PARTE SPECIALE F

I DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI ED I DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE EX ARTT. 24 BIS E 25 NOVIES D.LGS. 231/01

Revisione	Data	Descrizione	Approvato da
0	12/10/2017	Adozione	CdA

1.FINALITA'

La Parte Speciale ha la finalità di definire, in generale, linee, regole e principi di comportamento che tutti i Destinatari del Modello dovranno seguire e integra il sistema dei controlli delineato dalla Parte Generale.

In tale ambito, sono definite le specifiche attività "sensibili" svolte in Ergosud e le condizioni di correttezza e trasparenza nella conduzione delle attività che la Società deve assicurare al fine di prevenire la commissione dei reati previsti dal Decreto.

Al fine di rispondere alle suddette finalità, la presente Parte Speciale risulta così articolata:

- breve descrizione dei reati presupposto della responsabilità amministrativa ex d. lgs.231/01 alla cui prevenzione è diretta tale Parte Speciale;
- individuazione delle aree e/o i processi definiti " attività sensibili" ovvero a rischio di reato;
- definizione del sistema dei controlli, perfezionato dalla Società sulla base delle indicazioni fornite dalle Linee guida di Confindustria nonché dei *framework* e *standard* internazionalmente riconosciuti in tema di ICT Security Governance, Management & Compliance. Il sistema dei controlli, con riferimento alle Attività Sensibili individuate, prevede:
    a) i principi comportamentali generali che devono indirizzare i comportamenti dei Destinatari nelle varie aree operative, con lo scopo di prevenire comportamenti scorretti o non in linea con le direttive della Società;
    b) standard di controllo "generali", applicabili a tutte le Attività Sensibili;
    c) standard di controllo "specifici", applicati alle singole Attività Sensibili.

Gli standard di controllo, generali e specifici, sono intesi quali principi fondamentali di riferimento ai quali si ispira il sistema procedurale e organizzativo adottato dalla Società, quale parte integrante del modello di *governance* (paragrafo 2.2 della Parte Generale), e dei protocolli del Modello aventi caratteristiche comuni in relazione a tutte le fattispecie di reato previste dal Decreto (paragrafo 3.2 della Parte Generale).

L'insieme degli strumenti di controllo sopra descritti consente di individuare, rispetto a ciascuna attività sensibile, come si siano formate e attuate le decisioni dell'ente (cfr. art. 6, comma 2 lett. b, d.lgs. n. 231/2001).

2. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. N. 231/2001

Si riporta, qui di seguito, una breve descrizione dei reati contemplati dagli artt. 24 *bis* e 25 *novies* del D.lgs. 231/01.

I REATI INFORMATICI: ART. 24 BIS D.LGS. 231/01

Art. 491-bis c.p.: Documenti informatici
L'art. 1, lett. p) del D. Lgs. 82/2005 (Codice dell'amministrazione digitale), definisce documento informatico "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". In questo contesto normativo si inserisce l'art. 491 bis c.p. che estende la punibilità delle falsità documentali laddove prescrive che "Se alcuna delle falsità previste al presente capo (i.e. capo III Titolo VII libro II del c.p. "falsità in atti") riguarda un documento informatico pubblico o privato avente efficacia

probatoria si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".
La fattispecie di cui all'art. 491-bis c.p. ha quindi espressamente riconosciuto validità al documento elettronico, equiparato all'atto pubblico ed alla scrittura privata ed ha previsto una speciale forma di tutela da eventuali falsificazioni materiali o ideologiche per la possibilità di alterare, duplicare, immettere, modificare, manipolare o cancellare abusivamente le informazioni.
Attraverso il richiamo effettuato al capo III del c.p. vengono ad assumere rilevanza quali reati presupposto ai fini del Decreto anche le c.d. falsità in atti, disciplinate dagli artt. 476 e ss del c.p..

Accesso abusivo ad un sistema informatico o telematico (art . 615 ter c.p.)

Definizione: Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Da 100 a 500 quote
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi
Condotta: Tale ipotesi di reato si configura nel caso in cui taluno abusivamente s'introduca o permanga - contro la volontà espressa o tacita di colui che ha il diritto di escluderlo - all'interno di un sistema informatico o telematico protetto da misure di sicurezza.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)

Definizione: Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Fino a 300 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)

Definizione: Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Fino a 300 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)

Definizione: Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Da 100 a 500 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi
Condotta: Tale ipotesi di reato si configura quando taluno, fraudolentemente, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe.

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

Definizione: Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Da 100 a 500 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)

Definizione: Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Da 100 a 500 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi
Casistica: Tale reato si potrebbe, per esempio, concretizzare attraverso il deterioramento, la cancellazione o la soppressione di informazioni, dati o programmi informatici altrui.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)

Definizione: Salvo che il fatto costituisca piu' grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Da 100 a 500 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito

Divieto di pubblicizzare beni o servizi
Casistica: La fattispecie delittuosa potrebbe configurarsi, a titolo esemplificativo, nel caso in cui si verifichi la distruzione, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità.

Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)

Definizione: Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Da 100 a 500 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi
Casistica: Tale fattispecie di reato potrebbe essere integrata, ad esempio, tramite la distruzione, il danneggiamento o qualsiasi altra operazione che renda inservibili sistemi informatici o telematici altrui.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

Definizione: Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Da 100 a 500 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di pubblicizzare beni o servizi
Casistica: Tale fattispecie può realizzarsi, a titolo esemplificativo, attraverso la distruzione, il danneggiamento o qualsiasi altra operazione che renda inservibili sistemi informatici o telematici di pubblica utilità.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)

Definizione:

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a se´ o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Fino a 400 quote.
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Divieto di contrattare con la pubblica amministrazione Esclusione da, ed eventuale revoca di, agevolazioni, finanziamenti, contributi o sussidi Divieto di pubblicizzare beni o servizi

I DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE: ART. 25 NOVIES D.LGS. 231/01

Art. 171 comma 1 lett a bis) L. 633/1941

Definizione: Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: a) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa; [..] La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore. (III comma)
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Fino a 500 quote
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di contrattare con la pubblica amministrazione Esclusione da, ed eventuale revoca di, agevolazioni, finanziamenti, contributi o sussidi Divieto di pubblicizzare beni o servizi
Condotta: L'accertamento dell'illecito penale verte sulla dimostrazione che l'utente, all'interno della memoria del sistema informatico, disponga di file contenenti musica, film o software protetti dalle norme sulla proprietà intellettuale che sono stati condivisi su reti telematiche utilizzando un apposito programma (emule, bittorent, kazaa o altro). E', dunque, necessario aver scaricato, mediante un programma di file-sharing, quantomeno un file o parte di esso che ne consenta l'identificazione, per accertare se quanto immesso nella rete telematica a disposizione del pubblico sia tutelato dalla legge sul diritto d'autore ovvero si tratti di materiale liberamente circolatile.

Art. 171-bis L. 633/1941

Definizione: Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è punito con la pena della reclusione da sei mesi a tre anni e della multa da euro

2.582,00 ad euro 15.493,00.
La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.
La pena non è inferiore nel minimo a due anni di reclusione e la multa ad euro 15.493,00 se il fatto è di rilevante gravità.
Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582,00 ad euro 15.493,00. La pena non è inferiore nel minimo a due anni di reclusione e la multa ad euro 15.493,00 se il fatto è di rilevante gravità.

Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01:
Fino a 500 quote

Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01:
Interdizione dall'esercizio dell'attività
Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito
Divieto di contrattare con la pubblica amministrazione
Esclusione da, ed eventuale revoca di, agevolazioni, finanziamenti, contributi o sussidi
Divieto di pubblicizzare beni o servizi

Art. 171-ter L. 633/1941

Definizione:
E' punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582,00 ad euro 15.493,00 chiunque a fini di lucro:
a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende,

concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.
f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all' art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell' autorità amministrativa o giurisdizionale;
h) abusivamente rimuove o altera le informazioni elettroniche di cui all' articolo 102- quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.
È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582,00 ad euro 15.493,00 chiunque:
a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;
c) promuove o organizza le attività illecite di cui al comma 1.
La pena è diminuita se il fatto è di particolare tenuità.
La condanna per uno dei reati previsti nel comma 1 comporta:
a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;
c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.
Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01:
Fino a 500 quote

Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01:
Interdizione dall'esercizio dell'attività
Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito
Divieto di contrattare con la pubblica amministrazione
Esclusione da, ed eventuale revoca di, agevolazioni, finanziamenti, contributi o sussidi
Divieto di pubblicizzare beni o servizi

Art. 171-septies L. 633/1941

Definizione:
La pena di cui all'articolo 171-ter, comma 1, si applica anche:
a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i

quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi; b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Fino a 500 quote
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di contrattare con la pubblica amministrazione Esclusione da, ed eventuale revoca di, agevolazioni, finanziamenti, contributi o sussidi Divieto di pubblicizzare beni o servizi

Art. 171-octies L. 633/1941

Definizione: Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582,00 ad euro 25.822,00 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio. La pena non è inferiore a due anni di reclusione e la multa ad euro 15.493,00 se il fatto è di rilevante gravità.
Sanzione pecuniaria prevista ai sensi del D.Lgs. 231/01: Fino a 500 quote
Sanzione interdittiva prevista ai sensi del D.Lgs. 231/01: Interdizione dall'esercizio dell'attività Sospensione o revoca di autorizzazioni, licenze o concessioni funzionali per l'illecito Divieto di contrattare con la pubblica amministrazione Esclusione da, ed eventuale revoca di, agevolazioni, finanziamenti, contributi o sussidi Divieto di pubblicizzare beni o servizi

3. LE "ATTIVITÀ SENSIBILI" AI FINI DEL D. LGS. N. 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

L'analisi dei processi della Società ha consentito di individuare le seguenti attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24 -*bis* e dall'art. 25 *novies* del d. lgs. n. 231/2001:

1) **Gestione dei profili utente e del processo di autenticazione**
2) **Gestione e protezione della postazione di lavoro**
3) **Gestione degli accessi da e verso l'esterno**
4) **Gestione e protezione delle reti informatiche**
5) **Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD)**
6) **Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.).**
7) **Gestione dei sistemi hardware**
8) **Gestione dei sistemi software**
9) **Predisposizione documenti informatici e gestione relativa archiviazione**
10) **Gestione e acquisti di programmi per elaboratore dotati di licenze e materiale IT**

4. I DESTINATARI

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori, dirigenti, dipendenti nonché Collaboratori esterni e Partner della Società, compresi gli eventuali soggetti appartenenti ad altre società coinvolti nella gestione delle aree di attività a rischio, e comunque di chi, anche solo di fatto, rientri nelle categorie di apicali o subordinati della società.

5. PRINCIPI GENERALI DI COMPORTAMENTO E STANDARD DI CONTROLLO GENERALI

Di seguito si indicano i principi generali di comportamento che devono essere rispettati da tutti i Destinatari del presente Modello.

La presente Parte Speciale prevede l'espresso obbligo, a carico degli esponenti aziendali in via diretta e, tramite apposite clausole contrattuali, a carico dei collaboratori esterni e partner, di evitare tutti i comportamenti che integrino i reati sopra descritti.

Conseguentemente, la presente Parte Speciale prevede **l'espresso divieto** di:

- porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 24 bis e 25 novies del Decreto) o comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo o esserne strumentali;
- tenere comportamenti non in linea con il presente Modello o con il Codice Etico adottati dalla Società;
- porre in essere attività che siano in contrasto con le procedure e i principi di controllo in esse previsti ai fini della prevenzione dei reati in tali ambiti.

- rispettare tutte le leggi e regolamenti locali, nazionali ed internazionali in materia di tutela del diritto d'autore e di tutela della proprietà intellettuale;
- attenersi scrupolosamente alle modalità e ai criteri stabiliti per l'assegnazione, gestione e utilizzo delle misure di sicurezza su tutti i computer in uso, nonché su portatili, smartphone e tablet aziendali in dotazione;
- osservare e rispettare le disposizioni vigenti per il rilascio di un certificato qualificato di firma elettronica.

Inoltre, per quanto riguarda i rapporti con fornitori esterni, a prevenzione dei reati in oggetto, la Società ribadisce che è obbligatorio:

- formalizzare e definire in forma scritta tutte le condizioni ed i termini relativi ai contratti stipulati dalla Società con Fornitori o Partner;
- inserire un'apposita clausola contrattuale che i Fornitori e i Partner devono sottoscrivere in cui dichiarano di essere a conoscenza e di impegnarsi a rispettare i principi previsti dal Codice Etico adottato dalla Società, nonché dalla normativa di cui al D.Lgs. n. 231/2001. Tale clausola deve regolare anche le eventuali conseguenze in caso di violazione da parte degli stessi delle norme di cui al Codice Etico (es. clausole risolutive espresse, penali).

5.1 Standard di controllo generali

Gli standard di controllo di carattere generale da considerare e applicare con riferimento a tutte le Attività Sensibili individuate sono i seguenti:

- Esistenza di Procedure / Linee Guida Formalizzate: disposizioni idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività sensibile;
- Tracciabilità: tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici;
- Segregazione dei compiti: lo standard concerne l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate: devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni.

5.2 I contratti di servizio

Alcune delle attività sensibili indicate sono gestite, in tutto o in parte, da personale di altra società in forza di contratti di servizio che regolano formalmente le prestazioni di servizi, assicurando trasparenza agli oggetti delle prestazioni erogate ed ai relativi corrispettivi, determinati sulla base dei prezzi di mercato. Tali contratti prevedono l'impegno al rispetto dei principi di organizzazione e gestione idonei a prevenire la commissione degli illeciti ex d. lgs. n. 231/2001 da parte della Società affidataria.

6. PRINCIPI DI COMPORTAMENTO SPECIFICI ED IL SISTEMA DI CONTROLLO ESISTENTE

Nell'ambito delle suddette regole, **è fatto divieto**, in particolare, di:

- alterare o falsificare, in tutto o in parte, documenti informatici, pubblici o privati, aventi efficacia probatoria;

- alterare o contraffarre documenti informatici relativi a procedure amministrative quali, a mero titolo esemplificativo, autorizzazioni o certificati;
- inserire dati o informazioni non veritiere quando queste siano destinate ad elaborazioni informatizzate o elenchi o registri elettronici;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- scaricare tramite un programma di file sharing file contenenti musica, film o software protetti dal diritto d'autore e immetterli a disposizione del pubblico;
- mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;
- duplicare programmi per elaboratore o importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori e editori (SIAE);
- pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico o far fa ascoltare in pubblico duplicazioni o riproduzioni abusive, con fine di lucro;
- detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
- ritrasmettere o diffondere, in assenza di accordo con il legittimo distributore, con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
- rimuovere o alterare le informazioni elettroniche di cui all' articolo 102- quinquies, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse;

- porre in essere le condotte previste dall'art. 171 ter L. 633/1941;
- produrre, porre in vendita, importare, promuovere, installare, modificare, utilizzare per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.

Pertanto, i soggetti sopra indicati devono:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica;
- segnalare alle funzioni competenti il furto, il danneggiamento o lo smarrimento di tali strumenti; inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla funzione competente l'originale della denuncia all'Autorità di Pubblica Sicurezza;
- evitare di introdurre e/o conservare in Società (in forma cartacea, informatica e mediante utilizzo di strumenti della Società), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;
- evitare di trasferire all'esterno della Società e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- evitare di lasciare incustodito e/o accessibile ad altri il proprio Personal Computer (PC);
- evitare l'utilizzo di password di altri utenti della Società, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile Funzione IT;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza della Società per la protezione e il controllo dei sistemi informatici;
- non acquistare programmi e software in autonomia e rispettare la normativa a tutela del diritto d'autore.

Il sistema per la prevenzione dei reati perfezionato dalla Società è stato realizzato applicando alle attività sensibili prese in considerazione i seguenti standard di controllo.

La regolamentazione delle attività garantisce:

- l'esistenza di una politica in materia di sicurezza del sistema informativo che prevede, fra l'altro:
  a) le modalità di comunicazione anche a terzi;

b) le modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi.

- l'adozione e l'attuazione di uno strumento normativo che definisce i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni alla Società e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.
- l'adozione e attuazione di uno strumento normativo che definisce i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni alla Società e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.
- l'adozione e l'attuazione di uno strumento normativo che definisce i ruoli e le responsabilità per l'identificazione e la classificazione degli asset (ivi inclusi dati e informazioni).
- l'adozione e l'attuazione di uno strumento normativo che dispone controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.
- l'adozione e l'attuazione di uno strumento normativo che assicura la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite policy e procedure. In particolare, tale strumento normativo deve assicurare:
  a) il corretto e sicuro funzionamento degli elaboratori di informazioni;
  b) la protezione da software pericoloso;
  c) il back-up di informazioni e software;
  d) la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
  e) gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
  f) una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
  g) il controllo sui cambiamenti agli elaboratori e ai sistemi;
  h) la gestione di dispositivi rimovibili.
- l'adozione e l'attuazione di uno strumento normativo che disciplina gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo prevede:
  a) l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
  b) le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
  c) una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
  d) la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
  e) la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
  f) l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;

g) la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni della Società;
h) la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
i) la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
j) i piani e le procedure operative per le attività di telelavoro.

- l'adozione e l'attuazione di uno strumento che definisce adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo prevede:
  a) appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;
  b) l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;
  c) la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
  d) l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;
  e) appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
  f) l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
  g) l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;
  h) la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;
  i) la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.
- l'adozione e l'attuazione di uno strumento normativo che disciplina i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.
- l'adozione e l'attuazione di uno strumento normativo che prevede:
  a) la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
  b) specifiche attività di formazione e aggiornamenti periodici sulle procedure di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
  c) l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
  d) la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.
- l'adozione e l'attuazione di uno strumento normativo che definisce:
  a) l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;

b) la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
c) la confidenzialità, autenticità e integrità delle informazioni;
d) la sicurezza nel processo di sviluppo dei sistemi informativi.

- l'adozione e l'attuazione di uno strumento normativo che definisca i ruoli e le responsabilità nella gestione degli acquisti di software e materiale IT.

Tale processo viene svolto, in tutto o in parte, in service da EP Produzione Spa, sulla base di uno specifico contratto di servizio tra le parti. In particolare, tale contratto prevede termini e condizioni delle modalità di prestazione del servizio e dei relativi obblighi posti a carico delle parti, e l'impegno al rispetto dei principi di organizzazione e gestione idonei a prevenire la commissione degli illeciti ex d. lgs. 231/2001 da parte della Società affidataria.

Tali Attività Sensibili vengono svolte dall'affidatario secondo le modalità tecnico-operative regolamentate dalle proprie procedure di riferimento in ambito ICT.

7. REPORTING VERSO L'ORGANISMO DI VIGILANZA

Attraverso gli appositi canali dedicati:

- chiunque venga a conoscenza di violazioni del Modello Organizzativo o del Codice Etico o di situazioni di pericolo o anomalie rispetto alla gestione delle attività a rischio, deve immediatamente comunicarlo all'OdV;
- chiunque venga a conoscenza di violazioni o della mancata applicazione di procedure aziendali, deve immediatamente comunicarlo all'OdV.