità, alla correttezza, alla trasparenza e al rispetto delle norme
- evidenziare gli eventuali profili di rischio e assumere tutte le iniziative necessarie – mediante opportuni interventi – al fine di prevenire comportamenti illeciti di qualsiasi natura nello svolgimento della propria attività
- valorizzare i presidi e gli strumenti di controllo interno
- prevenire la commissione o la tentata commissione dei reati presupposto di cui al Decreto, esimando la Società dalla relativa responsabilità

Il presente Modello si integra all'interno della normativa, delle procedure e dei sistemi di controllo già esistenti ed operanti in Moneynet che incidono sul funzionamento della stessa e sul suo rapportarsi con la Pubblica Amministrazione.

Il contesto organizzativo della Società è costituito dall'insieme di regole, strutture e procedure che ne garantiscono il corretto funzionamento; si tratta dunque di un sistema estremamente articolato che rappresenta già di per sé uno strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli Enti.

Come anticipato, l'adozione del Modello non è obbligatoria; la scelta di Moneynet è fondata, tuttavia, sulla convinzione che l'efficacia di un idoneo Modello non rilevi solo in virtù della possibilità di esonero

dalla responsabilità dell'ente, ma migliori l'efficienza stessa dell'intero sistema societario, determinando, altresì, una maggiore competitività rispetto ai concorrenti.

## 2.2 Struttura e Componenti del Modello Organizzativo

Il Modello Organizzativo deve essere inteso come un sistema interno di gestione. Sostanzialmente, il Modello 231 è un sistema di organizzazione della compliance aziendale. Il presente documento rappresenta la descrizione di questo sistema nonché l'elemento formale della sua adozione.

Il sistema organizzativo 231, oltre al presente documento, si compone di tutte le procedure operative e gestionali adottate dalla Società e richiamate nel Modello. Si intendono parte integrante del Modello: il Codice Etico del Gruppo IVS (di seguito il "Codice Etico"), la documentazione redatta in ottemperanza alla normativa in materia di antiriciclaggio e antiterrorismo, di sicurezza sul lavoro ai sensi del D.Lgs. 81/2008, le procedure e istruzioni operative che regolano internamente l'attività della Società, la documentazione redatta in adeguamento alla normativa in materia di protezione dei dati personali (D.Lgs. 163/2006 e Gen. Reg. EU 2016/679 GDPR), ogni documento derivante dall'adempimento di disposizioni derivanti da leggi, regolamenti o prescrizioni da parte dell'Autorità.

La modalità di redazione del Modello 231 di Moneynet è basata sull'idea di approccio integrato nella valutazione e nella gestione del rischio in azienda. Questo approccio, condiviso dalle autorità ed esplicitato nelle linee guida di riferimento nella redazione dei Modelli 231, consente infatti, oltre a una razionalizzazione delle attività e dei costi, anche un concreto miglioramento delle attività di compliance e un elemento di facilitazione nella condivisione delle informazioni. Il risultato auspicato è quello di una mitigazione del rischio di informazioni parziali o disallineate su cui basare il risk assessment e al contempo di evitare duplicazioni e omissioni nella raccolta dei dati.

## 2.3 Destinatari

Le regole e le disposizioni del Modello si applicano e devono essere rispettate da tutti coloro che svolgono, anche di fatto, funzioni e prestazioni professionali nell'interesse della Società, nonché coloro i quali – pur non essendo ricompresi nell'organico – operano su mandato della medesima.

Si considerano quindi Destinatari del presente Modello:

- i componenti degli organi sociali
- i titolari di poteri di direzione, gestione e controllo di Moneynet (Presidente del CDA, Amministratori Delegati, Consiglieri Delegati)
- tutto il personale della Società, a prescindere dalla tipologia di rapporto contrattuale
- chiunque agisca in nome e per conto della Società sotto la sua direzione e vigilanza, a prescindere dal rapporto di subordinazione (per esempio i collaboratori a partita IVA).

Ai collaboratori esterni, ai consulenti, ai fornitori, ai partner commerciali e alle altre controparti contrattuali, Moneynet chiede il rispetto delle prescrizioni dettate dal Decreto e dei principi espressi nel Codice Etico tramite sottoscrizione di apposite clausole contrattuali.

## 2.4 Approccio Metodologico

Il presente Modello Organizzativo è stato redatto in linea con i requisiti previsti dal Decreto ed è stato impostato in modo da raggiungere lo scopo di un esaustivo risk assessment e di un'identificazione delle necessarie misure preventive e di controllo, tenendo presente le caratteristiche specifiche organizzative e di business di Moneynet.

In particolare, è stato dapprima analizzato il contesto nel quale inserire il risk assessment, ovvero la situazione organizzativa, gestionale, produttiva della Società, in modo da evidenziarne gli specifici processi nell'ambito dei quali identificare le attività sensibili rilevanti.

Quindi, si è proceduto all'attività di risk assessment, ovvero alla valutazione del rischio di commissione dei singoli Reati Presupposto (suddivisi per categoria come da Decreto) in relazione alle attività della Società. Questa analisi ha portato ad una "mappatura" (identificazione) dei rischi, alla quale fanno immediatamente riscontro le misure di gestione e controllo idonee a prevenire – nello specifico – il

rischio di commissione dei reati. In particolare, l'analisi dei processi e, all'interno dei singoli processi, delle attività cd. "sensibili" è stata effettuata prendendo in considerazione la possibilità concreta di commissione dei reati nella situazione specifica, anche alla luce dei meccanismi di controllo adottati.

## 2.5 Identificazione delle attività a rischio

Ai sensi dell'art. 6 del Decreto, che prevede l'identificazione delle attività nel cui ambito possono essere commessi i reati, la Società ha svolto un'analisi delle attività aziendali nonché dei processi di formazione delle decisioni e del sistema di controllo interno.

Tramite questa analisi sono stati individuati i soggetti, le attività e le categorie di operazioni per le quali esiste un rischio di commissione dei reati previsti dal Decreto.

I rischi individuati sono stati analizzati anche in funzione della probabilità di accadimento e dei controlli preventivi in essere; inoltre, ove ritenuto necessario, sono stati individuati gli eventuali opportuni adeguamenti al sistema di controllo.

Sulla base delle analisi di cui sopra ed in considerazione della struttura e delle attività svolte dalla Società, il management ha individuato come rilevanti i seguenti reati presupposto:

- Reati nei rapporti con la Pubblica Amministrazione – Art. 24
- Reati informatici e di trattamento illecito di dati – Art. 24 bis
- Reati di concussione, induzione indebita a dare o promettere utilità altrui e corruzione – Art. 25
- Reati societari – Art. 25 ter
- Delitti contro la personalità individuale – Art. 25 quinquies
- Reati di ricettazione e riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio – Art. 25 octies
- Reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria – Art. 25 decies
- Delitti in materia di strumenti di pagamento diversi dai contanti (Art. 25 octies-1), altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25 octies-2),

In relazione alla tipologia di business e alle attività svolte, nonché in base al risk assessment effettuato, il rischio relativo alla commissione dei seguenti reati è stato considerato remoto:

- delitti contro l'industria e il commercio;
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater), ;
- pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1),;
- delitti contro la personalità individuale;
- delitti in materia di violazione del diritto di autore;
- impiego di cittadini di paesi il cui soggiorno è irregolare;
- i reati ambientali;
- i reati di razzismo e xenofobia;
- i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati;
- il contrabbando;
- i delitti contro il patrimonio culturale.

Infine, le seguenti fattispecie di reato non risultano applicabili in quanto la Società non è soggetta alla normativa relativa alle società con titoli quotati in mercati regolamentati o diffusi tra il pubblico in misura rilevante o relativa alle società sottoposte a vigilanza ai sensi del Testo Unico della Finanza: gli abusi di mercato (art. 25-sexies, art.184 e 185 D.Lgs. n. 58/98), false comunicazioni sociali delle società quotate (art 25-ter e art.2622 c.c.) ed omessa comunicazione del conflitto d'interesse (art. 25-ter e art-2629-bis c.c.).

Il presente documento individua, nella successiva Parte Speciale, per ciascuna categoria di reati rilevanti per Moneynet, le attività della Società denominate sensibili a causa del rischio insito di commissione dei reati della specie di quelli qui elencati e prevede per ciascuna delle attività sensibili principi di prevenzione e presidi di controllo.

La Società valuta costantemente la rilevanza ai fini del Modello di eventuali ulteriori reati, sia già previsti sia di futura previsione nel Decreto.

## 2.6 Identificazione e analisi degli attuali presidi al rischio

Tale attività ha avuto lo scopo di individuare, tramite interviste dirette ai responsabili delle aree aziendali a rischio, le procedure operative e i concreti controlli esistenti e idonei a presidiare il rischio individuato. Anche il risultato di tale attività è stato documentato in schede e/o documenti.

## 2.7 Esiti Risk Assessment

L'attività di Risk Assessment, conclusasi a dicembre 2023, ha individuato le aree sensibili 231/01 e le attività potenzialmente collegate al rischio di commissione dei reati previsti dal Decreto Legislativo 231/01 (cd. «reati presupposto»). Poiché ad ogni attività può essere associato più di un reato presupposto, sono stati individuati i rischi 231.

A ciascuna attività mappata è stato associato un **rischio lordo**.

Sulla base della valutazione dei presidi e delle attività di mitigazione già poste in essere nella gestione dei processi, i **rischi netti** sono stati pertanto classificati come segue:

- **Non è stato individuato alcun rischio netto di livello ALTO.**
- **i rischi netti classificati di livello BASSO.** I controlli/presidi posti in essere dalla Società hanno determinato un sensibile abbassamento del rating del rischio lordo non richiedendo ulteriori attività di mitigazione;
- **i rischi netti classificati di livello MEDIO.** Sebbene il rischio lordo sia in parte mitigato dai presidi in essere, sono state identificate ulteriori attività di mitigazione e miglioramento.

Moneynet ha ritenuto pertanto che l'adozione del **Codice Etico**, dei principi generali di controllo interno, delle linee di condotta, delle specifiche procedure/policy e l'istituzione di dettagliati flussi informativi verso l'O.D.V., siano adeguati a prevenire le condotte illecite relative ai reati presupposti per tutti i rischi netti classificati di livello basso.

## 3. Redazione e diffusione del Modello organizzativo e gestionale

Nell'ultima fase, l'attività di Moneynet si è concentrata sulla redazione del Modello di Organizzazione e Gestione, la cui struttura verrà descritta al successivo paragrafo, unitamente alla diffusione del documento.

Al fine di renderlo concretamente applicato e rispettato, deve essere garantita la massima diffusione e conoscenza del Modello Organizzativo 231.

La Direzione provvede ad informare tutti i Destinatari dell'esistenza, della avvenuta adozione e del contenuto del presente Modello Organizzativo, con l'intento di renderne note le finalità e il carattere di cogenza. Al fine di garantire un'efficace e razionale attività di comunicazione, Moneynet promuove la conoscenza dei contenuti e dei principi del Modello e delle procedure di implementazione agli stessi applicabili, con grado di approfondimento diversificato a seconda della posizione assunta e del ruolo ricoperto.

Ai dipendenti e ai nuovi assunti viene consegnata copia del Codice Etico e viene garantita la possibilità di consultare il Modello 231 presente nel sistema informatico aziendale. In ogni caso, per i dipendenti che non hanno accesso alla rete intranet, tale documentazione viene messa a loro disposizione mediante l'affissione nelle bacheche aziendali. Inoltre, il Modello è consultabile in copia cartacea presso l'Ufficio Amministrativo.

Ai componenti degli organi sociali è resa disponibile copia cartacea della versione integrale del Modello e del Codice Etico al momento dell'accettazione della carica loro conferita e viene fatta loro sottoscrivere una dichiarazione di osservanza dei principi in essi contenuti. Idonei strumenti di comunicazione sono adottati in caso di aggiornamento della documentazione sulla base di ogni rilevante cambiamento procedurale, normativo o organizzativo.

Con riguardo alle controparti contrattuali e ai consulenti esterni, i contratti relativi a tali rapporti includono apposita clausola richiamante la conoscenza della normativa vigente in materia di responsabilità amministrativa della Società (con particolare riferimento alle previsioni del D.Lgs. 231/2001), nonché la dichiarazione relativa all'adozione ed attuazione di idonee procedure aziendali volte a prevenire la commissione dei reati di cui al Decreto.

### 3.1 La struttura del Modello della Società

Il Modello della Società contempla pertanto il coordinato funzionamento di un articolato sistema piramidale di principi e procedure che si può descrivere sinteticamente come segue:

- **Codice Etico:** è l'insieme dei principi generali (trasparenza, correttezza, lealtà) cui si ispira lo svolgimento e la conduzione degli affari nell'ambito di un più generale percorso di crescita sostenibile garantendo, nel contempo, l'efficienza e l'efficacia del Sistema di controllo interno. Moneynet ha ritenuto di adottare anche come proprio codice etico, il Codice Etico del Gruppo IVS.
- **Sistema di controllo interno:** è l'insieme degli "strumenti", attività, processi e strutture organizzative volti a fornire una ragionevole garanzia in ordine al raggiungimento degli obiettivi di efficienza e di efficacia operativa, affidabilità delle informazioni finanziarie e gestionali, rispetto delle leggi e dei regolamenti, nonché salvaguardia del patrimonio sociale anche contro possibili frodi. Il sistema di controllo interno si fonda e si qualifica su alcuni principi generali, appositamente definiti nell'ambito del Modello il cui campo di applicazione si estende trasversalmente a tutti i diversi livelli organizzativi (Amministratore Delegato, Direzione, Aree, Funzioni, Uffici).
- **Linee di condotta:** introducono regole specifiche al fine di evitare la costituzione di situazioni ambientali favorevoli alla commissione di reati in genere, e tra questi in particolare dei reati e degli illeciti amministrativi rilevanti ai sensi del Decreto. Talune regole sono altresì specifiche per la gestione dei rapporti con i rappresentanti della Pubblica Amministrazione e con i terzi in generale, nonché per gli adempimenti e le attività di natura societaria e di comunicazione al mercato.
- **Presidi organizzativi:** per lo più esplicitati nelle procedure adottate da Moneynet sono stati elaborati per tutti i processi operativi di medio rischio (l'attività di Risk Assessment 231 svolta ha infatti escluso, come detto, la presenza di processi di alto rischio netto) e per i processi strumentali. Tali schemi presentano un'analogia struttura che si sostanzia in un complesso di regole volte ad individuare le principali fasi di ogni processo, le specifiche attività di controllo per prevenire ragionevolmente i correlati rischi di reato, nonché appositi flussi informativi<sup>7</sup> verso l'Organismo di Vigilanza ("OdV", il cui ruolo è di seguito meglio dettagliato) al fine di evidenziare situazioni di eventuale inosservanza delle procedure stabilite nei modelli di organizzazione. Gli schemi di controllo interno sono stati elaborati alla luce di tre regole cardine e precisamente:

1. la **separazione dei ruoli** nello svolgimento delle attività inerenti ai processi;

2. la c.d. **“tracciabilità” delle scelte**, cioè la costante visibilità delle stesse (ad es. mediante apposite evidenze documentali), per consentire l’individuazione di precisi “punti” di responsabilità e la “motivazione” delle scelte stesse;
3. **l’oggettivazione dei processi decisionali**, nel senso di prevedere che, nell’assumere decisioni, si prescinda da valutazioni meramente soggettive, facendosi invece riferimento a criteri precostituiti.

L’Organismo di Vigilanza, il Collegio Sindacale, l’Internal Audit, la Compliance, nello svolgimento della propria attività e per quanto di propria competenza, hanno accesso diretto, completo, ed incondizionato a tutte le persone, attività, operazioni, documenti, archivi e beni aziendali.

### 3.2 Linee di condotta

Il presente paragrafo contiene le “Linee di Condotta” alle quali Amministratori, Sindaci, dirigenti, dipendenti, consulenti, collaboratori e in generale tutti coloro che operano per conto o in favore di Moneynet o che con lo stesso intrattengono relazioni di affari (“Destinatari delle Linee di Condotta”), ciascuno nell’ambito delle proprie funzioni e responsabilità, devono attenersi per evitare il determinarsi di situazioni ambientali favorevoli alla commissione di fatti illeciti in genere, e tra questi in particolare dei reati rilevanti ai sensi del Decreto.

Le Linee di Condotta individuano, se pur a titolo non esaustivo, comportamenti relativi all’area del “fare” e del “non fare”, con riferimento in particolare ai rapporti con la Pubblica Amministrazione, con i soggetti terzi, nonché alle attività e agli adempimenti societari, specificando in chiave operativa quanto espresso dai principi del Codice Etico.

#### “Area del fare”

I Destinatari delle Linee di Condotta sono impegnati al rispetto delle leggi e dei regolamenti vigenti in Italia. I Destinatari delle Linee di Condotta sono impegnati al rispetto delle procedure aziendali e si ispirano ai principi del Codice Etico in ogni decisione o azione attinente alla gestione della Società.

I responsabili delle aree devono curare che:

- per quanto ragionevolmente possibile, tutti i dipendenti siano edotti sulla normativa e sui comportamenti conseguenti e, qualora abbiano dei dubbi sulle modalità da seguire, siano adeguatamente indirizzati;
- sia attuato un adeguato programma di formazione e sensibilizzazione continua sulle problematiche attinenti al Codice Etico.

#### **Linee di Condotta nei rapporti con la P.A.**

Nell’eventuale partecipazione a gare indette dalla Pubblica Amministrazione e in generale in ogni trattativa con questa, i Destinatari delle Linee di Condotta devono operare nel rispetto delle leggi, dei regolamenti vigenti e della correttezza professionale.

I responsabili delle aree che hanno correntemente attività di contatto con la Pubblica Amministrazione devono:

- fornire ai propri collaboratori direttive sulle modalità di condotta operativa da seguire nei contatti formali ed informali intrattenuti con i diversi soggetti pubblici, secondo le peculiarità del proprio ambito di attività, trasferendo conoscenza della normativa e consapevolezza delle situazioni a rischio di reato;
- prevedere adeguati meccanismi di tracciabilità circa i flussi comunicativi/informativi verso la Pubblica Amministrazione.

Quando vengono richiesti allo Stato o ad altro ente pubblico o alle Comunità europee contributi, sovvenzioni o finanziamenti, tutti i Destinatari delle Linee di Condotta coinvolti in tali procedure devono:

- attenersi ai principi di correttezza, utilizzando e presentando dichiarazioni e documenti veritieri, completi e attinenti le attività per le quali i benefici possono essere legittimamente ottenuti;
- una volta ottenute le erogazioni richieste, destinarle alle finalità per le quali sono state richieste e concesse.

### **Linee di Condotta in materia societaria**

I componenti del Consiglio di Amministrazione, l'Amministratore Delegato, il Direttore Generale per quanto di rispettiva competenza, e le persone sottoposte alla loro vigilanza e, in generale, chiunque si occupi a qualunque titolo della redazione del bilancio sono tenuti alla piena osservanza della normativa aziendale e, in particolare, sono vincolati al rispetto delle procedure, delle istruzioni e delle norme operative di dettaglio in materia di redazione del bilancio e regolamentazione dei principali processi aziendali.

Il Responsabile dell'Area Amministrazione, nell'ambito dei compiti assegnati e per quanto di propria competenza, deve curare che ogni operazione sia:

- legittima, congrua, autorizzata e verificabile;
- correttamente ed adeguatamente registrata sì da rendere possibile la verifica del processo di decisione, autorizzazione e svolgimento;
- corredata di un supporto documentale idoneo a consentire, in ogni momento, i controlli sulle caratteristiche e motivazioni dell'operazione e l'individuazione di chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

I Destinatari delle Linee di Condotta coinvolti nelle attività di formazione del bilancio o di altri documenti simili devono comportarsi correttamente, prestare la massima collaborazione, garantire la completezza e la chiarezza delle informazioni fornite, l'accuratezza dei dati e delle elaborazioni, segnalare eventuali conflitti di interesse, ecc.

I componenti del Consiglio di Amministrazione, in conformità con quanto previsto dalla Procedura Conflitti d'interesse e operazioni con Parti Correlate adottata da Moneynet comunicano al CdA ed al Collegio Sindacale ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione della Società, precisandone la natura, i termini, l'origine e la portata; se si tratta di Direttore Generale, deve altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale.

I Destinatari delle Linee di Condotta e in particolare gli Amministratori:

- nella redazione del bilancio o di altri documenti simili devono rappresentare la situazione economica, patrimoniale o finanziaria con verità, chiarezza e completezza;
- devono rispettare puntualmente le richieste di informazioni da parte del Collegio Sindacale e facilitare in ogni modo lo svolgimento delle attività di controllo legalmente attribuite ai soci e ad altri organi sociali;
- fornire agli Organi di Vigilanza informazioni corrette e complete sulla situazione economica, patrimoniale o finanziaria.

Possono tenere contatti con la stampa solo i soggetti a ciò autorizzati e questi devono diffondere notizie sulla Società rispondenti al vero nel rispetto delle leggi e dei regolamenti vigenti.

### **Linee di Condotta nei rapporti con soggetti interni e terzi alla Società**

I Destinatari delle Linee di Condotta sono tenuti al rispetto delle leggi e dei regolamenti vigenti in Italia; non dovrà essere iniziato o proseguito alcun rapporto con chi non intenda rispettare tale principio.

L'incarico per operare in nome e/o per conto e/o nell'interesse della Società deve essere conferito in forma scritta e deve prevedere una specifica clausola che vincoli l'incaricato all'osservanza dei principi etico- comportamentali adottati dalla Società.

Il mancato rispetto di specifica clausola potrà permettere alla Società di risolvere il rapporto contrattuale. Tutti i consulenti, i fornitori e, in generale, qualunque soggetto terzo che agisca in nome e/o per conto e/o nell'interesse della Società sono individuati e selezionati con assoluta imparzialità, autonomia e indipendenza di giudizio. Nella loro selezione la Società ha cura di valutare la loro competenza, reputazione, indipendenza, capacità organizzativa e idoneità alla corretta e puntuale esecuzione delle obbligazioni contrattuali e degli incarichi affidati.

Tutti i consulenti e gli altri soggetti che prestano servizio presso la Società devono operare, sempre e senza eccezioni, con integrità e diligenza, nel pieno rispetto di tutti i principi di correttezza e liceità previsti dai codici etici dagli stessi eventualmente adottati.

### **“Area del non fare”**

È fatto divieto ai Destinatari delle Linee di Condotta di compiere, anche in forma associata, qualunque atto che sia o possa essere considerato contrario a leggi e/o a regolamenti vigenti, anche nel caso in cui da tale comportamento derivi o possa, anche solo in astratto, derivare un qualunque vantaggio o configurarsi un interesse per la Società.

I Destinatari delle Linee di Condotta sono tenuti a evitare qualunque situazione di conflitto di interessi con la Società, obbligandosi nel caso in cui la situazione di conflitto comunque si verifichi a segnalarlo immediatamente alla stessa Società.

I Destinatari delle Linee di Condotta devono astenersi da qualunque comportamento lesivo dell'immagine della Società.

### **Linee di Condotta nei rapporti con la P.A. e l'Unione Europea**

Nei rapporti con rappresentanti della Pubblica Amministrazione, sia italiani che esteri, è fatto divieto di:

- per i Consulenti e Collaboratori, promettere od offrire ai rappresentanti della P.A. o dell'Unione Europea (oppure a persone a questi “vicine” o “gradite”) denaro, doni o altra utilità in nome e/o per conto della Società;
- per gli Amministratori, Dipendenti e Dirigenti promettere od offrire ai rappresentanti della P.A. o dell'Unione Europea (oppure a persone a questi “vicine” o “gradite”) denaro, doni o altra utilità in elusione delle procedure societarie;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- promettere o fornire, anche tramite “terzi”, lavori/servizi di utilità personale (ad es. opere di ristrutturazione di edifici da loro posseduti o goduti – o posseduti o goduti da loro parenti, affini, conviventi amici, ecc.);
- fornire o promettere di fornire, sollecitare od ottenere informazioni e/o documenti riservati o comunque tali da poter compromettere l'integrità o la reputazione di una od entrambe le parti;
- favorire, nei processi d'acquisto, fornitori e sub-fornitori in quanto indicati dai rappresentanti stessi della Pubblica Amministrazione o dell'Unione Europea come condizione per lo svolgimento successivo delle attività (ad es. affidamento della commessa, concessione del finanziamento agevolato, concessione della licenza).

Tali azioni e comportamenti sono vietati se fatti sia direttamente dalla Società tramite i suoi dipendenti, sia tramite persone non dipendenti che agiscano in nome e/o per conto e/o nell'interesse di questa.

Inoltre, nei confronti della Pubblica Amministrazione o dell'Unione Europea, è fatto divieto di:

- esibire documenti/dati falsi od alterati;
- sottrarre od omettere documenti veri;
- tenere una condotta ingannevole che possa indurre la Pubblica Amministrazione in errore nella valutazione tecnico-economica dei prodotti e servizi offerti/forniti;
- omettere informazioni dovute, al fine di orientare indebitamente a proprio favore le decisioni della Pubblica Amministrazione o dell'Unione Europea;
- tenere comportamenti comunque intesi ad influenzare indebitamente le decisioni della Pubblica Amministrazione o dell'Unione Europea;
- abusare della posizione di incaricato di pubblico servizio per ottenere utilità a vantaggio personale o della Società;
- abusare della posizione di incaricato di pubblico servizio per indurre indebitamente altri a dare o promettere per sé o per altri denaro o altra utilità.

In conformità e nei limiti delle disposizioni normative vigenti, è fatto divieto di assumere o conferire incarichi di consulenza alle dipendenze della Società a ex dipendenti della Pubblica Amministrazione che abbiano partecipato personalmente e attivamente a una trattativa d'affari o abbiano avallato le richieste effettuate alla Pubblica Amministrazione o dell'Unione Europea dalla Società o da società controllate, collegate della medesima o sottoposte a comune controllo con la medesima.

Nel corso dei processi civili, penali o amministrativi, è fatto divieto di intraprendere, direttamente o indirettamente, alcuna azione illecita che possa favorire o danneggiare una delle parti in causa.

È fatto divieto a chiunque, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse della Società, di coartare la volontà dei Destinatari di rispondere all'Autorità giudiziaria o indurre di avvalersi della facoltà di non rispondere.

Nei rapporti con l'Autorità giudiziaria è vietata ogni forma di condizionamento che induca il Destinatario a rendere dichiarazioni non veritiere, in particolare in relazione alle dichiarazioni da rendere, al Destinatario non è consentito altresì accettare denaro o altra utilità, anche attraverso terzi.

### **Linee di Condotta nei rapporti con soggetti interni e terzi alla Società**

In generale è fatto divieto di:

- per i Consulenti e Collaboratori, promettere od offrire denaro, doni o altra utilità in nome e/o per conto della Società;
- per gli Amministratori, Dipendenti e Dirigenti promettere od offrire denaro, doni o altra utilità in elusione delle procedure societarie;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- promettere o fornire, anche tramite "terzi", lavori/servizi di utilità personale;
- fornire o promettere di fornire, sollecitare od ottenere informazioni e/o documenti riservati o comunque tali da poter compromettere l'integrità o la reputazione di una od entrambe le parti;
- favorire, nei processi d'acquisto, fornitori e sub-fornitori in quanto indicati dai soggetti come sopra individuati come condizione per lo svolgimento successivo delle attività (ad es. affidamento della commessa).

Tali azioni e comportamenti sono vietati se fatti sia direttamente dalla Società tramite i suoi dipendenti, sia tramite persone non dipendenti che agiscano in nome e/o per conto e/o nell'interesse di questa.

### **3.3 Principi generali dei presidi organizzativi**

Il sistema di controllo interno è definito come l'insieme dei "processi" presidiati dal Consiglio di Amministrazione, dal management e dagli altri membri della struttura aziendale, che si prefigge di fornire una ragionevole certezza in merito al conseguimento dei seguenti obiettivi:

- efficacia ed efficienza delle attività operative;
- affidabilità delle informazioni e del reporting economico/finanziario;
- conformità alle leggi, ai regolamenti alle norme e procedure interne;
- salvaguardia del patrimonio aziendale.

Il Sistema di Controllo Interno si articola in principi generali il cui campo di applicazione si estende con continuità attraverso i diversi livelli organizzativi.

### **Sistema delle deleghe e dei poteri**

I poteri di rappresentanza sono conferiti definendo i limiti in relazione alle dimensioni normali delle operazioni inerenti e secondo ambiti di esercizio strettamente collegati alle mansioni assegnate ed alla struttura organizzativa.

Le responsabilità devono essere definite e debitamente distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto.

Tutte le operazioni sono poste in essere secondo le modalità previste dai regolamenti interni ed in particolare dal sistema dei poteri e delle deleghe. I perimetri operativi di ciascuna area sono inoltre definiti ed esplicitati nella Relazione sulla Struttura Organizzativa che viene redatta con cadenza annuale secondo quanto previsto dalla normativa vigente.

### **Sistemi operativi**

I sistemi operativi devono essere coerenti con il Codice Etico.

In particolare, le informazioni finanziarie della Società devono essere predisposte:

- nel rispetto delle leggi e dei regolamenti, dei principi contabili statuiti e delle "best practice" internazionali;
- in coerenza con le procedure amministrative definite;
- nell'ambito di un completo ed aggiornato piano dei conti.

### **Valutazione dei rischi**

Gli obiettivi di ciascuna Area aziendale devono essere adeguatamente definiti e comunicati a tutti i livelli interessati per rendere chiaro e condiviso l'orientamento generale della stessa al fine anche di consentire l'individuazione dei rischi connessi al raggiungimento degli obiettivi, prevedendone periodicamente un adeguato monitoraggio ed aggiornamento.

Gli eventi negativi che possono minacciare la continuità operativa devono essere oggetto di apposita attività di valutazione dei rischi e di adeguamento delle protezioni.

I processi di innovazione relativi a prodotti/servizi, organizzazioni e sistemi devono prevedere un'adeguata valutazione dei rischi realizzativi.

### **Attività di controllo**

I processi operativi devono essere definiti prevedendo un adeguato supporto documentale (policy, norme operative, regolamenti interni, ecc.) e/o di sistema per consentire che siano sempre verificabili in termini di congruità, coerenza e responsabilità.

Le scelte operative devono essere tracciabili in termini di caratteristiche e motivazioni e devono essere individuabili coloro che hanno autorizzato, effettuato e verificato le singole attività.

Lo scambio di informazioni fra fasi/processi contigui deve prevedere meccanismi (riconciliazioni, quadrature, ecc.) per garantire l'integrità e la completezza dei dati gestiti.

Le risorse umane devono essere selezionate, assunte e gestite secondo criteri di trasparenza e in coerenza con i valori etici e gli obiettivi definiti dall'azienda.

Devono essere periodicamente analizzate le conoscenze e le competenze professionali disponibili nell'Area aziendale in termini di congruenza rispetto agli obiettivi assegnati.

Il personale deve essere formato e addestrato per lo svolgimento delle mansioni assegnate.

L'acquisizione di beni e servizi per il funzionamento aziendale deve avvenire sulla base di analisi dei fabbisogni e da fonti adeguatamente selezionate e monitorate.

## **Informazioni e Comunicazione**

Deve essere previsto un adeguato sistema di indicatori per processo/attività ed un relativo flusso periodico di reporting verso il management.

I Sistemi Informativi, amministrativi e gestionali devono essere orientati all'integrazione ed alla standardizzazione.

I meccanismi di sicurezza devono garantire un'adeguata protezione/accesso fisico-logico ai dati e ai beni dell'Unità Operativa, secondo il principio "need to know-need to do".

## **Monitoraggio**

Il sistema di controllo è soggetto ad attività di supervisione continua per valutazioni periodiche ed il costante adeguamento.

# **4 L'Organismo di Vigilanza**

## **4.1 Struttura e composizione dell'Organismo di Vigilanza**

L'Organismo di Vigilanza è una componente essenziale del Modello Organizzativo 231.

Il Decreto non fornisce indicazioni precise relativamente alla composizione dell'ODV, lasciando ai singoli enti la valutazione circa le relative caratteristiche. Pertanto, l'Organismo di Vigilanza deve essere costituito in modo che le finalità perseguite dalla legge siano assicurate dall'azione di un organo adatto in relazione alle dimensioni aziendali e alla complessità organizzativa.

Moneynet, in ragione della propria struttura e caratteristiche di business, ha optato per un Organismo di Vigilanza in forma monocratica. La nomina dello stesso avviene con delibera del Consiglio d'Amministrazione – previa verifica del possesso dei requisiti di legge da parte del professionista incaricato e dell'assenza di motivi di ineleggibilità –. In tale sede, sono deliberati anche l'emolumento del professionista che ha assunto l'incarico e l'accantonamento di un budget per eventuali spese sostenute dall'Organismo stesso per lo svolgimento della sua attività.

L'incarico conferito ha durata triennale, rinnovabile alla scadenza. L'incarico si intende rinnovato in assenza di delibere o dichiarazioni da parte dell'ODV di segno contrario. In caso di comunicazione di cessazione dall'incarico, l'organo amministrativo provvede alla relativa sostituzione con propria delibera. Fino alla nuova nomina, l'ODV garantisce la continuità della sua azione di vigilanza.

La revoca dell'incarico prima della scadenza potrà avvenire esclusivamente per giusta causa, intendendo compresi in tale concetto anche eventuali interventi di ristrutturazione della Società, mediante apposita delibera e sentito il Collegio Sindacale.

L'Organismo di Vigilanza di Moneynet ha adottato un proprio regolamento, che si intende parte integrante del presente Modello. Il Regolamento prevede nel dettaglio le modalità di funzionamento dell'ODV e di scambio dei flussi informativi con la Società.

## 4.2 Requisiti

### ➤ **Requisiti soggettivi di eleggibilità**

La nomina quale componente dell'OdV è condizionata alla presenza dei requisiti soggettivi di eleggibilità.

Costituiscono motivi di ineleggibilità e/o di decadenza dei componenti dell'OdV di Moneynet:

- trovarsi in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del codice civile;
- avere titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza su Moneynet;
- essere stato sottoposto a misure di prevenzione ai sensi del decreto legislativo 6 settembre 2011, n. 159 e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- aver riportato sentenza di condanna o patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
- per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267 (legge fallimentare);
- per uno dei delitti previsti dal titolo XI del Libro V del codice civile (società e consorzi);
- per un delitto non colposo, per un tempo non inferiore a un anno;
- per un delitto contro la P.A., contro la fede pubblica, contro il patrimonio, contro l'economia pubblica ovvero per un delitto in materia tributaria;
- per uno dei reati previsti dalle norme che disciplinano l'attività Societaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
- aver riportato, in Italia o all'estero, sentenza di condanna o di patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex D.Lgs. 231/01;
- essere destinatario di un decreto che dispone il rinvio a giudizio per tutti i reati/illeciti previsti dal D.Lgs. 231/01;
- aver svolto funzioni di amministratore esecutivo ricoperte, nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese:
  - sottoposte a procedure concorsuali;
  - operanti nel settore creditizio, finanziario, mobiliare e assicurativo sottoposte a procedure di liquidazione coatta amministrativa o amministrazione straordinaria.

### ➤ **Autonomia e indipendenza**

L'autonomia e l'indipendenza dell'OdV sono garantite:

- dal posizionamento, indipendente da qualsiasi area, all'interno della struttura organizzativa aziendale;
- dal possesso dei requisiti di indipendenza, onorabilità e professionalità dei membri dell'OdV;
- dalle linee di riporto verso il Vertice aziendale attribuite all'OdV;
- dalla insindacabilità, da parte di alcun altro organismo o struttura aziendale, delle attività poste in essere dall'OdV;

- dall'autonomia nello stabilire le proprie regole di funzionamento mediante l'adozione di un proprio Regolamento.

L'OdV dispone di autonomi poteri di spesa sulla base di un budget, approvato dal Consiglio di Amministrazione, su proposta dell'OdV stesso. In ogni caso, quest'ultimo può richiedere un'integrazione del budget assegnato, qualora non sufficiente all'efficace espletamento delle proprie incombenze, e può estendere la propria autonomia di spesa di propria iniziativa in presenza di situazioni eccezionali o urgenti, che saranno oggetto di successiva relazione al Consiglio di Amministrazione.

All'OdV e alla struttura della quale esso si avvale sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli.

Nell'esercizio delle loro funzioni l'OdV non deve trovarsi in situazioni, anche potenziali, di conflitto di interesse con Moneynet derivanti da qualsivoglia ragione (ad esempio di natura personale o familiare). In tali ipotesi essi sono tenuti ad informare immediatamente gli altri membri dell'OdV e devono astenersi dal partecipare alle relative deliberazioni.

#### ➤ **Professionalità**

L'OdV deve essere composto da soggetti dotati di adeguata esperienza aziendale e delle cognizioni tecniche e giuridiche necessarie per svolgere efficacemente le attività proprie dell'Organismo.. Ove necessario, l'OdV può avvalersi, con riferimento all'esecuzione delle operazioni tecniche necessarie per lo svolgimento della funzione di controllo, anche di consulenti esterni. In tal caso, i consulenti dovranno sempre riferire i risultati del loro operato all'OdV.

#### ➤ **Continuità di azione**

L'OdV deve essere in grado di garantire la necessaria continuità nell'esercizio delle proprie funzioni, anche attraverso la programmazione e pianificazione dell'attività e dei controlli, la verbalizzazione delle riunioni e la disciplina dei flussi informativi provenienti dalle strutture aziendali.

### **4.3 Revoca**

I membri dell'OdV possono essere revocati dal Consiglio di Amministrazione solo per giusta causa. La deliberazione di revoca è portata a conoscenza e sottoposta al previo assenso del Collegio Sindacale.

A tale proposito, per "giusta causa" di revoca si intende, a titolo esemplificativo e non limitativo:

- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico;
- l'"omessa o insufficiente vigilanza" da parte dell'OdV – secondo quanto previsto dall'art. 6, comma 1, lett. d), D.Lgs. 231/01 – risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti di Moneynet ai sensi del D.Lgs. 231/01 ovvero da sentenza di applicazione della pena su richiesta (il c.d. patteggiamento);
- l'accertamento, successivo alla nomina, che il membro dell'OdV abbia rivestito la qualifica di componente dell'OdV in seno a società nei cui confronti siano state applicate, con provvedimento definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del D.Lgs. 231/01), le sanzioni previste dall'art. 9 del del D.Lgs. 231/01, per illeciti commessi durante la loro carica;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'OdV.

In ogni caso qualsiasi provvedimento di disposizione di carattere organizzativo che riguardi un membro dell'OdV (ad es. cessazione rapporto di lavoro, spostamento ad altro incarico, licenziamento,

provvedimenti disciplinari, nomina di nuovo responsabile) dovrà essere portato alla presa d'atto del Consiglio di Amministrazione per il tramite del Presidente dell'OdV;

#### **4.4 Cause di sospensione**

Costituisce causa di sospensione dalla funzione di componente dell'OdV l'accertamento, dopo la nomina, che i componenti dell'Organismo di Vigilanza hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, con provvedimento non definitivo, le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica.

I componenti dell'OdV debbono comunicare al CdA, sotto la loro piena responsabilità, il sopravvenire della causa di sospensione di cui sopra. Il CdA, anche in tutti gli ulteriori casi in cui viene direttamente a conoscenza del verificarsi della suddetta causa, provvede a dichiarare la sospensione del soggetto (o dei soggetti) dalla carica di componente dell'OdV.

La decisione sulla eventuale revoca dei membri sospesi deve essere oggetto di deliberazione del CdA. Il componente non revocato è reintegrato nel pieno delle funzioni.

#### **4.5 Temporaneo impedimento**

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, ad un componente dell'OdV di svolgere le proprie funzioni o svolgerle con la necessaria autonomia ed indipendenza di giudizio, questi è tenuto a dichiarare la sussistenza dell'impedimento e, qualora esso sia dovuto ad un potenziale conflitto di interessi, la causa da cui il medesimo deriva, astenendosi dal partecipare alle sedute dell'Organismo o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso. A titolo esemplificativo, costituisce causa di temporaneo impedimento la malattia o l'infortunio che si protraggano per oltre tre mesi ed impediscano di partecipare alle riunioni dell'OdV.

Nel caso di temporaneo impedimento o in ogni altra ipotesi che determini per uno o più componenti l'impossibilità di partecipare alla riunione, l'Organismo opererà nella sua composizione ridotta, sempre che il numero dei rimanenti componenti (per i quali non sussistano le predette situazioni) non sia inferiore a tre, qualora tra questi vi sia il Presidente. In assenza del Presidente, il numero minimo dei componenti non potrà essere inferiore a due.

In tutto gli altri casi, il CdA dispone l'integrazione temporanea dell'Organismo di Vigilanza, nominando uno o più membri nel corso della prima seduta utile, il cui incarico avrà una durata pari al periodo di impedimento. Resta salva la facoltà per il CdA, quando l'impedimento si protragga per un periodo superiore a sei mesi, prorogabile di ulteriori 6, di addivenire alla revoca del o dei componenti per i quali si siano verificate le predette cause di impedimento.

#### **4.6 Definizione dei compiti e dei poteri dell'Organismo di Vigilanza**

L'attività di verifica e di controllo svolta dall'OdV è strettamente funzionale agli obiettivi di efficace attuazione del Modello e non va a surrogare o sostituire le funzioni di controllo istituzionali di Moneynet.

I compiti dell'OdV sono espressamente definiti dal D.Lgs. 231/01 al suo art. 6, comma 1, lett. b) come segue:

- vigilare su funzionamento e osservanza del Modello;
- curarne l'aggiornamento.

In adempimento a siffatti compiti, all'OdV sono affidate le seguenti attività:

- vigilare sul funzionamento del Modello rispetto alla prevenzione della commissione dei reati richiamati dal D.Lgs. 231/01;
- verificare il rispetto del Modello e dei protocolli decisionali, rilevando gli eventuali comportamenti anomali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i destinatari del Modello;
- svolgere periodica attività ispettiva e di controllo, di carattere continuativo e ogni volta lo ritenga necessario, in considerazione dei vari settori di intervento o delle tipologie di attività e dei loro punti critici al fine di verificare l'efficienza e l'efficacia del Modello;

Inoltre, con specifico riguardo alla disciplina sul sistema interno di segnalazione (cd. "whistleblowing"):

- verificare l'adeguatezza dei canali informativi, predisposti in applicazione della disciplina sul whistleblowing, affinché gli stessi siano tali da assicurare la corretta segnalazione dei reati o delle irregolarità da parte dei dipendenti della società e nell'assicurare la riservatezza di questi ultimi nell'intero processo di gestione della segnalazione;
- verificare il soddisfacimento dell'adozione del canale informatico di cui alla lettera b) del nuovo comma 2-bis dell'art. 6 Decreto 231;
- gestire il processo di analisi e valutazione della segnalazione;
- vigilare sul rispetto del divieto di "atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione" (art. 6, comma 2-bis, lett. c, del Decreto 231), che la nuova disciplina correda di un impianto sanzionatorio da integrare nel sistema disciplinare ex art. 6, comma 2, lett. e, del Decreto 231.
- vigilare sul corretto utilizzo dei canali informativi da parte dei segnalanti.

Nello svolgimento delle proprie attività, l'OdV può:

- accedere liberamente, anche per il tramite di strutture appositamente incaricate, a qualsiasi struttura di Moneynet – senza necessità di alcun consenso preventivo – per richiedere ed acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei propri compiti. Nel caso in cui venga opposto un motivato diniego all'accesso agli atti, l'OdV redige, qualora non concordi con la motivazione opposta, un rapporto da trasmettere al CdA;
- richiedere informazioni rilevanti o l'esibizione di documenti, anche informatici, pertinenti alle attività a rischio, agli amministratori, agli organi di controllo, alle società di revisione, ai collaboratori, ai consulenti ed in generale a tutti coloro che operano per conto di Moneynet;
- sviluppare e promuovere il costante aggiornamento del Modello, inclusa l'identificazione, la mappatura e la classificazione delle attività a rischio formulando, ove necessario, al CdA le proposte per eventuali integrazioni e adeguamenti che si dovessero rendere necessari in conseguenza di:
  - significative violazioni delle prescrizioni del Modello;
  - significative modificazioni dell'assetto interno di Moneynet e/o delle modalità di svolgimento dell'impresa;
- modifiche legislative al D.Lgs. 231/01, quali ad esempio introduzione di fattispecie di reato che potenzialmente hanno un impatto sul Modello della Società;
- definire e curare il flusso informativo che consenta all'OdV di essere periodicamente aggiornato dai referenti aziendali, al fine di individuare possibili carenze nel funzionamento del Modello e/o possibili violazioni dello stesso;
- attuare un efficace flusso informativo che consenta all'OdV di riferire agli organi sociali competenti in merito all'efficacia e all'osservanza del Modello;
- verificare la predisposizione di un efficace sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del D.Lgs. 231/01, garantendo la tutela e riservatezza del segnalante e promuovendo la conoscenza delle condotte che devono essere segnalate e le modalità di effettuazione delle segnalazioni;
- promuovere iniziative per la diffusione della conoscenza e della comprensione del Modello, dei contenuti del D.Lgs. 231/01, degli impatti della normativa sull'attività della Società, nonché

iniziative per la formazione del personale e la sensibilizzazione dello stesso all'osservanza del Modello;

- promuovere e coordinare le iniziative volte ad agevolare la conoscenza e la comprensione del Modello da parte di tutti coloro che operano per conto di Moneynet;
- fornire pareri in merito al significato ed all'applicazione delle previsioni contenute nel Modello, alla corretta applicazione dei protocolli e delle relative procedure di attuazione;
- formulare e sottoporre all'approvazione dell'organo dirigente la previsione di spesa necessaria al corretto svolgimento dei compiti assegnati, con assoluta indipendenza;
- segnalare tempestivamente all'organo dirigente, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo a Società e proporre le eventuali sanzioni;
- verificare l'idoneità del sistema disciplinare ai sensi e per gli effetti del D.Lgs. 231/01.

Nello svolgimento della propria attività, l'OdV, si avvale di una struttura organizzativa dedicata come definita in normativa interna e può ricorrere ad ogni altra struttura interna della società competente per le attività e/o i settori di intervento.

Il CdA dà incarico all'OdV di curare l'adeguata comunicazione alle strutture aziendali del Modello, dei compiti dell'OdV e dei suoi poteri.

I componenti dell'OdV, nonché i soggetti dei quali l'OdV stesso, a qualsiasi titolo, si avvale, sono tenuti a rispettare l'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni (fatte salve le attività di reporting al CdA).

I componenti dell'OdV assicurano la riservatezza delle informazioni di cui vengano in possesso, in particolare se relative a segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello. I componenti dell'Organismo di Vigilanza si astengono dal ricevere e utilizzare informazioni riservate per fini diversi da quelli compresi nel presente paragrafo, e comunque per scopi non conformi alle funzioni proprie dell'Organismo di Vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.

Ogni informazione in possesso dei componenti dell'OdV deve essere comunque trattata in conformità con la vigente legislazione in materia e, in particolare, in conformità al Regolamento (UE) 2016/679 (General Data Protection Regulation, cd G.D.P.R.)

Ogni informazione, segnalazione, report, relazione previsti nel Modello sono conservati dall'OdV in un apposito archivio (informatico e/o cartaceo).

#### **4.7 Reporting dell'Organismo di Vigilanza**

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'OdV relaziona direttamente al CdA della Società.

L'OdV riferisce al CdA almeno annualmente, nella fase di approvazione del bilancio, in merito:

- agli esiti dell'attività di vigilanza espletata nel periodo di riferimento, con l'indicazione di eventuali problematiche o criticità emerse e degli interventi opportuni sul Modello;
- agli eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno di Moneynet e/o delle modalità di svolgimento delle attività, che richiedono aggiornamenti del Modello (tale segnalazione ha luogo qualora non si sia previamente proceduto a sottoporla al CdA al di fuori della relazione annuale);
- al resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del Modello e dei protocolli, nonché all'esito delle conseguenti verifiche effettuate;
- ai provvedimenti disciplinari ed alle sanzioni eventualmente applicate da Moneynet con riferimento alle violazioni delle previsioni del Modello e dei protocolli;
- al rendiconto delle spese sostenute;
- alle attività pianificate cui non si è potuto procedere per giustificate ragioni di tempo e risorse;

- al piano delle verifiche predisposto per l'anno successivo.

L'OdV potrà in ogni momento chiedere di essere sentito dal CdA qualora accerti fatti di particolare rilevanza, ovvero ritenga opportuno un esame o un intervento in materie inerenti il funzionamento e l'efficace attuazione del Modello.

A garanzia di un corretto ed efficace flusso informativo, l'OdV ha inoltre la possibilità, al fine di un pieno e corretto esercizio dei propri poteri, di chiedere chiarimenti o informazioni direttamente all'Amministratore Delegato.

L'OdV può, a sua volta, essere convocato in ogni momento dal CdA per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del Modello.

#### **4.8 Flussi informativi nei confronti dell'Organismo di Vigilanza**

L'Organismo di Vigilanza deve essere tempestivamente informato, mediante apposito sistema di comunicazione in merito a quegli atti, comportamenti od eventi che possono determinare una violazione del Modello o che, più in generale, sono rilevanti ai fini del d.lgs. n. 231/2001.

L'obbligo di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello rientra nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro.

**I Destinatari delle Linee di Condotta hanno l'obbligo di segnalare all'Organismo di Vigilanza ogni violazione o sospetta violazione delle Linee di Condotta e del Modello, come di seguito meglio specificato.**

L'Organismo di Vigilanza valuta tutte le segnalazioni ricevute e intraprende le conseguenti iniziative a sua ragionevole discrezione e responsabilità nell'ambito delle proprie competenze, ascoltando eventualmente l'autore della segnalazione ed il responsabile della presunta violazione. Ogni conseguente decisione sarà motivata; gli eventuali provvedimenti conseguenti potranno costituire inadempimento alle obbligazioni primarie del rapporto di lavoro e/o contrattuale, con la possibilità di irrogazione nei confronti dei responsabili di misure sanzionatorie secondo le modalità previste da leggi, accordi collettivi, contratti.

L'OdV agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti comunque salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente o in mala fede.

I flussi informativi hanno pertanto ad oggetto tutte le informazioni e tutti i documenti che devono pervenire all'OdV al fine di consentire a quest'ultimo di aumentare il livello di conoscenza della Società, di acquisire informazioni atte a valutare la rischiosità insita in taluni processi sensibili, nonché di svolgere le proprie attività di verifica e di vigilanza in merito all'efficacia e all'osservanza del Modello.

I protocolli decisionali, le Procedure e le Policy - che costituiscono parte integrante del Modello - prevedono obblighi informativi relativi ai processi e alle attività sensibili e gravanti in generale sui destinatari del Modello (es. modifiche alle attività sensibili, anomalie di processo, rilievi di audit, informazioni rilevanti).

Sono stati inoltre identificati flussi informativi originati dalle funzioni di controllo e da altre strutture della Società che, in forza delle proprie attribuzioni, svolgono attività rilevanti ai fini del D. Lgs. n. 231/01.

A titolo esemplificativo i flussi informativi includono:

- operazioni che ricadano nella attività sensibili (ad es. prospetti periodici riepilogativi sulle convenzioni stipulate con Soggetti Pubblici, informazioni relative a nuove assunzioni di

personale o utilizzo di risorse finanziarie per l'acquisto di beni e servizi o altre attività di investimento, etc...);

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D. Lgs. 231/01 e che possano coinvolgere Moneynet;
- richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui D. Lgs. 231/01 e che possano coinvolgere Moneynet;
- i documenti predisposti dalle strutture di controllo (ad esempio Internal Audit, Compliance e Antiriciclaggio, Risk Management) nell'ambito delle loro attività di verifica, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D. Lgs. 231/01 o delle previsioni del Modello e dei protocolli di decisione;
- la pianificazione e le relazioni annuali delle attività svolte dalle funzioni di controllo;
- le contestazioni per omessa segnalazione di operazione sospetta ai sensi della normativa antiriciclaggio;
- la lettera annuale della società di revisione con evidenza delle eventuali anomalie rilevate nel processo di redazione del Bilancio Consolidato e del Bilancio d'Esercizio di Moneynet e l'evidenza periodica circa il monitoraggio delle azioni correttive;
- l'informativa sull'esercizio delle deleghe e delle sub-deleghe da parte delle strutture della Società e l'aggiornamento del sistema delle procure aziendali;
- le visite, le ispezioni e gli accertamenti avviati da parte degli enti competenti (a titolo meramente esemplificativo Guardia di Finanza, INPS, INAIL ecc.) o da parte di Autorità di Vigilanza e, alla loro conclusione, i relativi esiti;
- la reportistica in materia di salute e sicurezza sul lavoro incluse le segnalazioni di incidenti/infortuni, anche derivanti da fattori esterni (es. rapine), che hanno comportato lesioni gravi o gravissime a dipendenti e/o a terzi;
- i procedimenti disciplinari avviati per violazioni del Modello e dei protocolli di decisione, l'applicazione di sanzioni ovvero i provvedimenti di archiviazione di tali procedimenti e le relative motivazioni;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.Lgs. 231/01 e che possano coinvolgere Moneynet;
- i contenziosi aventi come controparte enti o soggetti pubblici (o soggetto equiparato) e, alla loro conclusione, i relativi esiti;
- le sentenze di condanna di dipendenti Moneynet a seguito del compimento di reati rientranti tra quelli presupposto del D.Lgs. 231/01.

Per quanto concerne consulenti o collaboratori esterni, è contrattualmente previsto un obbligo di informativa immediata a loro carico nel caso in cui gli stessi ricevano, direttamente o indirettamente, da un dipendente di Moneynet una richiesta di comportamenti che potrebbero determinare una violazione del Modello.

Nel normale svolgimento delle proprie funzioni e in ragione di considerazioni "*risk-based*", l'OdV si riserva, qualora lo ritenga opportuno, di richiedere qualsiasi informazione necessaria per l'esecuzione delle sue funzioni.

Il corretto adempimento dell'obbligo di informazione da parte del prestatore di lavoro non può dar luogo all'applicazione di sanzioni disciplinari.

Le informazioni di cui sopra possono essere segnalate all'OdV tramite una delle seguenti modalità:

Casella di posta elettronica riservata:

- Organismo di Vigilanza (odv@moneynet.it)

Forma cartacea al seguente indirizzo:

Moneynet - Organismo di Vigilanza 231/01

All'attenzione del Presidente dell'Organismo di Vigilanza  
Viale Aiace, 132  
90151 Palermo (PA)

## **5. La diffusione del Modello e la formazione**

Al fine di renderlo concretamente applicato e rispettato, deve essere garantita la massima diffusione e conoscenza del Modello Organizzativo 231.

La Direzione provvede ad informare tutti i Destinatari dell'esistenza, della avvenuta adozione e del contenuto del presente Modello Organizzativo, con l'intento di renderne note le finalità e il carattere di cogenza. Al fine di garantire un'efficace e razionale attività di comunicazione, Moneynet promuove la conoscenza dei contenuti e dei principi del Modello e delle procedure di implementazione agli stessi applicabili, con grado di approfondimento diversificato a seconda della posizione assunta e del ruolo ricoperto.

Ai dipendenti e ai nuovi assunti viene consegnata copia del Codice Etico e viene garantita la possibilità di consultare il Modello 231 presente nel sistema informatico aziendale. In ogni caso, per i dipendenti che non hanno accesso alla rete intranet, tale documentazione viene messa a loro disposizione mediante allegazione al cedolino paga o con l'affissione nelle bacheche aziendali. Inoltre, il Modello è consultabile in copia cartacea presso l'Ufficio Amministrativo.

Ai componenti degli organi sociali è resa disponibile copia cartacea della versione integrale del Modello e del Codice Etico al momento dell'accettazione della carica loro conferita e viene fatta loro sottoscrivere una dichiarazione di osservanza dei principi in essi contenuti. Idonei strumenti di comunicazione sono adottati in caso di aggiornamento della documentazione sulla base di ogni rilevante cambiamento procedurale, normativo o organizzativo.

Con riguardo alle controparti contrattuali e ai consulenti esterni, i contratti relativi a tali rapporti includono apposita clausola richiamante la conoscenza della normativa vigente in materia di responsabilità amministrativa della Società (con particolare riferimento alle previsioni del D.Lgs. 231/2001), nonché la dichiarazione relativa all'adozione ed attuazione di idonee procedure aziendali volte a prevenire la commissione dei reati di cui al Decreto. Copia del Codice Etico di Moneynet viene messa a disposizione degli stessi secondo le modalità opportune sulla base del caso concreto..

### **5.1 L'attività formativa 231**

L'attività di formazione, oggetto di pianificazione su base annuale di concerto con l'ODV, è articolata in relazione alla qualifica dei Destinatari, al livello di rischio dell'area in cui operano, nonché all'avere o meno essi funzioni di rappresentanza e/o amministrazione.

L'informazione sui contenuti del Modello e dei principi contenuti nel Codice Etico deve essere effettuata su base continuativa ed estesa ad ogni nuova circostanza rilevante

effettuata ex novo nei confronti dei lavoratori nuovi assunti al momento del loro inserimento rinnovata periodicamente nei confronti dei lavoratori che già prestano attività professionale per Moneynet.

Le registrazioni delle suddette attività formative devono essere archiviate, con la firma di tutti i presenti. L'Organismo di Vigilanza monitora il livello di recepimento del Modello attraverso periodiche specifiche verifiche.

## 6. Il sistema sanzionatorio

L'efficace attuazione del Modello necessita di un adeguato sistema sanzionatorio. Ai sensi del Decreto, il Modello può ritenersi efficacemente attuato solo qualora preveda un sistema disciplinare diretto a sanzionare il mancato rispetto delle regole e dei principi in esso contenute.

I requisiti indispensabili del sistema sanzionatorio sono:

- specificità ed autonomia: con specificità si intende la predisposizione di un sistema sanzionatorio interno alla Società avente scopo di sanzionare ogni violazione del Modello. Con autonomia si fa riferimento all'autosufficienza del funzionamento del sistema disciplinare interno. Moneynet ha l'obbligo di sanzionare la violazione indipendentemente dall'andamento dell'eventuale procedimento giudiziario in corso a carico dell'autore persona fisica
- compatibilità: il procedimento di accertamento e di applicazione della sanzione disciplinare nonché la sanzione stessa non possono essere in contrasto con le norme di legge e con quelle contrattuali che regolano il rapporto di lavoro in essere con la Società
- idoneità: il sistema disciplinare deve essere efficiente ed efficace per la prevenzione della commissione di reati
- proporzionalità: la sanzione deve essere proporzionata alla violazione rilevata e alla tipologia di rapporto di lavoro instaurato con il prestatore (subordinato, parasubordinato, dirigenziale, ecc.);
- redazione per iscritto ed idonea divulgazione: il sistema sanzionatorio va redatto per iscritto e deve essere oggetto di informazione e formazione puntuale verso i Destinatari.

### 6.1 Destinatari del sistema sanzionatorio

I destinatari del sistema disciplinare corrispondono ai Destinatari del Modello 231. I Destinatari hanno l'obbligo di uniformare la propria condotta ai principi sanciti nel Codice Etico, nonché a tutti gli standard organizzativi e di comportamento definiti nel Modello.

### 6.2 Principi generali relativi alle sanzioni

Le sanzioni previste saranno applicate ad ogni violazione delle disposizioni contenute nel Codice Etico e nel Modello 231 complessivamente inteso a prescindere dalla commissione di un reato e dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria.

Costituisce, altresì, violazione del Modello – e presupposto di applicazione di sanzioni - il mancato rispetto degli obblighi di riservatezza sull'identità del segnalante previsti dalla normativa in materia di tutela del segnalante di comportamenti illegittimi (whistleblowing) a tutela del dipendente o collaboratore che segnala illeciti, nonché il compimento di segnalazioni effettuate con dolo o colpa grave, che si rivelino infondate.

Per la contestazione, l'accertamento delle infrazioni e l'applicazione di sanzioni disciplinari restano validi i poteri già conferiti, nei limiti delle rispettive deleghe e competenze, nell'ambito dell'organizzazione interna di Moneynet.

In caso di segnalazione all'Organismo di Vigilanza, quest'ultimo, svolti gli opportuni accertamenti, formula una proposta in merito ai provvedimenti da adottare e comunica la propria valutazione agli organi aziendali competenti.

In ogni caso, le fasi di contestazione della violazione, nonché quelle di determinazione ed effettiva applicazione delle sanzioni, sono svolte nel rispetto delle norme di legge e di regolamento vigenti, nonché delle previsioni della contrattazione collettiva e dei Codici Disciplinari aziendali.

Le sanzioni relative devono rispettare il principio di gradualità e di proporzionalità rispetto alla gravità delle violazioni. La determinazione della tipologia, così come dell'entità della sanzione deve considerare:

- la gravità dell'inadempimento
- la posizione rivestita dal soggetto agente all'interno dell'organizzazione aziendale, anche in considerazione delle responsabilità connesse alle sue mansioni
- eventuali circostanze aggravanti e/o attenuanti che possano essere rilevate in relazione al

comportamento tenuto dal Destinatario.

### 6.3 Sanzioni relative al personale dipendente

Assumono rilievo gli illeciti disciplinari relativi al personale dipendente derivanti da:

- mancato rispetto delle procedure e/o prescrizioni del Modello dirette a garantire lo svolgimento dell'attività in conformità della legge e ad eliminare tempestivamente situazioni di rischio, ai sensi del Decreto
- violazione e/o elusione dei sistemi di controllo interno, posta in essere mediante la sottrazione, la distruzione o l'alterazione di documentazione ovvero mediante impedimento del controllo o dell'accesso alle informazioni ed alla documentazione ai soggetti preposti al controllo, incluso l'ODV
- inosservanza delle regole contenute nel Codice Etico
- inosservanza degli obblighi di informativa all'ODV e/o al diretto superiore gerarchico
- omessa vigilanza, secondo i compiti e le responsabilità come definiti dall'organizzazione interna aziendale, sul rispetto delle procedure e delle prescrizioni del Modello da parte dei propri sottoposti, nell'ambito delle aree sensibili a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio-reato
- inosservanza degli obblighi di comportamento in materia di salute e sicurezza sul lavoro come disciplinati dalla legge (D.lgs. 81/2008), regolamenti e/o altre disposizioni aziendali

Le sanzioni nei confronti dei dipendenti rientrano in quelle previste dal sistema disciplinare aziendale e/o dal sistema sanzionatorio previsto dal CCNL, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori ed eventuali normative speciali applicabili. Per il personale dipendente, in applicazione del Contratto Collettivo Nazionale di Lavoro, si prevedono le seguenti sanzioni:

- richiamo verbale
- ammonizione scritta
- multa non superiore a 3 ore di retribuzione oraria calcolata sul minimo tabellare
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di 3 giorni
- licenziamento con preavviso
- licenziamento senza preavviso

### 6.4 Sanzioni relative al personale dipendente con qualifica di dirigente

Il rapporto dirigenziale si caratterizza per la sua natura fiduciaria. Il comportamento del dirigente si riflette infatti non solo all'interno della Società, ma anche all'esterno. Eventuali infrazioni poste in essere da dirigenti della Società potranno essere sanzionate attraverso provvedimenti disciplinari adeguati a ciascun caso. Le sanzioni a carico dei dirigenti di Moneynet saranno applicate in caso di violazione di disposizioni contenute nel Modello Organizzativo e nel Codice Etico.

Nella Società trova applicazione per i dipendenti dirigenti il Contratto Collettivo Nazionale di Lavoro per i Dirigenti del settore di riferimento.

- Sono da considerarsi sanzionabili, a titolo esemplificativo, per violazione delle disposizioni contenute del Modello, i comportamenti illeciti posti in essere dal dirigente, il quale:
- ometta di vigilare sul personale da lui stesso gerarchicamente dipendente, affinché venga assicurato il rispetto delle disposizioni del Modello per lo svolgimento delle attività nelle aree a rischio reato e per le attività strumentali a processi operativi a rischio di reato
- non provveda a segnalare mancate osservanze e/o anomalie inerenti all'adempimento degli obblighi di cui al Modello, qualora ne abbia notizia, tali da rendere inefficace il Modello con conseguente potenziale pericolo per la Società alla irrogazione di sanzioni di cui al Decreto 231
- non provveda a segnalare all'Organismo di Vigilanza criticità inerenti lo svolgimento delle attività nelle aree sensibili a rischio reato, riscontrate in occasione del monitoraggio da parte delle autorità preposte
- incorra egli stesso in una o più gravi violazioni alle disposizioni del Modello, tali da comportare

la commissione dei reati contemplati nel Modello, esponendo così la Società all'applicazione di sanzioni ex D.Lgs. n. 231/2001.

### **6.5 Sanzioni relative ai componenti dell'organo amministrativo**

Moneynet valuta con estrema severità le infrazioni al presente Modello attuate da coloro che ricoprono il ruolo di vertici della Società e la rappresentano verso i dipendenti, i clienti, i fornitori, le Autorità di Vigilanza. La responsabilità degli amministratori nei confronti della Società è, a tutti gli effetti, regolata dall'art. 2392 c.c.

L'organo amministrativo è competente per la valutazione dell'infrazione e per l'assunzione dei provvedimenti più idonei nei confronti dei soggetti che hanno commesso le Infrazioni. In tale valutazione, l'organo amministrativo è coadiuvato dall'ODV. Al fine di garantire il pieno esercizio del diritto di difesa deve essere previsto un termine entro il quale l'interessato possa far pervenire giustificazioni e/o scritti difensivi e possa essere ascoltato.

Le sanzioni applicabili sono la revoca delle deleghe o dell'incarico e, nel caso in cui il soggetto sia legato alla Società da un rapporto di lavoro subordinato, il licenziamento.

### **6.6 Misure nei confronti delle controparti contrattuali**

La violazione da parte di partner commerciali, consulenti, o altri soggetti aventi rapporti contrattuali con la Società delle disposizioni e delle regole di comportamento previste dal Modello agli stessi applicabili, o l'eventuale commissione dei reati contemplati dal D.Lgs. n. 231/2001 da parte degli stessi, sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali che saranno inserite nei relativi contratti.

Tali clausole, facendo esplicito riferimento al rispetto delle disposizioni e delle regole di comportamento previste dal Modello, potranno prevedere, ad esempio, l'obbligo, da parte di questi soggetti terzi, di non adottare atti o tenere comportamenti tali da determinare una violazione del Modello da parte della Società.

In caso di violazione di tale obbligo, dovrà essere prevista la facoltà della Società di risolvere il contratto con eventuale applicazione di penali. Resta ovviamente salva la prerogativa della Società di richiedere il risarcimento dei danni derivanti dalla violazione delle disposizioni e delle regole di comportamento previste dal Modello da parte dei suddetti soggetti terzi.

Pertanto, i comportamenti non conformi alle disposizioni del presente Modello comporteranno, indipendentemente ed oltre gli eventuali procedimenti penali a carico del/degli autore/i della violazione, l'applicazione di sanzioni disciplinari ai sensi di quanto sopra rappresentato.

## 7. PROTOCOLLI

### SELEZIONE E APPROVVIGIONAMENTO FORNITORI

#### Descrizione processo

Il processo di acquisizione di beni e servizi si articola nelle seguenti fasi:

- emissione della Richiesta di Acquisto;
- scelta del fornitore e formalizzazione contrattuale;
- gestione dei rapporti col fornitore;
- rilascio beneplacito, contabilizzazione e pagamento fatture.

#### Attività di Controllo

Il sistema di controllo si basa sugli elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo, della tracciabilità degli atti, a garanzia della trasparenza delle scelte effettuate e della valutazione complessiva delle forniture.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- 1) Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - richiesta della fornitura;
  - effettuazione dell'acquisto;
  - certificazione dell'esecuzione dei servizi/consegna dei beni;
  - effettuazione del pagamento.
  
- 2) Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva:
  - comparazione delle offerte (sulla base di criteri oggettivi e documentabili ed in un'ottica volta ad assicurare alla Moneynet la migliore configurazione possibile di costo, qualità e tempo).
  
- 3) Verifica preventiva dei contratti di fornitura:
  - Moneynet richiede al fornitore una bozza del contratto che sarà oggetto di verifica del Responsabile del settore di riferimento e, ove ritenuto necessario, del Responsabile dell'Ufficio Legale o al Responsabile Compliance;
  - al fine di garantire la liceità e la piena pertinenza di ogni rapporto di affari che Moneynet intrattiene con i propri fornitori, si richiede al fornitore una dichiarazione di presa visione del Codice Etico e di impegno ad attenersi ai principi e alle regole che compongono il Modello di Organizzazione, Gestione e Controllo (ex D.Lgs. 231/01) con l'espreso avvertimento che a fronte di eventuali violazioni verranno adottate delle sanzioni, quali la risoluzione del contratto stesso;
  - nel caso non sia possibile inserire la suddetta clausola negli accordi tra società e soggetto terzo, Moneynet invia mediante posta elettronica certificata o lettera raccomandata A.R o a mani., un'informativa finalizzata a notificare alla controparte l'esistenza di un Codice Etico aziendale, che fa parte di un Modello di Organizzazione, Gestione e Controllo (ex D.Lgs. 231/01) adottato da Moneynet.

Moneynet si accerta di ricevere, come risposta all'informativa, una specifica dichiarazione di avvenuta presa di conoscenza.

- 4) Esistenza di livelli di approvazione per le richieste di acquisto e per la certificazione della fornitura/erogazione.
- 5) Esistenza di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni.
- 6) Tenuta a manutenzione dell'albo dei fornitori tra cui dovrà preferibilmente essere selezionato il fornitore.

- 7) Compilazione scheda di valutazione del fornitore a cura del Responsabile dell'area.
- 8) Tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.

### **Indicazioni comportamentali generali**

#### È fatto obbligo di:

- segnalare tempestivamente alle strutture/aree competenti qualsiasi comportamento in contrasto con quanto prescritto dal Modello: tale obbligo grava su tutti i dipendenti della Società, che vengano in qualsiasi forma a conoscenza, nonché sui fornitori, che li subiscano; qualora i fornitori non adempiano a tale obbligo, saranno estromessi dall'elenco dei fornitori e dal singolo affare.

#### È fatto divieto di:

- esercitare violenze, minacce, pressioni, attività ingannatorie o comunque indebite sollecitazioni nei confronti delle parti contraenti, anche su induzione da parte delle medesime, finalizzate al conseguimento di illeciti vantaggi per l'ente nel cui interesse questi agiscono;
- richiedere o accettare elargizioni o promesse di denaro o di altre utilità, compresi omaggi o regali;
- utilizzare fornitori scelti principalmente in base a criteri di amicizia, parentela o altra cointeressenza, e comunque tali da inficiare la validità in termini di prezzo e/o qualità, o che appaiano meramente strumentali alla realizzazione di una delle condotte illecite indicate nel D.Lgs. 231/01;
- negoziare condizioni contrattuali occulte, che non risultano da idonea documentazione conservata unitamente a quella relativa all'acquisto.

In particolare, nelle seguenti attività è fatto divieto di tenere comportamenti che:

- Richiesta della fornitura:
  - consentano di non espletare un'adeguata attività selettiva fra i diversi offerenti e di obiettiva comparazione delle offerte;
  - consentano di privilegiare fornitori segnalati o "graditi" a soggetti pubblici in assenza dei criteri tecnico-economici per la selezione dei potenziali candidati (Qualificazione e inserimento in un Albo Fornitori).
- Effettuazione dell'acquisto:
  - consentano a soggetti non autorizzati di procedere alla stipulazione dei contratti ed all'approvazione delle relative varianti/integrazioni.
- Certificazione dell'esecuzione dei servizi/consegna dei beni
  - consentano l'emissione di fatture a fronte di forniture in tutto o in parte inesistenti o la creazione di fondi patrimoniali a fronte di forniture contrattualizzate a prezzi non congrui o non corrispondenti a quanto pattuito in sede di definizione contrattuale;
  - consentano di effettuare pagamenti che non trovino adeguata giustificazione in relazione alla fornitura oggetto del contratto.
- Effettuazione del pagamento
  - non consentano di liquidare gli importi dovuti in modo trasparente, documentabile e ricostruibile ex post. In particolare, che non consentano la verifica circa la corrispondenza fra il soggetto beneficiario del pagamento ed il fornitore.

## CONSULENZE E PRESTAZIONI PROFESSIONALI

### Descrizione processo

Il processo riguarda l'assegnazione di incarichi di consulenza e prestazioni professionali a soggetti terzi e pertanto si configura, pur nella specificità dell'oggetto contrattuale, come un processo d'acquisizione, articolato nelle seguenti fasi:

- emissione della Richiesta di Consulenza/Prestazione Professionale;
- scelta della fonte d'acquisto e formalizzazione del contratto;
- gestione operativa del contratto;
- rilascio benessere, contabilizzazione e pagamento fatture.

### Attività di Controllo

Il sistema di controllo si basa sui due elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo, della tracciabilità degli atti, a garanzia della trasparenza delle scelte effettuate e del servizio ricevuto.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - richiesta della consulenza;
  - autorizzazione;
  - definizione contrattuale;
  - certificazione dell'esecuzione dei servizi (rilascio benessere);
  - effettuazione del pagamento.
- Esistenza di requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti.
- Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili); in assenza di tale attività selettiva evidenziazione formale delle ragioni della deroga ed esecuzione da parte del responsabile di una valutazione sulla congruità del compenso pattuito (rispetto agli standard di mercato).
- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati.
- Per consulenze svolte da soggetti terzi incaricati di rappresentare la Società deve essere prevista una specifica clausola che li vincoli all'osservanza dei principi etico-comportamentali adottati dalla stessa.
- Esistenza di livelli di approvazione per le richieste di consulenza.
- Validazione del servizio reso.
- Esistenza di livelli autorizzativi (in coerenza con il sistema di procure/poteri aziendali) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni.
- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione).

Sono escluse: le consulenze e le prestazioni professionali di modesto importo.

### Indicazioni comportamentali

In tutte le fasi del processo, ed in particolare nelle seguenti attività è fatto divieto di tenere comportamenti che:

- Richiesta della consulenza
  - consentano l'inoltro della richiesta di conferimento dell'incarico a consulenti esterni per lo svolgimento di attività che possono essere svolte da risorse interne alla Società.

- Autorizzazione alla consulenza
  - consentano l'affidamento dell'incarico in assenza di previa selezione fra una rosa di almeno due potenziali consulenti, ad eccezione delle forniture per le quali si richiede una particolare tecnicità e previa motivazione espressa;
  - consentano l'assegnazione dell'incarico a ex dipendenti della Pubblica Amministrazione o dell'Unione Europea che abbiano partecipato personalmente ed attivamente a una trattativa d'affari o abbiano avallato le richieste effettuate alla Pubblica Amministrazione dalla Società o da società controllate, collegate della medesima o sottoposte a comune controllo con la medesima;
  - consentano l'assegnazione dell'incarico a persone o società "vicine" o "gradite" a soggetti pubblici o privati con i quali la Società ha rapporti commerciali e/o interessi in assenza dei necessari requisiti di qualità e convenienza dell'operazione;
  - consentano la scelta di consulenti che non garantiscano la migliore combinazione in termini di qualità del servizio, prezzo, tempi di consegna, congruità del corrispettivo pattuito ecc.;
  - consentano l'autorizzazione al conferimento dell'incarico al consulente da parte di soggetti a ciò non autorizzati.
  
- Definizione contrattuale
  - consentano la mancata tracciabilità del conferimento formale dell'incarico;
  - non garantiscano l'apposizione di specifica informativa sulle norme comportamentali adottate dalla Società con riferimento al Decreto e sulle conseguenze che possono avere, con riguardo ai rapporti contrattuali, comportamenti contrari alle previsioni del Codice Etico ed alla normativa vigente.
  
- Certificazione dell'esecuzione dei lavori (rilascio benestare)
  - consentano l'emissione di fatture o la creazione di fondi patrimoniali a fronte di operazioni in tutto o in parte inesistenti o a fronte di operazioni contrattualizzate a prezzi superiori di quelli di mercato o comunque non congrui o corrispondenti a quanto pattuito in sede di definizione contrattuale;
  - consentano di effettuare pagamenti e riconoscere rimborsi spese in favore di consulenti, che non trovino adeguata giustificazione in relazione al tipo di incarico svolto, che non siano supportate da giustificativi fiscalmente validi e che non siano esposte in fattura o in parcella.
  
- Effettuazione del pagamento
  - non consentano di liquidare i compensi in modo trasparente, documentabile e ricostruibile ex post. In particolare, che non consentano la verifica circa la corrispondenza fra il soggetto beneficiario del pagamento ed il consulente che ha effettivamente erogato il servizio oggetto dell'incarico conferito.

## UTILIZZO DEGLI STRUMENTI INFORMATICI

### Descrizione processo

Il processo di "Utilizzo degli Strumenti Informatici" si articola in attività volte alla gestione, alla manutenzione e/o all'utilizzo di Sistemi Informativi, inclusi i sistemi di terzi e/o forniti da terzi.

Il processo si articola nelle seguenti fasi:

- identificazione del fabbisogno di accesso al/i sistema/i;
- definizione profili di accesso e attivazione al/i sistema/i;
- manutenzione di/del sistema/i (tra cui: attività di controllo, verifica eccezioni/anomalie).

L'infrastruttura tecnologica e i sistemi informatici rappresentano una risorsa fondamentale e strategica per la Società; l'utilizzo di strumenti e tecnologie informatiche è diffuso e trasversale all'interno della Società: il personale appartenente alle diverse aree aziendali utilizza sistematicamente gli strumenti informatici messi a disposizione per lo svolgimento delle attività di propria competenza, in qualità di utente interno, nell'ambito ad esempio della gestione dei processi di amministrazione, contabilità e controllo di gestione.

I profili di accesso al sistema informatico sono puntualmente identificati dalle competenti strutture in coordinamento con le funzioni/aree interessate, in modo che sia garantita la separatezza delle funzioni e la coerenza dei livelli autorizzativi.

L'uso di credenziali di accesso a sistemi, applicazioni e/o banche dati di terze parti deve essere formalmente autorizzato dalla Direzione Generale così come le variazioni al contenuto dei profili (estensioni delle autorizzazioni) che sono eseguite esclusivamente dall'amministratore di sistema, su richiesta delle funzioni/aree interessate. La funzione/area richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative coperte.

Resta inteso che i diritti di accesso alle risorse di rete (cartelle condivise, stampanti, ecc) sono definiti dalla Direzione Generale e configurati sul server direttamente dal responsabile EDP. In particolare i diritti di accesso alla rete richiedono la definizione di diritti specifici per singoli utenti, che devono essere documentate, ridotte in termini numerici e sempre autorizzate dalla Direzione Generale.

Le attività di gestione ed utilizzo dei sistemi informativi della Società sono soggette a una costante attività di controllo che si esplica sia attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità con particolare riferimento al trattamento dei dati personali, sia tramite l'adozione, per l'insieme dei processi aziendali, di specifiche soluzioni di continuità operativa di tipo tecnologico, organizzativo e infrastrutturale che assicurino la predetta continuità anche a fronte di situazioni di emergenza.

Tra i servizi aziendali di base accessibili ai dipendenti e collaboratori dotati di postazioni di lavoro personali vi sono in particolare la posta elettronica e la navigazione in internet, il cui utilizzo è regolato da specifiche procedure e misure di sicurezza.

Qualora sia previsto il coinvolgimento di soggetti terzi (a titolo esemplificativo, fornitori, consulenti e professionisti) nelle attività a rischio-reato di cui alla presente Parte Speciale, il sistema dei controlli e i principi di comportamento ivi contenuti si applicano anche a presidio delle attività poste in essere dagli stessi.

### Attività di Controllo

Il sistema di controllo per la prevenzione dei reati di criminalità informatica si basa, nel rispetto della normativa applicabile, sugli elementi qualificanti della tracciabilità, della formalizzata separazione di ruolo nelle fasi chiave del processo, oltre che sul rispetto del Codice Etico e delle Linee di Condotta e del complesso della normativa interna (Regolamenti, Circolari, Manuali, Procedure aziendali) vigente. In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- **Separazione** dei ruoli che intervengono nelle attività di gestione e accesso ai Sistemi Informativi.
- **Tracciabilità** degli accessi degli amministratori di sistema e delle attività modificative svolte sui sistemi informatici. In particolare:

- tutti i documenti sono salvati e archiviati in apposite cartelle elettroniche, denominate per argomento e data, presenti sul server della Società;
- le operazioni eseguite dall'amministratore di sistema dai fornitori esterni sono tracciate secondo quanto previsto dal Provvedimento del Garante del 27 novembre 2007 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- in generale, al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la funzione/area di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica;
- il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;
- è garantita la completa tracciabilità di tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente, ecc.), con particolare riguardo all'operato di utenze con privilegi speciali.

- **Raccolta, analisi e gestione di segnalazioni** a fronte di eccezioni/anomalie rilevate.

### **Indicazioni comportamentali**

Per la prevenzione dei crimini informatici, i dipendenti e i collaboratori della Società devono adottare comportamenti conformi, oltre che al Codice Etico e alle Linee di Condotta, anche a tutte le direttive e norme di comportamento contenute nelle politiche e regolamenti in vigore per assicurare i livelli richiesti di sicurezza.

In particolare, non devono essere adottati comportamenti a rischio di reato e non conformi alle suddette norme nell'ambito delle attività svolte a supporto dei principali processi aziendali, nonché, nell'utilizzo degli strumenti informatici che consentono l'accesso ai siti e di pubblica utilità, quando l'utilizzo illecito o non conforme di tali strumenti può provocare il danneggiamento di informazioni pubblicate, procurando un profitto ovvero un vantaggio competitivo o di immagine alla Società.

Il Personale è responsabile del corretto utilizzo degli strumenti informatici a lui assegnati (ad esempio, personal computer fissi o portatili), che devono essere utilizzate in conformità con le normative interne. Tali strumenti devono essere conservati in modo appropriato e la Società deve essere tempestivamente informata di eventuali furti o danneggiamenti.

Il Personale è tenuto alla segnalazione alle competenti strutture dell'Area EDP di eventuali incidenti di sicurezza, anche concernenti attacchi al sistema informatico da parte di hacker esterni).

### È in particolare fatto divieto di:

- introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, trojan, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;

- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato contemplate nel Decreto, nonché atti idonei diretti in modo non equivoco a realizzarle;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato, possano potenzialmente diventarlo.

I Destinatari sono inoltre tenuti a osservare le previsioni legislative esistenti in materia e i principi contenuti nel Codice Etico, nel Documento Programmatico sulla Sicurezza dei dati per la gestione sicurezza fisica e logica del backup (DPS) e nel Piano di Continuità Operativa e del Disaster Recovery (BC&DR) (si chiamano così in Moneynet?)

Il presente protocollo e tutti i presidi adottati dalla Società con riferimento al sistema informatico operano anche con riferimento alla prevenzione del reato di Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti ed ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale, a condizione che ne siano oggetto materiale strumenti di pagamento diversi dai contanti, le attività aziendali sensibili della Società nelle quali può essere commessa questa tipologia di reato, riguardano tutti i processi aziendali che comportano la movimentazione di flussi finanziari sia della Società che per conto della propria clientela attraverso le differenti tipologie di strumenti di pagamento diverse dai contanti e dei relativi applicativi:

Si evidenzia altresì che nell'ambito di protocolli che regolano altre attività sensibili relative ai reati di cui all'art. 25 octies vi sono anche le procedure sulla selezione e gestione dei fornitori e quelli relativi alle consulenze e prestazioni professionali.

## ADEMPIMENTI ANTIRICICLAGGIO

### Descrizione processo

La Società effettua un'accurata attività di formazione e addestramento per tutte le aree aziendali. Per garantire continuità e sistematicità all'attività di qualificazione del personale, l'attività di formazione in materia di antiriciclaggio è incentrata sulla partecipazione del personale sia a corsi esterni e interni, sia a aggiornamenti periodici sull'evoluzione della normativa.

### Attività di Controllo

Il sistema di controllo si basa sugli elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo e della tracciabilità degli atti.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di direttive sulle modalità di condotta operativa da adottare in attuazione della normativa antiriciclaggio.
- Nomina dell'esponente responsabile per l'antiriciclaggio (l'"Esponente Responsabile AML" o "Esponente") che ha il compito di fungere da punto di contatto tra il responsabile della funzione antiriciclaggio (il "Responsabile Antiriciclaggio") e gli organi aziendali, assicurando a questi ultimi il trasferimento delle informazioni necessarie per ben comprendere la rilevanza dei rischi di riciclaggio cui la Società è esposta
- Istituzione di una Funzione Antiriciclaggio.
- Formalizzazione di una politica e di una procedura antiriciclaggio.
- Formalizzazione degli eventuali rapporti con soggetti esterni (consulenti legali, terzi rappresentanti o altro) incaricati di svolgere attività antiriciclaggio a favore della Società, prevedendo, tra l'altro, nei contratti, l'inserimento di una specifica clausola che li vincoli al rispetto dei principi etico- comportamentali adottati dalla Società.
- Rendicontazione in merito agli adempimenti antiriciclaggio posti in essere ed alle relative risultanze e tracciabilità degli atti e delle fonti documentali che ne stanno alla base.

### Indicazioni comportamentali

È fatto divieto di adottare comportamenti contrari al Codice Etico e alle Linee di Condotta in tutte le fasi del processo ed in particolare nelle seguenti attività:

- in sede di gestione ed implementazione degli adempimenti antiriciclaggio a cui la Società è tenuta;
- nel corso delle fasi degli adempimenti antiriciclaggio anche a mezzo di soggetti terzi di cui la Società eventualmente si avvale;
- in sede di ispezioni e verifiche da parte della Autorità competenti.

Nello specifico:

- ai sensi della normativa vigente, qualora non vi sia la possibilità di adempiere agli obblighi di identificazione e verifica del cliente o del titolare effettivo o dell'eventuale esecutore, ovvero di ottenere le informazioni sullo scopo e la natura del rapporto, quindi laddove il cliente rifiuti di fornire al soggetto che entra in contatto con il cliente le informazioni e/o i documenti richiesti ai fini del corretto assolvimento degli obblighi di adeguata verifica oppure la Società, non sia in grado di verificare la veridicità e/o l'attendibilità dei dati/documenti raccolti la Società deve astenersi dall'instaurare il rapporto continuativo;
- sono dettagliati nell'ambito di politiche, regolamenti/norme operative interne le regole comportamentali ad integrazione e maggiore specificazione della normativa esterna e dei principi sanciti dal Modello in materia di contrasto al riciclaggio e finanziamento del terrorismo;
- in caso di richiesta di chiarimenti da parte delle funzioni/aree gerarchicamente sovraordinate, i responsabili della funzione/area forniscono le informazioni in modo tempestivo;
- devono essere assicurate lo sviluppo e la gestione operativa delle applicazioni utilizzate nelle attività di contrasto finanziario al terrorismo/riciclaggio;

- deve essere verificato e garantito l'aggiornamento / manutenzione / diffusione delle liste interne di soggetti/ Paesi/ merci interessati da provvedimenti restrittivi emanati da UE, OFAC, BI-UIF;
- nel caso di valutazione di clientela ovvero di operazioni che interessino più strutture operative, le stesse devono collaborare tra loro e, ove vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza del cliente e delle sue abitudini operative;
- è necessario assicurare con continuità e sistematicità la formazione e l'addestramento del personale sulla normativa antiriciclaggio e sulle finalità dalle stesse perseguite;
- devono essere diffusi a tutti i collaboratori, indipendentemente dalle mansioni in concreto svolte, la normativa di riferimento ed i relativi aggiornamenti;
- tutti i Destinatari del Modello, senza distinzioni di rapporto giuridico in base al quale sono legati alla Società, devono partecipare fattivamente al processo di analisi della clientela e della relativa attività per l'individuazione e la segnalazione di operazioni sospette; in tale ambito, ciascun collaboratore dovrà fare riferimento al Responsabile della funzione/area aziendale di appartenenza, comunicando allo stesso per iscritto ogni operazione, comportamento, anomalia, per qualsivoglia circostanza conosciuta a ragione delle funzioni esercitate, reputata suscettibile di valutazione ai fini di un eventuale avvio dell'iter di segnalazione.

Con specifico riferimento al reato di autoriciclaggio, rilevano inoltre come attività a rischio-reato gli ambiti aziendali nei quali potrebbero potenzialmente essere generati illecitamente denaro, beni o altre utilità (successivamente impiegabili, sostituibili, trasferibili in attività economiche, finanziarie, imprenditoriali o speculative). A titolo esemplificativo, possono essere individuate le seguenti attività a rischio-reato: Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (partner commerciali), Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze, Operazioni di rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa e di gestione degli aspetti fiscali.

I principi di controllo e di comportamento implementati con riferimento a dette attività sono pertanto considerati validi presidi anche ai fini della prevenzione del reato di autoriciclaggio.

In generale, comunque, ove non sia chiara la provenienza di denaro, beni o altre utilità oggetto di attività e/o operazioni svolte nell'ambito dell'operatività aziendale, nonché in tutti i casi in cui si riscontrino elementi tali da farne sospettare una provenienza delittuosa, i Destinatari coinvolti sono tenuti a sospendere immediatamente le attività e/o operazioni interessate, comunicando e rappresentando il fatto ai propri responsabili e a eventuali altri soggetti/strutture/aree competenti, affinché siano posti in essere gli approfondimenti e accertamenti necessari.

## SPESE DI RAPPRESENTANZA

### Descrizione processo

Il processo concerne il sostenimento di spese per la cessione gratuita di beni e servizi a favore di terzi non dipendenti, con lo scopo di offrire un'immagine positiva della Società e dell'attività.

Il processo si articola nelle seguenti fasi:

- sostenimento della spesa;
- autorizzazione al rimborso;
- rimborso.

### Attività di Controllo

Il sistema di controllo si basa sugli elementi qualificanti della individuazione dei soggetti abilitati (a sostenere e ad autorizzare le spese) e sulla tracciabilità degli atti.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- Definizione delle categorie di spesa effettuabili;
- Identificazione dei soggetti aziendali abilitati a sostenere le spese;
- Esistenza di specifici range economici, con espressa indicazione degli importi entro i quali la spesa è da considerarsi di modico valore;
- Esistenza di livelli di autorizzazione per il rimborso delle spese effettuate;
- Esistenza di registrazione, presso il soggetto aziendale abilitato, delle spese sostenute sia a favore dei dipendenti della Pubblica Amministrazione sia dei privati.
- Esistenza, presso i soggetti coinvolti, di evidenza documentale delle singole fasi del processo.

### Indicazioni comportamentali

In tutte le fasi del processo, ed in particolare nelle seguenti attività, è fatto divieto di tenere comportamenti che:

- Sostenimento della spesa:

- consentano l'indicazione di voci di spesa rientranti fra quelle appartenenti alle categorie autorizzate, ma non corrispondenti a quelle effettivamente sostenute;
- permettano il sostenimento della spesa da parte di soggetti a ciò non abilitati.

- Autorizzazione al rimborso:

- consentano l'autorizzazione al rimborso della spesa da parte di soggetti a ciò non autorizzati;
- consentano la registrazione di spese sostenute a favore di soggetti diversi dagli effettivi beneficiari.

- Rimborso

- consentano il rimborso di spese non sostenute in tutto o in parte;
- consentano il rimborso di spese non sorrette da giustificativi fiscalmente validi.

## WHISTLEBLOWING

### Descrizione processo

Il processo concerne la gestione della ricezione, analisi e trattamento di segnalazioni (Whistleblowing) relative violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità di Moneynet di cui siano venute a conoscenza nell'ambito del contesto lavorativo.

Inoltre, tale protocollo si propone di disciplinare le modalità di effettuazione delle segnalazioni e le tutele che Moneynet assicura ai segnalanti ed ai segnalati, nelle more dell'accertamento della fondatezza della segnalazione e di eventuali responsabilità.

Moneynet. intende infatti garantire che i destinatari delle segnalazioni trattino con confidenzialità l'identità del segnalante e del segnalato, nel rispetto assoluto del principio di riservatezza, nonché delle normative di tutela dei lavoratori e della privacy di tempo in tempo vigenti.

### Ambito di Applicazione

Il presente protocollo si riferisce a qualunque illecito commesso da chi è collegato in senso ampio al Moneynet. nel cui ambito si è verificata la violazione (o il tentativo di violazione):

- dipendente;
- lavoratore autonomo;
- collaboratore esterno;
- liberi professionisti e consulenti;
- colui che svolge tirocinio (retribuito o meno);
- volontario (retribuito o meno);
- colui il cui rapporto di lavoro è terminato o non è ancora incominciato (ex dipendente o candidato);
- colui che lavora sotto la supervisione e direzione di appaltatori, sub-appaltatori e fornitori;
- azionisti e persone con funzioni di amministrazione, direzione, vigilanza o rappresentanza.

La normativa NON si applica alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate.

### Riferimenti

- Direttiva (UE) 2019/1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.
- D.lgs. 24/2023 di recepimento della Direttiva (UE) 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali
- Regolamento europeo sui dati personali 679/2016 (GDPR).
- Codice etico;

### Segnalazioni

### Definizioni

Per segnalazione si intende qualsiasi comunicazione avente ad oggetto comportamenti, di qualsiasi natura anche meramente omissivi e/o informazioni che possano integrare gli estremi di un :

- i) reato;
- ii) o condotte inappropriate, scorrette o di presunta violazione dei principi espressi nel Codice Etico, dal Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 (nelle

legislazioni ove applicabili/ove esistente), da policy e procedure adottate dalla Società, da leggi e regolamenti applicabili alla Società.

L'oggetto della segnalazione sono le informazioni sulle violazioni che ledono l'interesse pubblico o l'integrità della Società.

A titolo esemplificativo:

- comunicazioni di presunte violazioni, di richieste o di induzioni alla violazione di norme di leggi o regolamenti, di prescrizioni del Codice Etico, di procedure interne, con riferimento alle attività e prestazioni di interesse di Moneynet (es: inosservanza di clausole contrattuali, frodi, improprio utilizzo di dotazioni aziendali etc.);
- situazioni che violano i diritti umani, tra cui molestie, lavoro minorile, ecc...;
- situazioni che mettono in pericolo la salute o la sicurezza delle persone o che causano danni all'ambiente;
- Violazione della normative antitriciclaggio;
- corruzione o altri reati penali, tra cui corruzione, conflitti d'interesse, omaggi illegali ecc;
- violazioni delle norme sulla concorrenza e sugli aiuti di Stato;
- azioni che ledono i diritti dei consumatori;
- comunicazioni di presunte violazioni del Modello di organizzazione gestione e controllo ex D. Lgs. 231/2001, ove applicabile, anche a seguito di comportamenti a rischio reato e/o illecito previsti da tale Modello
- denunce, provenienti da terzi aventi ad oggetto presunti rilievi, irregolarità e fatti censurabili;
- comunicazioni riguardanti frodi, corruzione e qualsiasi altra attività illegale connessa alle spese dell'Unione;
- comunicazioni afferenti alla protezione dei dati personali e alla sicurezza delle reti e dei sistemi informatici;
- esposti riguardanti tematiche di contabilità, controlli di processo, disapplicazione di procedure operative etc.

E' da intendersi come segnalazione anche la richiesta di chiarimenti sulla correttezza di comportamenti propri o altrui ai fini della piena osservanza della documentazione etica, del Modello Organizzativo ex D. Lgs. 231/2001(ove applicabile) e delle procedure aziendali in genere.

## Soggetti

Può effettuare una segnalazione il dipendente o collaboratore di Moneynet, il cliente, fornitore, business partner o chiunque per via di qualsiasi altra relazione con Moneynet, venga a conoscenza di azioni o condotte che sono, o potrebbero sembrare, non in linea con i valori della Società, non appropriate, corrette, lecite o che possano mettere a rischio il Gruppo, l'ambiente di lavoro e tutti i collaboratori

A titolo esemplificativo ricordiamo:

- i dipendenti;
- i lavoratori autonomi, i liberi professionisti e i consulenti che prestano la propria attività presso l'Ente;
- i volontari e tirocinanti, retribuiti o non, che prestano la propria attività presso Moneynet;
- gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;
- le persone del medesimo contesto lavorativo del segnalante e che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- i colleghi di lavoro della persona segnalante che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente.

## Requisiti

Le segnalazioni

- devono essere effettuate in buona fede
- devono essere circostanziate e fondate su elementi di fatto precisi e concordanti

- devono riguardare fatti riscontrabili e conosciuti direttamente da chi segnala
- devono contenere, se conosciute, tutte le informazioni necessarie per individuare gli autori della condotta potenzialmente illecita.

A tal fine, di seguito si indicano gli elementi che le segnalazioni dovrebbero preferibilmente contenere:

- le generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta nell'ambito dell'azienda.
- una chiara e completa descrizione dei fatti oggetto di segnalazione;
- se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi i fatti oggetto di denuncia;
- se conosciute, le generalità o altri elementi che consentano di identificare il soggetto che ha posto in essere i fatti segnalati (es: la qualifica o il settore in cui svolge l'attività), ovvero i soggetti che hanno concorso alla commissione dell'illecito;
- l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- eventuali documenti che possano confermare la fondatezza dei fatti riportati;
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati;
- dichiarazione del segnalante in merito all'assenza o alla sussistenza di un interesse privato collegato alla segnalazione.

È comunque garantita la possibilità di presentare la segnalazione in forma anonima, che ha lo stesso valore di quella identificata.

Le segnalazioni anonime, rispetto a quelle identificate, devono essere dettagliate in maniera più approfondita affinché i fatti e le situazioni contestati siano sufficienti a poterne valutare la fondatezza e a portare avanti l'istruttoria.

## 5 Ambito e gestione delle segnalazioni

Di seguito sono indicate le modalità operative di effettuazione, ricezione, analisi e trattamento delle segnalazioni, da chiunque inviate o trasmesse.

### Invio delle segnalazioni

Indirizzi dedicati alle Segnalazioni

Le segnalazioni, unitamente agli eventuali documenti a supporto, devono essere inviate dal segnalante ai seguenti recapiti:

- compilando il modulo online disponibile al presente indirizzo [https:// ethicpoint.eu/moneynet](https://ethicpoint.eu/moneynet) (di seguito "Modulo Online")
- casella e-mail aperta: [moneynet@ethicpoint.eu](mailto:moneynet@ethicpoint.eu)
- inviando comunicazione a : Comitato Etico IVS Group, Via dell'Artigianato, Seriate (BG) in cui dovrà essere specificato il nome dell'ente per cui si sta procedendo alla segnalazione;
- chiamando il numero verde 800985231 per l'Italia;

I canali sopra indicati garantiscono, anche tramite strumenti di crittografia, la riservatezza dell'identità del segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa comunicazione.

Indipendentemente dai canali utilizzati per le segnalazioni, è previsto che le stesse vengano gestite dal Comitato Etico, composto da membri esterni all'Ente, autonomo ed indipendente in grado di offrire adeguate garanzie di riservatezza e protezione dei dati.

E' previsto l'obbligo in capo al Comitato Etico di tenere traccia scritta, mediante la predisposizione di apposita reportistica (c.d. "Registro delle segnalazioni") di tutte le segnalazioni ricevute.

Periodicamente viene svolto un controllo di completezza a cura del Comitato Etico al fine di accertare che tutte le segnalazioni pervenute siano state trattate ed inserite nella reportistica sopra citata.

### **Gestione della segnalazione**

Al fine di assicurare una efficiente e tempestiva gestione della segnalazione, il Comitato Etico:

- rilascia alla persona segnalante, entro 7 giorni dalla data di ricezione, avviso di ricevimento della segnalazione;
- mantiene le interlocuzioni con la persona segnalante;
- dà un corretto seguito alle segnalazioni ricevute;
- fornisce un riscontro al segnalante.

Il Comitato Etico dovrà valutare la sussistenza dei requisiti essenziali della segnalazione per valutarne l'ammissibilità e poter quindi accordare al segnalante le tutele previste.

Non sono ritenute ammissibili le segnalazioni che risultano:

- manifestamente infondate per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- generiche nella definizione dell'oggetto dell'informativa che appare incomprensibile;
- corredate da documentazione non appropriata o inconferente.

Una volta valutata l'ammissibilità della segnalazione, il Comitato Etico avvia l'istruttoria interna sui fatti o sulle condotte segnalate per valutare la sussistenza degli stessi.

Nel corso dell'istruttoria il Comitato Etico provvede a:

- a) avviare analisi specifiche, avvalendosi, se del caso, della funzione internal audit e delle funzioni aziendali coinvolte;
- b) concludere l'istruttoria in qualunque momento se, nel corso della medesima, sia accertata l'infondatezza;
- c) avvalersi, se necessario, di esperti o periti esterni alla Società;
- d) eventualmente concordare con il responsabile della funzione aziendale interessata dalla segnalazione ed i vertici aziendali, le eventuali azioni correttive necessarie per la rimozione delle possibili debolezze di controllo rilevate, garantendo, altresì, il monitoraggio della loro relativa attuazione;
- e) concordare con il responsabile della funzione aziendale interessata dalla segnalazione eventuali iniziative da intraprendere a tutela degli interessi del Gruppo IVS (ad es. azioni giudiziarie, sospensione/cancellazione di fornitori) da proporre ai vertici aziendali;
- f) richiedere l'avvio di un procedimento disciplinare nei confronti del segnalante, nel caso di segnalazioni in relazione alle quali siano accertate la malafede del segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della stessa Segnalazione.

All'esito dell'istruttoria, viene fornito riscontro alla segnalazione entro il termine di 3 mesi dalla data di avviso di ricevimento o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine di 7 giorni dalla presentazione della segnalazione.

Qualora il Comitato Etico valuti la segnalazione come una semplice lamentela personale o verificato che il fatto riportato è già stato riscontrato dalla Società o dall'Autorità competente, procede all'archiviazione della segnalazione, informandone il segnalante ove non anonimo.

Allo stesso modo il Comitato Etico può contattare il segnalante - se noto – al fine di chiedere di fornire elementi utili all'indagine.

Qualora risulti fondata, il Comitato Etico dà immediata comunicazione per iscritto:

- all'Amministratore Delegato in caso di comportamento scorretto o illecito riferibile a personale dipendente;
- al Consiglio di Amministrazione per le violazioni da parte di figure apicali;
- agli Amministratori Delegati della capogruppo in caso di comportamento scorretto o illecito riferibile all'organo gestorio di Moneynet;
- 

In aggiunta, il Comitato Etico, nella propria relazione annuale, riferisce al Consiglio d'Amministrazione della Società l'elenco delle segnalazioni pervenute e gli esiti delle analisi effettuate

## **Segnalazioni rilevanti ai fini del dlgs 231/2001**

Qualora la segnalazione abbia rilievo ai fini del D. Lgs. 231/2001, integrando la stessa una violazione del Modello Organizzativo o del Codice Etico o uno dei fatti di reato previsti dal decreto, ne viene data comunicazione all'Organismo di Vigilanza di Moneynet.

L'Organismo di Vigilanza, informato della segnalazione, nel rispetto dei principi di riservatezza e/o anonimato del segnalante, collaborerà all'accertamento e alla gestione della stessa, prenderà le necessarie decisioni e adotterà i provvedimenti conseguenti alla segnalazione rilevante ai fini 231, in applicazione della procedura dedicata.

## **Situazioni di conflitto d'interessi**

La procedura garantisce che la gestione delle segnalazioni venga affidata a soggetti che non si trovano in situazioni di conflitto di interessi.

Qualora la segnalazione riguardi una notizia di comportamento scorretto o illecito riferibile ad uno o più dei componenti del Comitato Etico o dell'Organismo di Vigilanza (D.Lgs. 231/2001), ai soggetti interessati viene inibito l'accesso alla segnalazione.

La segnalazione relativa ad un componente del Comitato Etico o dell'Organismo di Vigilanza verrà indirizzata all'attenzione degli Amministratore Delegato della Società.

Tali disposizioni si applicheranno anche nel caso in cui si verifichi un conflitto di interesse in una fase successiva al ricevimento della segnalazione, con la sostituzione delle persone coinvolte nei rispettivi ruoli secondo le regole di cui sopra.

Tutte le situazioni di conflitto di interessi devono essere dichiarate senza esitazioni e riportate nel Registro delle Segnalazioni.

## **Denuncia all'autorità giurisdizionale**

Il segnalante può valutare di rivolgersi alle Autorità nazionali competenti, giudiziarie e contabili, per inoltrare una denuncia di condotte illecite di cui siano venuti a conoscenza nell'ambito dell'attività di Moneynet.

## **Tutele**

### **Obblighi di riservatezza sull'identità del Segnalante**

L'identità del segnalante, della persona coinvolta e di quelle menzionate nella segnalazione, viene protetta in ogni contesto successivo alla segnalazione, fatta eccezione per i casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione e delle ipotesi in cui l'anonimato non è opponibile per legge.

Moneynet garantisce adeguata protezione dell'identità del segnalante censurando ogni condotta che violi le misure previste a tutela di quest'ultimo mediante l'applicazione di quanto previsto in proposito dal sistema disciplinare adottato dalla Società.

### **Divieto di discriminazione nei confronti del Segnalante**

Nei confronti del segnalante non è consentita né è tollerata alcuna forma di ritorsione o misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla Segnalazione.

Moneynet si riserva il diritto di adottare le opportune azioni nei confronti di chiunque ponga in essere, o minacci di porre in essere, atti di ritorsione contro coloro che abbiano presentato segnalazioni in conformità alla presente Procedura, fatto salvo il diritto degli aventi causa di tutelarsi legalmente qualora siano state riscontrate in capo al segnalante responsabilità di natura penale o civile legate alla falsità di quanto dichiarato o riportato.

Resta inteso che il Moneynet potrà intraprendere le più opportune misure disciplinari e/o legali a tutela dei propri diritti, beni e della propria immagine, nei confronti di chiunque, in mala fede, abbia effettuato segnalazioni false, infondate o opportunistiche e/o al solo scopo di calunniare, diffamare o arrecare

pregiudizio al segnalato o ad altri soggetti citati nella segnalazione. Costituisce altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente procedura.

**Tutela della riservatezza dell'identità delle persone segnalate (o coinvolte) e di altri soggetti.**

La riservatezza dei soggetti segnalati e delle persone diverse dal segnalato implicate in quanto menzionate nella segnalazione è tutelata dalla disciplina sui dati personali.

**Conservazione e accesso alla documentazione**

Le funzioni coinvolte nelle attività disciplinate dalla presente Procedura assicurano, ciascuna per quanto di competenza e anche mediante i sistemi informativi utilizzati, la tracciabilità dei dati e delle informazioni e provvedono alla conservazione e archiviazione della documentazione prodotta, cartacea e/o elettronica, in modo da consentire la ricostruzione delle diverse fasi del processo stesso. La documentazione in originale, cartacea e/o elettronica, deve essere conservata per il tempo necessario all'esecuzione delle attività per le quali sono raccolti, che, in mancanza di diverse esigenze, non supererà i due anni, dopodiché verranno conservati in esecuzione di obblighi di legge e disposizioni vigenti, per finalità di tipo amministrativo e/o per far valere e/o difendere i diritti e/o legittimi interessi della Società o di terzi, anche in caso di reclami, contenziosi o precontenziosi.

## 8. FLUSSI INFORMATIVI

Si riporta di seguito lo schema dettagliato dei Flussi Informativi minimi destinati all'OdV.

È fatto salvo qualsivoglia ulteriore flusso informativo previsto dalla normativa interna di Moneynet che dovesse venire istituito a seguito dell'adozione del presente Modello.

AREA/RISCHIO	INFORMAZIONE	PERIODICITA'
<b>RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE O L'UNIONE EUROPEA</b>	Elenco di eventuali bandi cui si partecipa, della loro natura e delle modalità di partecipazione	Elenco iniziale da aggiornare semestralmente
	Transazioni/comunicazioni/contratti con la PA o l'Unione Europea	Su richiesta dell'OdV
	Elenco delle attività ispettive effettuate dalle Autorità di Vigilanza e verbale conclusivo	Ad evento
<b>CONTENZIOSI GIUDIZIALI O STRAGIUDIZIALI</b>	Elenco dei contenziosi (attivi e passivi) e dei responsabili della gestione	Elenco iniziale da aggiornare annualmente
<b>TRANSAZIONI FINANZIARIE</b>	Comunicazione di eventuali anomalie nella registrazione di fatture/pagamenti/incassi	Opinion della Società di revisione
	Comunicazione di eventuali irregolarità o anomalie riguardo, in particolare: <ul style="list-style-type: none"> <li>• al pagamento di fatture; pagamenti relativi anche alle somme da versare al fisco e agli enti previdenziali;</li> <li>• corrispondenza tra accordi;</li> <li>• ordini di acquisti e fatturazioni.</li> </ul>	Confronto con il Collegio Sindacale

<b>SELEZIONE E GESTIONE DEL PERSONALE</b>	Report periodici sulle assunzioni, contenenti sia le modalità di selezione dei candidati utilizzate sia eventuali eccezioni/deroghe alle regole standard	Semestrale
	Elenco delle attività/programma di formazione e aggiornamento dei dipendenti	Annuale
<b>SELEZIONE E GESTIONE DEGLI INCARICHI, DELLE CONSULENZE E PRESTAZIONI PROFESSIONALI</b>	Elenco degli incarichi/consulenze/prestazioni professionali di importo superiore a € 25.000,00 (esclusi organi sociali)	Annuale
<b>REGALI, OMAGGI E SPESE DI RAPPRESENTANZA</b>	Elenco di tutti gli omaggi/spese di rappresentanza di importo superiore al modico valore effettuati nel periodo	A richiesta
<b>BILANCI, RELAZIONI E COMUNICAZIONI SOCIALI IN GENERE</b>	Verbale delle Funzioni di controllo qualora siano emerse criticità nello svolgimento delle attività di revisione	Ad evento
	Verbale di approvazione del bilancio da parte del CdA	Annuale
<b>OPERAZIONI SOCIETARIE CHE POSSONO INCIDERE SULLA INTEGRITA' DEL CAPITALE SOCIALE</b>	Elenco delle operazioni societarie che possono incidere sulla integrità del capitale sociale	Ad evento
	Verbali del CdA e dell'Assemblea	Ad evento

<b>RAPPORTI CON TERZE PARTI</b>	Comunicazione delle attività di raffronto con il mercato	Annuale
<b>ANTIRICICLAGGIO</b>	Elenco delle attività di controllo dei flussi finanziari aziendali in entrata	Relazione funzione antiriciclaggio
	Segnalazioni di operazioni sospette	Relazione funzione antiriciclaggio
	Informativa sui clienti censiti sull'anagrafe societaria in liste antimafia/antiterrorismo	Relazione funzione antiriciclaggio
<b>SALUTE E DI SICUREZZA SUL LAVORO</b>	Elenco dei soggetti incaricati al presidio della sicurezza sul lavoro: delegati, RSPP, RSL, Medico competente	Elenco iniziale e aggiornamenti ad evento

	DVR ed eventuali aggiornamenti	Annuale
	Verbale delle riunioni tra RSPP e RLS	Annuale
<b>REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI</b>	Attività di controllo e verifica della sicurezza dei sistemi informativi e sulla loro efficacia ed efficienza	Trasmissione degli esiti e delle verifiche svolte internamente
	Comunicazione degli incidenti e dei problemi relativi alla sicurezza informatica	Ad evento
	Dichiarazione di conformità sul trattamento dei dati personali	Relazione di compliance
	Copia della denuncia all'autorità giudiziaria in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società	Ad evento