MOG ex D.lgs. 231 PARTI SPECIALI:
B. Reati Societari e di riciclaggio
C. Reati Informatici e diritto d'autore
D. Reati di Sicurezza sul Lavoro e tutela ambientale

di Terni Reti Srl unipersonale

REVISIONE 0 (Prima emissione) –
DETERMINA N. 73 del 30 novembre 2016

SOMMARIO

VI - MOG PARTE SPECIALE D - "Reati in violazione delle norme di sicurezza sul lavoro e di tutela ambientale"

IV - MOG PARTE SPECIALE B - "Reati societari e reati di ricettazione e riciclaggio di provenienza illecita".

IV.1 INTRODUZIONE

Le tipologie di reati descritte in questa Parte Speciale sono finalizzate a tutelare interessi giuridici tra loro differenti; tuttavia, poiché le fattispecie di reato insistono principalmente nei processi amministrativo-contabili oppure trovano una barriera al loro verificarsi nella corretta gestione contabile e finanziaria si è preferito trattarle contestualmente in un unico documento.

Di seguito si fornisce, separatamente l'elencazione dei reati societari (art. 25 ter) e reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 octies). Tali disposizioni prevedono specifiche sanzioni pecuniarie a carico dell'ente "*in relazione a reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica*" Si tratta di reati cosiddetti "propri", che possono, pertanto, essere commessi dai soli soggetti esplicitamente individuati nella disposizione in esame (amministratori, direttori generali, liquidatori).

Si fa presente, inoltre, che dopo un'attenta valutazione sono stati considerati non applicabili o irrilevanti per la natura stessa dell'amministrazione proprietaria di Terni Reti i seguenti reati:

- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

  La fattispecie in esame è un reato di danno che si configura qualora gli amministratori, attraverso l'acquisto o la sottoscrizione di azioni o quote, sociali o della società controllante, cagionino un'effettiva lesione dell'integrità del capitale sociale o delle riserve non distribuibili per legge.

- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

  La fattispecie criminosa, che rileva solo nel caso in cui la società venga messa in liquidazione, consiste nel ripartire i beni sociali tra i soci prima di aver pagato i creditori sociali, ovvero prima di aver accantonato le somme necessarie a soddisfarli.

- Aggiotaggio (art. 2637 c.c.)

  Oggetto materiale del reato sono gli "strumenti finanziari" emessi dalla Società, non quotati o per i quali non è stata presentata richiesta di quotazione.

IV.2 RISCHI DI REATO (da Catalogo dei reati)

IV.2.1 Reati societari ex art. 25 ter D.lgs. 231/2001

LE FALSITÀ IN COMUNICAZIONI, PROSPETTI E RELAZIONI

False comunicazioni sociali (artt. 2621 e 2622 c.c.): il reato è riconducibile a due disposizioni normative che, nel punire le diverse ipotesi di rappresentazione non veritiera della situazione economica della società, si differenziano per il verificarsi o meno di un danno patrimoniale per i soci o i creditori. Entrambe le disposizione intendono tutelare la veridicità e completezza delle informazioni per il corretto esercizio dell'attività economica e per il rispetto dei soggetti che non possono intervenire i alcun modo sulle decisioni dell'ente.

La condotta penalmente rilevante si concretizza nella falsa descrizione di fatti materiali, anche se oggetto di valutazioni, nonché nella omissione di informazioni imposte dalla legge, idonee ad alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria[1] della società o del gruppo al quale essa appartiene e devono riguardare bilanci, relazioni o altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico.

La prima ipotesi (art. 2621 c.c.) è una fattispecie di pericolo ed è costruita come una contravvenzione dolosa; la seconda (art. 2622 c.c.) è invece un delitto che richiede per la sua consumazione il verificarsi di un danno per il patrimonio di soci e creditori. La norma richiede la consapevole volontà di ingannare i soci o il pubblico, al fine di conseguire un ingiusto profitto all'agente o a terzi (dolo specifico).

LA TUTELA PENALE DEL CAPITALE SOCIALE E DEL PATRIMONIO

Indebita restituzione dei conferimenti (art. 2626 c.c.)

La norma, che si pone a tutela dei creditori e dei terzi, è volta a salvaguardare l'integrità e l'effettività del capitale sociale.

Si tratta di un reato proprio di chi riveste la qualifica di amministratore. Il reato punisce il fatto degli amministratori che, in assenza di legittime ipotesi di riduzione del capitale sociale, provvedono a restituire i conferimenti effettuati dai soci o li liberino gli stessi dall'obbligo di restituirli. Il reato assume rilievo solo se, per effetto degli atti compiuti dagli amministratori si intacca il capitale sociale e non i fondi o le riserve rispetto ai quali si applicherà il reato previsto dall'art 2627 c.c.

Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

È una fattispecie di natura contravvenzionale posta a tutela dell'integrità del capitale e delle riserve obbligatorie per legge, quale strumento per il conseguimento dell'utile sociale e di

[1] La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico d'esercizio al lordo delle imposte non superiore al 5% o una variazione del patrimonio netto non superiore all'1%; in ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate differiscono in misura non superiore al 10% di quella corretta.

garanzia dei creditori. La norma contiene la clausola di riserva qualora il fatto possa configurarsi nel più grave reato di appropriazione indebita (art. 646 c.p.). Il reato si estingue in caso di restituzione degli utili e nel caso di ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

Si tratta di un reato proprio di chi riveste la qualifica di amministratore. Il reato, procedibile a querela della persona offesa, è diretto a tutelare il patrimonio sociale in occasione di operazioni straordinarie (riduzione del capitale sociale, fusioni, scissioni) effettuate in violazione delle disposizioni di legge a tutela dei creditori e si estingue nel caso in cui avvenga il risarcimento del danno ai creditori prima del giudizio. Il dolo è generico e si concretizza nella consapevolezza di violare le prescrizioni di legge.

Formazione fittizia del capitale (art. 2632 c.c.)

Si tratta di un reato proprio, i cui soggetti attivi possono essere gli amministratori o i soci conferenti. Le tre condotte rilevanti che possono favorire la realizzazione dell'evento delittuoso di formazione fittizia del capitale sociale sono: la sottoscrizione reciproca di azioni o quote; la sopravvalutazione rilevante dei conferimenti dei beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione. Questa disposizione, è posta a tutela della effettività ed integrità del capitale sociale ed è procedibile d'ufficio.

ALTRI ILLECITI

Impedito controllo (art. 2625 c.c.).

La fattispecie consiste nell'impedire o ostacolare da parte degli amministratori, mediante qualsiasi comportamento commissivo o omissivo, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci o ad altri organi sociali (quale in particolare i Collegio Sindacale) o alle società di revisione procurando un danno ai soci stessi

Se la condotta illecita ha causato un danno ai soci, si applica una sanzione di natura penale; in caso contrario la sanzione a carico dell'agente sarà unicamente amministrativa. È prevista la procedibilità a querela di parte.

Illecita influenza sull'assemblea (art. 2636 c.c.)

Il reato punisce il fatto di chiunque riesca a determinare la maggioranza in assemblea – con atti simulati o con la frode – allo scopo di conseguire, per sé o per altri, un ingiusto profitto. La condotta illecita si perfeziona con la formazione irregolare di una maggioranza che altrimenti non si sarebbe avuta, attraverso il compimento di atti simulati o fraudolenti.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

Si tratta di un reato che può essere commesso dagli amministratori, dai direttori generali o dai liquidatori di società sottoposti per legge al controllo delle autorità pubbliche di vigilanza. Il reato è

riconducibile a due fattispecie delittuose distinte: la prima centrata su esposizioni di fatti non rispondenti al vero al fine di ostacolare le funzioni di vigilanza; la seconda sulla realizzazione intenzionale dell'evento di ostacolo attraverso una condotta che può essere sia attiva, sia omissiva. È necessario che sussista nell'attore la consapevolezza di ostacolare con la propria condotta le funzioni degli organismi di vigilanza (dolo generico).

IV.2.2 Reati di ricettazione e riciclaggio di denaro di provenienza illecita ex art. 25 octies.

La responsabilità della società per i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, è stata introdotta con il D.lgs. 231/2007, in seguito all'attuazione da parte del Governo della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca le misure di esecuzione.

L'Ente è punibile per i reati di ricettazione, riciclaggio e impiego di capitali illeciti, anche se compiuti in ambito prettamente "nazionale", sempre che ne derivi un interesse o vantaggio per l'ente medesimo.

Ricettazione (Art. 648 c.p.)

Il fatto materiale consiste nell'acquistare, ricevere od occultare denaro o cose provenienti da qualsiasi delitto, ovvero nell'intromettersi nel farli acquistare, ricevere o occultare da terzi, con la consapevolezza della provenienza illecita del bene ricevuto ed al fine di procurare a sé o ad altri un profitto (dolo specifico).

Riciclaggio (Art. 648-bis c.p.)

La condotta tipica del reato presenta una triplice modalità di commissione: la sostituzione di denaro, beni o altra utilità di provenienza delittuosa, il trasferimento o il compimento di qualsiasi operazione rivolta ad ostacolare l'identificazione della provenienza. La commissione del reato presuppone la volontaria esecuzione di una delle operazioni tipiche, con la consapevolezza della provenienza delittuosa del bene (dolo generico).

Impiego di denaro, beni o utilità di provenienza illecita (Art. 648-ter c.p.)

La fattispecie mira a prevenire l'integrazione nei circuiti economici di denaro di provenienza illecita, mediante l'immissione nelle strutture dell'economia legale di capitali preventivamente ripuliti. La norma ha carattere sussidiario rispetto alle disposizioni di cui agli artt. 648 e 648bis del codice penale e trova quindi un ambito di applicabilità piuttosto limitato. Il reato presuppone la consapevolezza della provenienza illecita dei capitali impiegati (dolo generico).

IV.2.3 Sanzioni ex D.lgs.231/2001

Descrizione Reato	Sanzioni pecuniarie n. quote (*)	Sanzioni interdittive	Pubblicazione sentenza e confisca
False comunicazioni sociali art. 2621 del Codice Civile (CC) art. 2622 1°c. del CC art. 2622 3°c. del CC	 Da 100 a 150 Da 150 a 330 Da 200 a 400	NO	NO
Indebita restituzione dei conferimenti (art. 2626 c.c.)	Da 100 a 180	NO	NO
Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)	Da 100 a 130	NO	NO
Operazioni in pregiudizio dei creditori (art. 2629 c.c.)	Da 150 a 330	NO	NO
Formazione fittizia del capitale (art. 2632 c.c.)	Da 100 a180	NO	NO
Impedito controllo (art. 2625 c.c.)	Da 100 a 180	NO	NO
Illecita influenza sull'assemblea (art. 2636 c.c.)	Da 150 a 330	NO	NO
Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)	Da 200 a 400	NO	NO
Ricettazione (art. 648 CP), Riciclaggio (art. 648 bis), impiego di denaro beni e utilità di provenienza illecita (art. 648 ter).	Da 800 a 1000	SI	SI

(*) il valore della quota è stabilito dal giudice da un minimo di €. 258 a un massimo di €. 1549

IV.3 LA VALUTAZIONE DEI RISCHI

La valutazione dei rischi ha consentito di individuare le aree sensibili alla commissione dei reati "societari" e di "ricettazione, riciclaggio e impiego di capitali illeciti", di identificare e valutare i potenziali eventi in cui Terni Reti potrebbe essere considerata responsabile per reati commessi nel suo interesse o a suo vantaggio.

In sintesi sono state considerate le seguenti aree/attività sensibili ai rischi di reati societari:

REF	MACRO ATTIVITÀ SENSIBILE
1a - B	Amministrazione e contabilità - Ciclo Passivo.
1b - B	Amministrazione e contabilità - Ciclo Attivo.
1c - B	Amministrazione e contabilità - Ciclo di vita dei Cespiti.
1d - B	Amministrazione e contabilità - Gestione delle risorse finanziarie e della tesoreria
2a - B	Formazione del Bilancio di esercizio
3a - B	Altre attività – Rapporti con il Collegio Sindacale e i rappresentanti dell'Amministrazione Vigilante
3b - B	Altre Attività – Preparazione e svolgimento delle Assemblee dei Soci
3c - B	Altre Attività – Operazioni straordinarie .
3d - B	Altre Attività – Comunicazione al pubblico delle informazioni finanziarie
4 - B	Verifiche anti riciclaggio ex D.lgs. 231/2007

Il livello di rischio per tutti i potenziali comportamenti delittuosi esaminati è stato valutato "trascurabile" in considerazione dell'azione svolta da Terni Reti per rafforzare i presidi di controllo di tipo trasversale e dei controlli cui è sottoposta come società patrimoniale dell'Ente socio, affidatario di servizi "*in house*", nonché degli importi singolarmente poco significativi delle transazioni eseguite e della presenza di prassi consolidate nelle aree sensibili.

Tuttavia, a scopo unicamente preventivo e in relazione ad una potenziale estensione dell'attività della Società, è stato programmato l'aggiornamento o l'emanazione di nuove procedure, l'istituzione di controlli e l'adozione di strumenti, come specificato nell'allegato "Piano d'azione Area Amministrazione", allo scopo di formalizzare il sistema dei controlli esistenti e adeguarlo nei casi in cui ne è stata ravvisata l'utilità.

Di seguito, per ogni area sensibile è riportata una breve descrizione del processo/attività, l'elenco dei rischi di reato che, in via del tutto ipotetica, possono essere compiuti, il sistema di prevenzione esistente e le azioni programmate.

IV.4 LE AREE SENSIBILI E IL SISTEMA DEI CONTROLLI ESISTENTI – SICUREZZA SUL LAVORO

IV.4.1 Amministrazione e contabilità

La contabilità è supportata da un apposito sistema informatico denominato B.POINT di proprietà di OSRA Srl unipersonale che consente di gestire le scritture contabili e gli adempimenti periodici IVA, comprese le relative dichiarazioni, di elaborare il bilancio con la possibilità di acquisire dati da altre procedure o da Excel, di operare le rettifiche contabili generate in automatico e di controllare la quadratura delle imposte.

Sono considerati a rischio teorico di commissione dei reati ex D.lgs. 231/2001 i seguenti processi amministrativo contabili: ciclo passivo; ciclo attivo, ciclo di vita dei cespiti e gestione finanziaria.

I rischi di commissione di reati di false comunicazioni sociali (art. 25 ter) e riciclaggio ricettazione e impiego di denaro beni e utilità di provenienza illecita (art. 25 octies), sono i seguenti:

- rilascio di dati contabili, valutazioni o altre informazioni non veritiere che confluiscono nel bilancio o nelle altre comunicazioni sociali per avvantaggiare la società (anche in concorso con i vertici aziendali);
- acquisto di beni di inventario come beni di consumo oppure svalutazione/radiazione di cespiti da utilizzare quale provvista per la corruzione di pubblici ufficiali o incaricati di pubblico servizio;
- incasso consapevole di denaro di provenienza delittuosa oppure compimento di operazioni in relazione ad esso volte ad ostacolare l'identificazione della loro provenienza.
- le diverse operazioni societarie che possono incidere sulla integrità del capitale sociale.

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le “misure” descritte nella Parte Generale del presente Modello, tra cui in particolare:

- il Codice Etico al § 3.10 “Eticità nella comunicazione d’informazioni economiche, patrimoniali e finanziarie”;
- gli obblighi di trasparenza ex D.lgs. 33/2013;
- “il controllo delle registrazioni” tramite il protocollo informatico aziendale che consente di tenere traccia con data certa della documentazione gestionale a supporto delle registrazioni contabili.

Inoltre, si segnala la rilevanza della revisione contabile affidata al Collegio Sindacale e del controllo contabile su singoli aspetti esercitato dal competente Ufficio del Comune di Terni, quale Amministrazione vigilante; nonché l’esistenza di un buon controllo organizzativo che agisce

attraverso le autorizzazioni o approvazioni dell'AU/Direttore generale (secondo competenza) e la separazione delle funzioni operative da quelle di controllo (in particolare attraverso la registrazione in protocollo di documenti contabili e gestionali).

Da ultimo la regolamentazione deli cicli, attraverso prassi consolidate, nel rispetto delle disposizioni di legge e in applicazione dei corretti principi contabili, adeguatamente supportate dal sistema informatico B.POINT in cui sono funzionanti adeguati controlli (ad esempio accoppiamento incasso o pagamento con le relative fatture).

Ciclo Passivo: l'Area amministrativa, dopo aver verificato la conformità degli importi fatturati con il relativo contratto/ordine di acquisto, procede alla registrazione del documento contabile nel sistema di contabilità con assegnazione di un numero progressivo automatico. Il Report riepilogativo dei fornitori da pagare, esclusivamente da pagare con bonifico bancario, è sottoscritto per approvazione dall'Amministratore Unico dopo l'effettuazione dei controlli previsti (morosità, regolarità contributiva, CIG ecc.).
La contabile in formato cartaceo dell'Istituto di credito viene protocollata ed assegnata alla Direzione Generale e all'Area amministrativa; quest'ultima effettua la registrazione nel sistema contabile con accoppiamento alla fattura.

Il Ciclo attivo trae origine dai rapporti contrattuali formalmente istaurati con i clienti. Le fatture attive sono elaborate dal sistema contabile, nel rispetto dei tempi di fatturazione stabiliti in contratto, numerate progressivamente in automatico e inviate tramite posta certificata ai clienti, previa registrazione nel protocollo aziendale con assegnazione (per la visione) alla Direzione Generale e Responsabile del servizio.

I documenti emessi verso la Pubblica Amministrazione devono rispettare i requisisti previsti dalla normativa vigente in materia di fatturazione elettronica. Il documento deve essere emesso in formato xml e l'autenticità ed integrità del contenuto sono garantite tramite l'apposizione della firma elettronica qualificata dell'Amministratore Unico in rappresentanza della Società. L'invio del documento è vincolato dalla presenza del codice identificativo univoco dell'ufficio destinatario e la trasmissione avviene attraverso il sistema informatico denominato di Interscambio (SdI) che effettua tutti i controlli necessari per garantire il successivo corretto inoltro alla P.A.

Ogni fattura evidenzia l'IBAN del c/c intestato alla Società su cui deve essere effettuato il pagamento.
La verifica degli incassi da altri clienti è eseguito tempestivamente dall'Area amministrativa tramite il sistema di *home banking*: pervenuta la contabile cartacea di accredito, regolarmente protocollata all'arrivo, l'Area amministrativa effettua le registrazione nel sistema contabile, attribuendo l'incasso alla fattura effettivamente liquidata.

Gestione finanziaria: le "riconciliazione bancarie" delle movimentazioni dei conti correnti sono effettuate giornalmente dall'Area amministrativa che provvede a comunicare i saldi contabili alla Direzione Societaria.

Trimestralmente il Collegio Sindacale controlla le movimentazioni delle schede contabili intestate agli Istituti di credito, in cui vengono registrate le entrate e le uscite, confrontandole con gli estratti conti bancari per verificarne la corrispondenza.

Azioni programmate: sulla base delle prassi esistenti saranno elaborate le procedure riguardanti il ciclo attivo (fatturazione e incasso), il ciclo passivo (ordine, entrata merci, liquidazione fattura e pagamento) e il ciclo di vita dei cespiti (acquisizione, dismissione, etichettatura e inventariazione).

Inoltre, allo scopo di prevenire reati di riciclaggio, seppure del tutto ipotetici, la verifica della regolarità dei pagamenti dovrà prevedere il controllo puntuale della piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni, nonché la sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.). o eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie.

Sarà emanata una procedura per la gestione finanziaria e di tesoreria, funzionale anche alla prevenzione dei reati di corruzione, che prevederà l'adozione di soglie più stringenti per i pagamenti per contanti (500,00 euro) ed escluderà l'utilizzo di libretti al portatore o anonimi per la gestione della liquidità. ecc..

I controlli sui pagamenti a terzi dovranno riguardare anche gli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese), allo scopo di prevenire ipotetici rischi di riciclaggio.

IV.4.2 La formazione del bilancio.

Il processo di formazione del bilancio riguarda le attività amministrativo-contabili e i relativi controlli, svolti all'interno della Società, inerenti le modifiche al piano dei conti, la definizione delle tempistiche e delle responsabilità per le attività di chiusura contabile, l'analisi del bilancio di verifica, le scritture contabili di accertamento di costi e ricavi di competenza e di assestamento di bilancio, le procedure di riconciliazione dei saldi contabili con i dettagli gestionali, la raccolta degli elementi per le Note al bilancio e di informazioni per la Relazione sulla gestione, la predisposizione del progetto di bilancio e le attestazioni di conformità.

In Terni Reti l'elaborazione del bilancio è supportata dal sistema B.POINT.

Nell'ambito del processo sono considerate a rischio teorico di commissione dei reati ex D.lgs. 231 le seguenti fasi:

- analisi del bilancio di verifica e modifiche al piano dei conti;

- scritture contabili di accertamento di costi e ricavi di competenza;
- scritture contabili tipiche di chiusura e assestamento di bilancio;
- riconciliazione dei saldi contabili con i dettagli gestionali;
- raccolta elementi di dettaglio per le Note al bilancio e di informazione per la Relazione sulla gestione;
- predisposizione del progetto di bilancio.

I rischi inerenti il processo, considerati in ottica strumentale alla commissione di reati di false comunicazioni sociali (art. 25ter) sono i seguenti:

- rilascio di dati contabili, valutazioni o altre informazioni non veritiere che confluiscono nel bilancio o nelle altre comunicazioni sociali per avvantaggiare la società (anche in concorso con i vertici aziendali);
- rilascio di informazioni false od omissione di informazioni imposte dalla legge sulla situazione finanziaria della società (anche in concorso con i vertici aziendali).

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le "misure" descritte nella Parte Generale del presente Modello, tra cui in particolare:

- il Codice Etico al § 3.10 "Eticità nella comunicazione d'informazioni economiche, patrimoniali e finanziarie",
- gli obblighi di trasparenza ex D.lgs. 33/2013;
- "il controllo delle registrazioni" tramite il protocollo informatico aziendale che consente di tenere traccia con data certa della documentazione gestionale a supporto delle registrazioni contabili e delle valutazioni.

Inoltre, si segnala la rilevanza della revisione contabile affidata al Collegio Sindacale e del controllo contabile su singoli aspetti esercitato dal competente Ufficio del Comune di Terni, quale amministrazione vigilante.

Da ultimo la regolamentazione del processo di formazione del bilancio attraverso prassi consolidate e il Manuale utente di B.POINT che descrive le operazioni di chiusura.

I controlli interni attualmente esistenti sono i seguenti:

- trasmissione al Collegio Sindacale del libro giornale, bilancio di verifica e schede partitari per le verifiche di competenza;
- raccolta ordinata (per tipo di operazione) della documentazione, dei fogli di calcolo e dei controlli eseguiti archiviati presso Area Amministrazione;
- approvazione dell'Amministratore Unico del bilancio di verifica, previa verifica di coerenza delle relative stime, e della corretta allocazione negli appositi conti dei saldi delle partite aperte nei conti "fatture da ricevere/emettere";

- attestazione del responsabile di Area Amministrazione, previa verifica del Direttore Generale, della completezza e correttezza dei saldi di bilancio, dei dettagli riportati sulle Note al bilancio e delle informazioni e dei dati contenuti nella Relazione sulla gestione;
- presentazione del Progetto di Bilancio al Collegio Sindacale, che dovrà verificare la congruità dei prospetti contabili e la loro conformità con le norme di legge e i principi contabili;
- approvazione del bilancio di esercizio dall'Assemblea dei Soci e deposito presso l'Ufficio del Registro delle Imprese

Azioni programmate: emissione della procedura di Formazione del bilancio di esercizio.

Verifica annuale delle variazioni apportate nel piano dei conti della contabilità generale con il Collegio Sindacale.

Attestazione della data di avvenuta "chiusura contabile" tramite stampa del relativo report di sistema e registrazione al protocollo informatico.

IV.4.3 Altre Attività sensibili

RAPPORTI CON IL COLLEGIO SINDACALE E I RAPPRESENTANTI DELL'AMMINISTRAZIONE VIGILANTE

La responsabilità della gestione dei rapporti con il Collegio Sindacale e con la Direzione Partecipate del Comune di Terni è attribuita al Responsabile Area Amministrativa supervisionata dall'Amministratore Unico.

L'attività consiste nell'evasione tempestiva ed esaustiva delle richieste pervenute e di fornire informazioni veritiere e corrette.

Il rischio inerente il processo, considerato in ottica strumentale alla commissione di reati di impedito controllo (art. 25ter) è il seguente:

- occultamento di documenti richiesti / necessari ai controlli del Collegio dei revisori, dei Soci, dell'amministrazione vigilante (e concorso con i vertici aziendali).

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le "misure" descritte nella Parte Generale del presente Modello, tra cui in particolare.

- il Codice Etico al § 3.10 "Eticità nella comunicazione d'informazioni economiche, patrimoniali e finanziarie";
- gli obblighi di trasparenza ex D.lgs. 33/2013;
- "il controllo delle registrazioni" tramite il protocollo informatico aziendale che consente di tenere traccia con data certa ed una pronta disponibilità delle richieste pervenute e delle relative risposte. In particolare:

- le richieste ricevute dal Collegio Sindacale sono protocollate, riepilogate, con indicazione delle date di richiesta, di evasione attesa e di effettiva evasione,;
- le richieste riguardanti i dati contabili sono inviate direttamente via email al Responsabile Area Amministrazione che inoltra la richiesta e la relativa risposta all'Amministratore Unico e Direttore Generale per il monitoraggio;
- le richieste di accesso alle informazioni da parte dei rappresentanti dell'Amministrazione vigilante sono acquisite direttamente dall' Amministratore Unico e Direttore Generale, immesse nel protocollo informatico ed evase con il supporto dell'Area Amministrazione.

Azioni programmate: per agevolare il compito di monitoraggio dell'Amministratore Unico, anche le richieste del Collegio Sindacale inviate direttamente per e-mail al Responsabile Area Amministrazione saranno riepilogate in un documento in cui sarà riportato l'oggetto della richiesta, gli estremi della risposta e le relative date.

PREPARAZIONE E SVOLGIMENTO DELLE ASSEMBLEE DEI SOCI

L'Amministratore Unico è responsabile dell'assolvimento dell'obbligo di trasmissione preventiva della documentazione connessa con l'ordine del giorno dell'evento societario, assicurando che la stessa sia fornita in maniera completa, adeguata e con il necessario anticipo.

I rischi inerenti l'attività, considerati in ottica strumentale alla commissione di reati di impedito controllo e illecita influenza sull'Assemblea (art. 25ter) sono i seguenti:

- occultamento di documenti richiesti / necessari ai controlli dei Soci;
- manipolazione di informazioni e dati relativi a delibere da assumere in Assemblea.

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le "misure" descritte nella Parte Generale del presente Modello, tra cui in particolare:

- il Codice Etico al § 3.10 "Eticità nella comunicazione d'informazioni economiche, patrimoniali e finanziarie",
- gli obblighi di trasparenza ex D.lgs. 33/2013
- "il controllo delle registrazioni" tramite il protocollo informatico aziendale che consente di tenere traccia con data certa ed una pronta disponibilità delle richieste pervenute e delle relative risposte.

Inoltre, è ritenuto essenziale per il sistema dei controlli il coinvolgimento operativo dell'Area Amministrativa, di supporto all'Amministratore Unico, nella raccolta della documentazione e nell'inoltro ai Soci e al Collegio Sindacale.

OPERAZIONI STRAORDINARIE (CON EFFETTI SULLA CONSISTENZA PATRIMONIALE DELLA SOCIETÀ)

Il piano di razionalizzazione delle società partecipate, approvato dal Comune di Terni a marzo 2015, aveva individuato Terni Reti come società patrimoniale dell'Amministrazione Comunale a cui trasferire gli *asset* del patrimonio comunale per l'espletamento dei servizi pubblici locali ad essi riconducibili.

L'approvazione del Piano Strategico societario e del nuovo statuto, avvenuta con delibera di Consiglio Comunale n. 502 del 16 novembre 2015, ha avviato tale processo di trasformazione di Terni Reti, che vedrà il suo completamento con il conferimento nel capitale sociale dei beni patrimoniali comunali strumentali alla gestione dei servizi pubblici affidati.

Sistema dei controlli esistente: in questa circostanza, come pure nella fase finale di trasferimento di *asset* del patrimonio comunale in corso di svolgimento, Terni Reti si è attenuta e si atterrà alle seguenti prescrizioni minime:

- le "proposte" di operazioni straordinarie sono sottoposte all'approvazione dell'Assemblea dei Soci, in conformità ai requisiti statutari e alle prescrizioni del codice civile e delle normative applicabili al settore;
- le strutture aziendali competenti devono essere coinvolte attivamente nell'istruttoria e nell'affidamento dei relativi studi di fattibilità seppure condotti da consulenti;
- i suddetti studi sono sottoposti alla supervisione degli Uffici preposti dell'Amministrazione vigilante;
- le informazioni eventualmente necessarie per l'elaborazione di situazioni previsionali di carattere economico, patrimoniale e finanziario sono fornite dall'Amministratore Unico con il supporto dell'Area Amministrativa che ne assicura la congruenza e la correttezza.

COMUNICAZIONE AL PUBBLICO DI INFORMAZIONI FINANZIARIE, CIRCA I FATTI DELLA SFERA DI ATTIVITÀ AZIENDALE

I comunicati stampa che riguardano i fatti della sfera di attività aziendale potenzialmente idonei ad avere un effetto sulla reputazione e sul valore della Società sono effettuati dall'Amministratore Unico.

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le "misure" descritte nella Parte Generale del presente Modello, tra cui in particolare il Codice Etico:

- § 2.5. "Riservatezza",
- § 3.10 "Eticità nella comunicazione d'informazioni economiche, patrimoniali e finanziarie",

- § 3.11 ”Eticità nei rapporti con i mass media”,
- § 3.12 “Trattamento delle informazioni riservate e privilegiate”.

Inoltre, il corretto adempimento degli obblighi di trasparenza ex D.lgs. 33/2013 attenua ulteriormente il rischio.

VERIFICHE ANTIRICICLAGGIO EX D.LGS. 231/2007

La Società non ha mai istaurato rapporti commerciali o di partenariato con Soggetti aventi domicilio fiscale in Paesi Black List o a rischio terrorismo, o che si avvalgono di istituti di credito che non hanno insediamenti fisici in alcun Paese o di strutture fiduciarie o con Soggetti che, comunque, rientrano negli indicatori di anomalia elaborati dalla Banca d’Italia pubblicati il 24 agosto 2010.

Tuttavia, come già specificato nel sistema dei controlli esistente nell’area amministrativa all’occorrenza si atterrà alle seguenti prescrizioni:

- verifica dell’identità, dell’attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari;
- i pagamenti a terzi dovranno prevedere preventivi controlli sulla sede legale degli Istituti di credito utilizzati al fine di escludere banche che non hanno insediamenti fisici in alcun Paese.

ALLEGATO AL MOG PARTE SPECIALE B

PIANO DI AZIONE - AREA AMMINISTRAZIONE

#	Descrizione dell'azione pianificata	Responsabile	Data pianificata	Data attuazione
MOG-B. 1	**Procedure del ciclo attivo (fatturazione e incasso).**	Resp. Area Amministrativa	I semestre 2017	
MOG-B. 2	**Procedura del ciclo passivo (ordine, entrata merci, liquidazione fattura e pagamento)** Allo scopo di prevenire reati di riciclaggio, introdurre controlli di adeguata verifica ex D.lgs. 231/2007 (piena coincidenza tra ordinanti dei pagamenti e controparti, sede legale o eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie.	Resp. Area Pianificazione e Controllo / Resp. Area Amministrativa	I semestre 2017	
MOG-B. 3	**Procedura del ciclo di vita dei cespiti e inventario fisico/contabile** (acquisizione, dismissione, etichettatura e inventariazione).	Resp. Area Amministrativa	I semestre 2017	
MOG-B. 4	**Procedura per la gestione finanziaria** Ai fini della normativa antiriciclaggio deve prevedere soglie per i pagamenti per contanti, di utilizzo di libretti al portatore o anonimi per la gestione della liquidità.	Resp. Area Amministrativa	I semestre 2017	
MOG-B. 5	**Procedura di Formazione del bilancio di esercizio (e dei periodi intermedi).** La procedura deve contenere un modello di "Elenco annuale delle variazioni al Piano dei Conti" - nuovi conti aperti e conti di Terni Reti nell'anno da registrare al protocollo informatico. Inoltre deve prevedere la registrazione al protocollo informatico della "Certificazione data di avvenuta chiusura contabile".	Resp. Area Amministrativa	I semestre 2017	
MOG-B.6	**Documento riepilogativo richieste del Collegio Sindacale inviate per e-mail direttamente al Responsabile Area Amministrazione** Per agevolare il compito di monitoraggio del Direttore, saranno riepilogate in un documento in cui sarà riportato l'oggetto della richiesta, gli estremi della risposta e le relative date.	Resp. Area Amministrativa	I semestre 2017	

V - MOG PARTE SPECIALE C - "Reati informatici e in materia di violazione del diritto d'autore".

V.1 INTRODUZIONE

Anche se le due tipologie di reati trattate in questa parte del Modello tutelano interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Parte Speciale in quanto:

- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei destinatari del Modello in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

Di seguito si fornisce, quindi, separatamente l'elencazione dei delitti informatici e trattamento illecito di dati (artt. 24-bis) e in violazione del diritto d'autore (art. 25-novies).

V.2 RISCHI DI REATO (da Catalogo dei reati)

V.2.1 Reati informatici e trattamento illecito di dati ex art. 24 bis D.lgs. 231/2001

ILLECITO TRATTAMENTO DEI DATI

Falsità di documento informatico (art. 491bis c.p.)

L'articolo estende le disposizioni sui reati di falso documentale (atto pubblico o scrittura privata) ai documenti informatici pubblici o privati aventi efficacia probatoria, integrando le fattispecie di reato previste dagli articoli da 476 a 493 del codice penale (Capo III del titolo VII). Il bene giuridico tutelato è la fede pubblica documentale, si tratta cioè di quella particolare fiducia che la collettività ripone sulla veridicità o autenticità di un documento.

I reati previsti sono i seguenti:

- falsità materiale o ideologica commessa dal pubblico ufficiale in atti pubblici;
- falsità materiale o ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative ;
- falsità materiale o ideologica commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti;
- falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità;
- falsità ideologica commessa dal privato in atto pubblico;

- falsità in registri e notificazioni;
- falsità in scrittura privata;
- falsità in foglio firmato in bianco. Atto privato e atto pubblico;
- uso di atto falso;
- soppressione, distruzione e occultamento di atti veri;
- copie autentiche che tengono luogo degli originali mancanti;
- falsità commesse da pubblici impiegati incaricati di un servizio pubblico.

Per documento informatico si intende qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; i documenti informatici rilevanti ai fini delle norme in questione sono quelli pubblici o privati, dotati di efficacia probatoria, cioè con firma elettronica qualificata o emessi nel rispetto di quelle regole tecniche[2] finalizzate a garantirne paternità, provenienza, integrità e immodificabilità.

Occorre sottolineare che anche un soggetto che non riveste le qualifiche richieste per la commissione dei reati propri può commettere il reato in concorso con il pubblico ufficiale o l'incaricato di un pubblico servizio.

DELITTI INFORMATICI PROPRIAMENTE DETTI

Accesso abusivo ad un sistema informatico o telematico (artt. 615 ter e quater c.p.)

L'accesso abusivo si realizza attraverso l'introduzione non autorizzata in un sistema informatico o telematico protetto da misure di sicurezza ovvero il mantenersi nel sistema contro la volontà di chi ha il diritto di esclusione.

Con riferimento alla prima condotta considerata, il reato si perfeziona con la violazione del sistema attuata attraverso la forzatura delle misure di sicurezza atte a proteggerlo[3].

La seconda condotta si configura nel caso di accesso ad un'area del sistema (ad es. area del server o directory) diversa da quella cui si è autorizzati ad accedere.

Reato preparatorio all'accesso abusivo è la detenzione e diffusione abusiva di codici di accesso ai sistemi (art. 615 quater).

Intercettazione, impedimento e interruzione di comunicazioni informatiche o telematiche (artt. 617 quater e quinquies c.p.)

Il reato sanziona chiunque fraudolentemente intercetta, impedisce o interrompe comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, nonché chiunque rivela tali comunicazioni mediante qualsiasi mezzo di informazione al pubblico.

[2] Può trattarsi di qualunque atto scritto, file o altro contenuto di un programma informatico, del quale sia riconoscibile l'autore che in esso si palesa, contenente una dichiarazioni di scienza (esposizione di dati o fatti) o manifestazioni di volontà.

[3] In giurisprudenza prevale la tesi di considerare fra le misure di sicurezza non solo le protezioni di tipo logico (ad es. password) ma anche quelle fisiche esterne al sistema (ad es. meccanismi di selezione dell'accesso ai locali in cui sono collocati i sistemi).

A titolo esemplificativo, le intercettazioni di comunicazioni possono essere attuate attraverso *spyware*, che consentono di acquisire informazioni dal sistema oggetto di attacco, mentre si configura impedimento (o rallentamento) o interruzione di comunicazioni in caso di interventi fraudolenti su pagine *web* o blocchi di server di posta elettronica.
È punita inoltre l'installazione di apparecchiature atte a porre in essere una delle condotte sopra indicate. (art.617 quinquies).

Danneggiamento informatico (artt. 635 bis, ter, quater e quinquies e artt. 615 quinquies e 617 quinquies c.p.)
Sono delineate quattro fattispecie di reato distinte in base alla rilevanza (pubblica o privata) di "informazioni, dati, programmi informatici", costituiti dai *file* di dati e dai software per la generazione ed elaborazione degli stessi, e di "sistemi informatici e telematici" (elaboratori, ivi compresi palmari, cellulari, ecc.).
Per quanto concerne il danneggiamento di "informazioni, dati e programmi informatici", le condotte illecite considerate sono: la distruzione, il deterioramento, la cancellazione, l'alterazione e la soppressione.
Nel danneggiamento di "sistemi informatici e telematici" sono puniti: la distruzione, il danneggiamento, il rendere inservibile o l'ostacolare gravemente il funzionamento del sistema.
Infine, sono autonomamente sanzionate una serie di condotte prodromiche al danneggiamento, che si sostanziano nella diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare i sistemi o i dati (artt. 615 quinquies e 617 quinquies).

V.2.2 Reati in violazione dei diritto d'autore ex art. 25 octies D.lgs.231/2001.

L. 22 aprile 1941, n. 633, art. 171 1° comma lettera a-bis) e terzo comma
Salvo quanto previsto dall'art. 171 bis e dall'art. 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, 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.

L. 22 aprile 1941, n. 633, art. 171 bis
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 (S.I.A.E.), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493.

L. 22 aprile 1941, n. 633, art. 171 ter
È 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 a euro 15.493 chiunque a fini di lucro 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.

L. 22 aprile 1941, n. 633, art. 171 septies

La pena di cui all'articolo 171 ter, comma 1, si applica anche ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181 bis, i quali non comunicano alla S.I.A.E. entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi.

L. 22 aprile 1941, n. 633, art. 171 octies

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 a euro 25.822 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.

V.2.3 Sanzioni ex D.lgs.231/200

Descrizione Reato	Sanzioni pecuniarie n. quote (*)	Sanzioni interdittive	Pubblicazione sentenza e confisca
Accesso abusivo ad un sistema informatico o telematico (artt. 615 ter) Detenzione abusiva di codici di accesso e apparecchiature (615 quater e quinquies c.p.)	Da 100 a 500 Da 100 a 300	SI	SI
Intercettazione, impedimento e interruzione di comunicazioni informatiche o telematiche (art. 617 quater) Istallazione di apparecchiature atte a … (art. 617 quinquies c.p.).	Da 100 a 500 Da 100 a 500	SI	SI
Danneggiamento informatico (artt. 635 bis, ter, quater e quinquies c.p.) Diffusione apparecchiature o programmi diretti a danneggiare art 615 quinquies c.p.)	Da 100 a 500 Da 100 a 300	SI	SI
Delitti in violazione del diritto d'autore (articoli 171, primo), e terzo comma, 171-bis, 171-ter, 171- septies e 171-octies della legge 22 aprile 1941, n. 633)	Da 100 a 500	SI (**)	SI

(*) il valore della quota è stabilito dal giudice da un minimo di €. 258 a un massimo di €. 1549.

(**) Per una durata non superiore a un anno.

V.3 LA VALUTAZIONE DEI RISCHI

In astratto la possibilità di commissione di un reato informatico è connessa all'utilizzo di strumenti informatici da parte di soggetti appartenenti alla Società.

Considerato il diffuso impiego delle tecnologie nello svolgimento delle attività aziendali, a livello teorico sono sensibili la maggior parte dei processi societari, pertanto, il personale di tutte le Aree che gestiscono e utilizzano sistemi informativi hanno comunque una reale e concreta esposizione al rischio di reati informatici.

Inoltre, è ragionevole ritenere che il processo societario maggiormente esposto al rischio di commissione dei reati sopra indicati, soprattutto in considerazione delle competenze specialistiche possedute dalle risorse ad esso dedicate, è quello che governa i sistemi informatici aziendali e l'utilizzo delle reti informatiche.

In sintesi sono state considerate le seguenti aree/attività sensibili ai reati informatici e di trattamento illecito di dati e in violazione del diritto d'autore:

REF	MACRO ATTIVITÀ SENSIBILE
1 - C	Gestione servizi informativi e del sito internet.
2 - C	Tutte le attività aziendali nelle quali è previsto l'utilizzo di servizi informatici (posta elettronica e internet).
3 - C	Gestione documentale
4- C	Utilizzo della firma digitale

Tuttavia, si può ragionevolmente ritenere che il livello di rischio del verificarsi di condotte che integrino le fattispecie di reato trattate in questa parte speciale sia valutabile come "trascurabile" in considerazione di quanto prescritto nel Codice Etico § 3.14 "trattamento delle informazioni riservate e previlegiate" e dei presidi di carattere trasversale trattati nella Parte Generale del MOG e, in particolare e nel Cap II.4 "Gestione della sicurezza informatica", che traggono origine dal sistema organizzato per gli adempimenti ex L.196/2004 "Codice della Privacy" ritenuti efficaci a ostacolare il rischio di un coinvolgimento dell'ente per comportamenti che costituiscano reati presupposto ex D.lgs.231/2001.

Ciononostante, come specificato in seguito e riportato nel "Piano d'azione - Area Adempimenti Privacy e Sicurezza Informatica", a scopo unicamente preventivo e nei casi in cui ne è stata ravvisata l'utilità, è stata programmata l'emanazione di Istruzioni e Disciplinari *ad hoc* ad integrazione di quanto già presente nel Codice Etico, nonché l'istituzione di controlli e l'adozione di strumenti, allo scopo di migliorare il sistema dei controlli esistenti.

Di seguito, per ogni area sensibile sono riportati l'elenco dei rischi di reato che in via del tutto ipotetica possono essere compiuti, il sistema di prevenzione esistente e le azioni programmate.

V.4 LE AREE SENSIBILI E IL SISTEMA DEI CONTROLLI ESISTENTI

V.4.1 Gestione dei sistemi informativi

La gestione dei sistemi informativi aziendali è finalizzata ad assicurare il funzionamento e la manutenzione dell'hardware e del software, degli apparati e delle reti di trasmissione dati e di connessione alla internet, l'evoluzione della piattaforma tecnologica e applicativa IT, nonché la sicurezza informatica, la gestione del sito internet e dei servizi di posta elettronica, l'acquisizione ed istallazione di software nelle postazioni di lavoro.

I rischi di commissione di reati di frode informatica a danno dello Stato e degli enti pubblici, di reati informatici e di trattamento illecito di dati e di reati in violazione del diritto d'autore (artt. 24 bis e 25 novies del D.lgs. 231) sono i seguenti:

- manipolazione di documento informatico di terzi per avvantaggiare un soggetto particolare;
- accesso in un sistema informatico volto all'acquisizione di informazioni contenute in banche dati di terzi, strumentale alla commissione di frodi o di atti concorrenza sleale.
- impedimento o interruzione di un servizio web di terzi strumentale ad atti di concorrenze sleale;
- l'installazione e l'utilizzo di programmi per elaboratore nonché la gestione dei contenuti del sito internet in violazione del diritto d'autore.

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le seguenti "misure" di carattere trasversale:

- Codice Etico in cui sono declinati i valori dei valori etici di Integrità, Legalità, Trasparenza e Riservatezza nonché nei principi di comportamento enunciati § 3.14 "trattamento delle informazioni riservate e previlegiate";
- MOG Parte Generale al Cap II.4 "Gestione della sicurezza informatica".

Riguardo alle azioni organizzative e gestionali previste al Cap. II.4 del MOG assumono particolare rilevanza la formale adozione delle "Misure minime di sicurezza informatica" ex D.lgs..196/2003 tra cui l'esistenza di:

- adeguate profilazioni (amministratore di sistema e utenti);
- blocchi logici nei sistemi atti a impedire istallazione di software, connessione con dispositivi diversi da quelli aziendali, utilizzo di sistemi di diagnostica per identificare le vulnerabilità,

decifrare i file criptati, intercettare il traffico in transito e le modifiche alle configurazioni delle postazioni di lavoro;
- sistemi firewall e antivirus volti ad impedire l'uno l'accesso informatico non autorizzato ed eventuali minacce causate da virus contratti dall'utilizzo della rete internet;
- servizio di posta elettronica gestito da un soggetto esterno che garantisce standard qualitativi elevati per quanto concerne la protezione dei dati digitali;
- autenticazione utenti gestito attraverso un sistema di credenziali (nome utente e password[4])
- sistema di backup dei dati presso idonee strutture, esterne ai locali della Società Stessa.

Azioni programmate: emissione del "Disciplinare tecnico sulla sicurezza informatica" che compendi la policy di sicurezza informatica e le misure di sicurezza adottate, da allegare ai contratti di outsourcing dei servizi di Information & Communication Technology.

Istituzione di un "Giornale dei login dell'Amministratore di sistema" a disposizione della Società e a tutela dell'interessato.

V.4.2 Tutte le attività svolte con risorse informatiche della Società

Hanno una reale esposizione al rischio di commissione di reati informatici tutti i destinatari del Modello, in possesso di avanzate competenze informatiche, che svolgono le attività aziendali loro assegnate utilizzando postazioni di lavoro con accesso diretto a risorse informatiche della Società, quali in particolare il servizio di posta elettronica e internet.

I rischi di illecito trattamento dei dati e di reati informatici propriamente detti ex art. 24 bis del D.lgs. 231/2001 sono i seguenti:

- accedere a un sistema informatico allo scopo di acquisire informazioni contenute in banche dati di terzi, strumentale alla commissione di frodi o di atti concorrenza sleale;
- impedire o interrompere un servizio web di terzi strumentale ad atti di concorrenze sleale;
- formare o concorrere a formare, con un pubblico ufficiale o incaricato di pubblico servizio, documenti informatici falsi o alterare atti veri;
- alterare o contraffare, per sé o in concorso con un pubblico ufficiale o incaricato di pubblico servizio, certificati o autorizzazioni amministrative e le relative condizioni di validità, copie in forma legale su documento informatico di un atto pubblico o privato inesistente o una copia diversa dall'originale, un attestato, una falsa attestazione di un fatto o di aver ricevuto dichiarazioni;
- concorrere con un esercente una professione sanitaria o forense o altro servizio di pubblica necessità nell'attestare falsamente, in un certificato sotto forma di

[4] **I**a password rispetta i canoni di sicurezza minimi che saranno stabiliti dal codice del trattamento dati e viene sostituita obbligatoriamente dall'utente nei termini stabiliti dallo stesso Codice

documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità;

- attestare falsamente, oralmente o per iscritto, a un pubblico ufficiale in un atto pubblico, sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità;
- scrivere o lasciare scrivere false indicazioni nelle registrazioni, sotto forma di documento informatico, soggette all'ispezione dell'autorità di Pubblica Sicurezza o nelle notificazioni, sotto forma di documento informatico, alla stessa autorità, riguardanti operazioni industriali, commerciali o professionali;
- formare in tutto o in parte scritture private false, sotto forma di documento informatico, o alterazione di scritture private vere, utilizzandole o lasciando che altri le utilizzino.
- scrivere o far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto privato produttivo di effetti giuridici diversi da quelli previsti, utilizzandolo o lasciando che altri lo utilizzino;
- scrivere o far scrivere, ovvero concorrere con un pubblico ufficiale nello scrivere o nel far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto pubblico diverso da quello a cui il pubblico ufficiale stesso era obbligato o autorizzato.

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le seguenti “misure” di carattere trasversale:

- Codice Etico nel Capitolo II in cui sono declinati i valori dei valori etici di Integrità, Legalità, Trasparenza e Riservatezza e nei principi di comportamento enunciati § 3.14 “trattamento delle informazioni riservate e previlegiate”;
- MOG Parte Generale al Cap II.4 “Gestione della sicurezza informatica”.

Riguardo alle azioni organizzative e gestionali previste al Cap. II.4 del MOG assumono particolare rilevanza gli “Atti di nomina individuali al trattamento dati ex D.lgs. 196/2003”, consegnati a tutto il personale e firmati per accettazione, che prevedono espressi divieti di:

- ottenere credenziali di accesso a sistemi informatici aziendali, dei clienti o di terze parti, senza la previa autorizzazione della Società;
- divulgare, cedere o condividere con altri le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o di terze parti;
- accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri dipendenti o terzi – nonché accedervi al fine di manomettere qualsiasi dato ivi contenuto;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;

- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere;
- acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
- accedere abusivamente al sito Internet della Società al fine di manomettere o alterare qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali (immagini, infografica, video, ecc.) in violazione della normativa sul diritto d'autore e delle procedure aziendali applicabili
- comunicare a persone non autorizzate, interne o esterne, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati
- mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti Virus o altri programmi in grado di danneggiare o intercettare dati, lo spamming come pure ogni azione di risposta al medesimo;
- inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato contenuto in un documento informatico, previa alterazione o falsificazione dei medesimi.

L'informazione e la formazione rivolta a tutto il personale dipendente sulle norme di utilizzo dei sistemi informatici e telematici aziendali e sulle misure di sicurezza, è stata erogata in occasione della presentazione del Codice Etico avvenuta in maggio 2016 e sarà periodicamente ripetuta.

Azione programmata: Elaborare un apposito paragrafo del "Disciplinare tecnico sulle norme di comportamento degli utilizzatori dei sistemi informatici e telematici aziendali" in cui siano dettagliati i divieti inerenti il trattamento illecito dei dati già riportati negli atti di nomina.

V.4.3 La gestione documentale

Il processo riguarda la creazione, la protezione, l'emissione, l'archiviazione, la conservazione, l'eliminazione, la divulgazione, l'immissione in reti informatiche/telematiche di documenti informatici e la manutenzione in genere degli archivi di documenti informatici.

I rischi di illecito trattamento dei dati (art. 24 bis D.lgs. 231/2001) sono i seguenti:

- distruzione, soppressione, occultamento in tutto o in parte di una scrittura privata o un atto pubblico veri, sotto forma di documento informatico;
- manipolazione di documento informatico di terzi per avvantaggiare un soggetto particolare.

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci i seguenti presidi di carattere trasversale:

- MOG Parte Generale, Cap II.4 "Gestione della sicurezza informatica";

- MOG Parte Generale, Cap. II.8 “Trasparenza e tracciabilità” in cui è descritto il processo di gestione documentale, affidato alla Segreteria;
- Codice Etico nel Capitolo II in cui sono declinati i valori dei valori etici di Integrità, Legalità, Trasparenza e Riservatezza.

La gestione è affidata all’Ufficio Segreteria con la collaborazione dell’ufficio Pianificazione e Controllo, Marketing ed Acquisti, avvalendosi del sistema informatico denominato “Isharedoc”.

Il processo è disciplinato da una procedura interna con la quale è stabilito l’organigramma di protocollo (profilazione degli utenti) e le modalità di protocollazione e fascicolazione dei documenti.

Azioni programmate: emissione di una Procedura “protocollazione e archivio” che dovrà evidenziare i rischi ex D.lgs. 231 riguardanti il trattamento illecito dei dati. Detta revisione dovrà essere preceduta da una verifica di completezza e idoneità della procedura stessa riguardo alle modalità di creazione, eventuale protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici.

V.4.4 Utilizzo della Firma Digitale

La Società utilizza la “firma digitale” in tutti i casi in cui l’Amministratore Unico, rappresentante legale, ha la necessità di sottoscrivere documenti informatici.

Tale utilizzo è regolamentato da formale attribuzione e assunzione di responsabilità.

Il rischio di commissione di reato informatico, ex art.24 bis del D.lgs. 231/2001, è il seguente:

- utilizzo abusivo della firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l’utilizzo.

Sistema dei controlli esistente: per la prevenzione/riduzione del rischio sono ritenute ragionevolmente efficaci le seguenti “misure” di carattere trasversale:

- MOG Parte Generale Cap II.4 “Gestione della sicurezza informatica”;
- Codice Etico Cap. II in cui sono enunciati i valori etici di Integrità, Legalità, Trasparenza e Riservatezza, assunti da Terni Reti.

Azioni programmate: elaborare un apposito paragrafo del Disciplinare Tecnico in corso di emanazione in cui siano introdotte le seguenti istruzioni per l’uso della firma digitale:

- è consentito il possesso della firma digitale al solo Amministratore Unico per sottoscrivere documenti informatici nei casi previsti dalla legge o nei casi ritenuti opportuni;
- il sistema hardware e software utilizzato per apporre la firma digitale è composto da: *smart card*, lettore di *smart card*, e software DIKE (Kit rilasciato dalla competente Camera

di commercio). Tale sistema può essere istallato sul personal computer in dotazione al legale rappresentante e/o sul personal computer in dotazione al responsabile dell'Area amministrativa;

- la *smart card* è custodita dal legale rappresentante della Società personalmente o avvalendosi di appositi locali e casseforti presenti nei locali della Società;
- l'utilizzo della firma digitale avviene in presenza del legale rappresentante avvalendosi del supporto operativo del responsabile dell'Area amministrativa o di altri soggetti indicati dal legale rappresentante stesso;
- la Responsabilità per la custodia e l'uso della *smart card* è propria del legale rappresentante.

Dette istruzioni saranno riportate anche nell'atto di formale attribuzione del dispositivo di firma elettronica.

ALLEGATO AL MOG PARTE SPECIALE C

PIANO DI AZIONE - AREA ADEMPIMENTI PRIVACY E SICUREZZA INFORMATICA

#	**Descrizione dell'azione pianificata**	Responsabile	Data pianificata	Data attuazione
MOG-C. 1	"Disciplinare tecnico sulla sicurezza informatica" che compendi la policy di sicurezza informatica e le misure di sicurezza adottate, da allegare ai contratti di outsourcing dei servizi di Information & Communication Technology (V.4.1)	Resp. Privacy	Giugno 2017	
MOG-C. 2	Giornale dei login dell'Amministratore di sistema (V.4.1)	Amministratore di Sistema	Giugno 2017	
MOG-C 3	Disciplinare tecnico sulle norme di comportamento degli utilizzatori dei sistemi informatici e telematici aziendali – paragrafo Divieti reati informatici (V.4.2)	Resp. Privacy	Giugno 2017	
MOG-C. 4	Emissione di una procedura Protocollazione e archivio (Rischi trattamento illecito dei dati). (V.4.3)	Direttore Segreteria	Dicembre 2017	

VI - MOG PARTE SPECIALE D
"Reati in violazione delle norme di sicurezza sul lavoro e di tutela ambientale".

VI.1 INTRODUZIONE

Sicurezza sul Lavoro

L'art. 9 della Legge n. 123 del 3 agosto 2007 (c.d. Legge in materia di tutela della salute e della sicurezza sul lavoro) ha immesso l'art. 25-septies nel D.lgs. n. 231/2001, estendendo la responsabilità amministrativa degli enti ai reati di omicidio colposo e lesioni personali gravi o gravissime[5], con ciò prevedendo per la prima volta la responsabilità anche per reati di natura colposa[6].

La responsabilità prevista dal D.lgs. n. 231/2001 è configurabile solo se dal fatto illecito ne sia derivato un vantaggio per l'ente, che, nel caso di specie, potrebbe essere rinvenuto in un risparmio di costi o di tempi.

Ai fini dell'applicabilità dell'art. 25-septies del D.lgs. n. 231/2001, la responsabilità del datore di lavoro (o del dirigente delegato) è dovuta alla mancata adozione di tutte le misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili alla luce dell'esperienza e delle più avanzate conoscenze tecnico-scientifiche (come specificato dall'art. 3, comma 1, lett. b, del D.lgs. n. 626/1994).

Tutela Ambientale

Con il D.lgs. 121/2011 del 1.8.2011, recante attuazione della Direttiva 2008/99/CE, alcune fattispecie di reati in materia ambientale sono entrati a far parte del novero dei reati presupposto.

I reati introdotti sono quasi tutti di pura condotta, indifferentemente sorretta dal dolo e dalla colpa; la responsabilità investe, quindi, le persone giuridiche per i reati ambientali quando siano stati commessi nel loro interesse o a loro vantaggio.

Nel capitolo seguente si fornisce, separatamente l'elencazione dei delitti di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies) e dei reati ambientali (dell'art. 25 undecies).

[5] L'art. 300 del D.lgs. n. 81/2008 ha modificato l'art. art. 25-septies introducendo criteri di graduazione delle sanzioni previste.

[6] Si tratta di una colpa specifica derivante dall'intenzionalità della sola condotta dell'autore (e non anche dell'evento) in violazione delle procedure e delle disposizioni interne predisposte e puntualmente implementate dall'azienda per prevenire la commissione degli illeciti di cui si tratta o anche soltanto di condotte a tali effetti "pericolose".

Si fa presente che dopo un'attenta valutazione sono stati considerati non applicabili alla Terni Reti S.r.l. Uninominale tutti i reati ambientali ad esclusione di quelli di trattamento dei rifiuti derivanti dalla attività svolta (produzione dei rifiuti)[7].

VI.2 RISCHI DI REATO

VI.2.1 Reati in violazione delle norme di salute e sicurezza sul lavoro (art. 25 septies)

Art. 589 Omicidio colposo.

Art. 590 Lesioni personali colpose.

I reati si configurano in tutti i casi in cui l'agente compie per negligenza, imprudenza, imperizia o violazione di leggi o regolamenti, un atto da cui deriva la morte o le lesioni gravi o gravissime[8] di un lavoratore, per effetto dell'inosservanza di norme antinfortunistiche e sulla salute ed igiene sul lavoro.

La specifica violazione di norme in materia di prevenzione infortunistica, così come l'omissione dell'adozione di misure o accorgimenti per la più efficace tutela della integrità fisica dei lavoratori, in violazione dell'art. 2087 c.c., costituisce aggravante.

In linea teorica, soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare le norme di prevenzione e protezione (datori di lavoro, titolari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, preposti, lavoratori).

[7] Le fattispecie di reato introdotte dal nuovo art. 25 undecies, per le quali le aziende possono essere chiamate a rispondere, sono riconducibili alle seguenti macro aree:
- distruzione di specie animali o vegetali protette – art. 727 bis CP; deterioramento di habitat protetti - art. 733 bis CP; detenzione e tratta di specie animali in estinzione - L. 150/1992 art. 1,3,6;
- scarico di acque reflue - D.lgs. 152/2006 art. 137;
- trattamento dei rifiuti - D.lgs. 152/2006 art.256, 259, 260;
- inquinamento di suolo, sottosuolo, acque - D.lgs. 152/2006 art. 257;
- emissioni in atmosfera - D.lgs. 152/2006 art. 279;
- emissione di sostanze lesive dell'ozono - L. 549/1993;
- inquinamento doloso e colposo provocato dalle navi alla qualità delle acque (scarichi di "sostanze inquinanti") - D.lgs. 202/2007;
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari SISTRI e non SISTRI art. 258 e 260 D.lgs. 152/2006

[88] L'entità della lesione può essere:
- grave: se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia od un'incapacità ad attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni, oppure se il fatto produce l'indebolimento permanente di un senso o di un organo o, ancora, se la persona offesa è una donna incinta e dal fatto deriva l'acceleramento del parto;
- gravissima: se dal fatto deriva una malattia certamente o probabilmente insanabile, la perdita di un senso, la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella. Ed ancora, nei casi in cui essa determini la deformazione ovvero lo sfregio permanente del viso o l'aborto della persona offesa

VI.2.2 Reati in materia ambientale ex art. 25 undecies D.lgs.231/2001.

Art. 256 del d.lgs. 3 aprile 2006, n. 152 “Gestione di rifiuti non autorizzata”

art. 256, co. 1, lett. a) e b) - (Concorso in) Raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti, non pericolosi e pericolosi, in mancanza della prescritta autorizzazione, iscrizione o comunicazione.

Ciascuna delle attività di gestione sopra richiamata presuppone, per poter essere correttamente esercita, il rilascio di specifica autorizzazione.

Terni Reti, affidando lo smaltimento dei rifiuti prodotti o di beni strumentali fuori uso a soggetto non autorizzato o con autorizzazioni scadute, potrebbe in via del tutto teorica concorrere nel reato indicato.

Realizzazione o gestione di una discarica non autorizzata (art. 256, co. 3, primo periodo).

Realizzazione o gestione di discarica non autorizzata destinata, anche in parte, allo smaltimento di rifiuti pericolosi (art. 256, co. 3, secondo periodo).

In base a quanto stabilito nel D.lgs. n. 36/2003, la discarica è definita come: “area adibita a smaltimento dei rifiuti mediante operazioni di deposito sul suolo o nel suolo, compresa la zona interna al luogo di produzione dei rifiuti adibita allo smaltimento dei medesimi da parte del produttore degli stessi, nonché qualsiasi area ove i rifiuti sono sottoposti a deposito temporaneo per più di un anno. Sono esclusi da tale definizione gli impianti in cui i rifiuti sono scaricati al fine di essere preparati per il successivo trasporto in un impianto di recupero, trattamento o smaltimento, e lo stoccaggio di rifiuti in attesa di recupero o trattamento per un periodo inferiore a tre anni come norma generale, o lo stoccaggio di rifiuti in attesa di smaltimento per un periodo inferiore a un anno”.

Attività non consentite di miscelazione di rifiuti (art. 256, co. 5)

Ai sensi dell’articolo 187, comma 1, del D.lgs. 152/2006 è vietato miscelare rifiuti pericolosi con rifiuti non pericolosi, fatte salve le deroghe previste al successivo co. 2.

Nel caso si miscelassero in maniera non consentita i rifiuti come sopra, si integrerebbe il reato di attività svolta in assenza delle autorizzazioni previste agli artt. 208, 209 e 211.

Certificati analitici contenenti false indicazioni (art. 258 co. 4, secondo periodo)

Viene prevista la fattispecie punita all'articolo 483 del Codice penale nei confronti di chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.

VI.2.3 Sanzioni ex D.lgs.231/200

Descrizione Reato	Sanzioni pecuniarie n. quote (*)	Sanzioni interdittive	Pubblicazione sentenza e confisca
Omicidio colposo (art. 589 c.p.) - se in violazione art. 55 co.2 DLgs.81/2008	Da 250 a 500 1000	SI	SI
Lesioni personali colpose (art. 590 c.p.)	Da 100 a 250	SI	SI
Raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 Se si tratta di rifiuti pericolosi	Da 100 a 250 Da 150 a 250	SI	SI
Chiunque realizza o gestisce una discarica non autorizzata	Da 150 a 250	SI	SI
Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti	Da 150 a 250	SI	SI

(*) Il valore della quota è stabilito dal giudice da un minimo di €. 258 a un massimo di €. 1549.

VI.3 LA VALUTAZIONE DEI RISCHI

In linea teorica, i reati di in violazione delle norme di sicurezza sul lavoro indicati dal decreto si realizzano in tutti i casi in cui nello svolgimento dell'attività produttiva e delle attività volte agli adempimenti normativi, giuridicamente attribuite al datore di lavoro, può manifestarsi la "colpa" (negligenza, imprudenza, imperizia o violazione di leggi o regolamenti) di un rappresentante della società, designato per gli aspetti attinenti la sicurezza, nonché dei medesimi lavoratori, di non adempiere compiutamente ai propri obblighi, determinando così un infortunio, una malattia ovvero la morte di un dipendente o di un soggetto terzo per c.d. rischio di interferenza.

Nella colpa, può essere individuato il vantaggio (verosimilmente economico) che *completa i presupposti* della responsabilità amministrativa degli enti.

Riguardo ai reati ambientali indicati dal decreto, la rischiosità di Terni Reti è riconducibile agli adempimenti di tutela ambientale conseguenti alla gestione e all'acquisizione dell'Aviosuperficie di Terni riguardo agli impianti di depurazione e di erogazione del carburante; mentre i rischi connessi al "trattamento e conferimento di rifiuti speciali (consumabili per la stampa) a smaltitore

autorizzato", al momento è inesistente, ricadendo la responsabilità oltreché l'onere di smaltimento in capo alla ditta appaltatrice del "global service".

In sintesi sono state considerate le seguenti aree/attività sensibili ai reati in violazione delle norme di sicurezza sul lavoro e di tutela ambientale:

REF	MAPPA DELLE MACRO ATTIVITÀ SENSIBILI
1 - D	Adempimenti organizzativi.
2 - D	Politica di sicurezza sul lavoro e Piano di miglioramento
3a - D	Sistema per assolvimento obblighi giuridici – Standard Tecnico strutturali Attrezzature, Impianti e Macchinari
3b - D	Sistema per assolvimento obblighi giuridici – Attività di valutazione dei rischi
4a - D	Gestione delle emergenze
4b - D	Gestione degli appalti
4c - D	Riunioni periodiche e Consultazione RLS
5 - D	Sorveglianza sanitaria
6 - D	Informazione e Formazione
7 - D	Vigilanza sul rispetto di procedure e istruzioni di sicurezza
8 - D	Acquisizione di documentazione e certificazioni obbligatorie
9 - D	Verifica di osservanza del MOG
10 - D	Sistemi di registrazione del funzionamento del MOG
11 - D	Trattamento e conferimento di rifiuti speciali a smaltitori autorizzati
12 - D	Adempimenti di tutela ambientale presso l'Aviosuperficie

Tuttavia, si può ragionevolmente ritenere che **il livello di rischio** del verificarsi di condotte che integrino le fattispecie di reato trattate (sia di sicurezza sul lavoro sia di tutela ambientale) sia valutabile come "**trascurabile**".

Infatti, va tenuto conto del *basso livello di rischio di sicurezza sul lavoro* connesso alle attività svolte dalla Terni Reti, come si evince dal Documento di Valutazione dei Rischi (DVR) vigente, nonché *dall'attuazione degli adempimenti previsti dal D.lgs. 81/2008*, e dalla *limitata produzione di rifiuti speciali* (dovuti ai consumabili per la stampa dismessi).

Infine, va considerato l'effetto positivo, in termini di prevenzione dei rischi, dei presidi di carattere trasversale riportati nella Parte Generale del MOG e, in particolare, nel Codice Etico nel quale la

società "*si impegna ad operare, a tutti i livelli, al fine di garantire l'integrità fisica e morale dei propri dipendenti e collaboratori, condizioni di lavoro rispettose della dignità individuale ed ambienti di lavoro sicuri e salubri, nel pieno rispetto della normativa vigente in materia, in conformità ai principi indicati dall'articolo 15 del D.lgs. 81/2008*".

VI.4 LE AREE SENSIBILI E IL SISTEMA DEI CONTROLLI ESISTENTI

VI.4.1 Introduzione normativa ex art 30 del D.lgs. 81/2008

Con il DM del 13.2.2014 del Ministero del Lavoro e delle Politiche sociali sono state emesse in allegato le "procedure semplificate" ad uso delle piccole e medie imprese per la predisposizione e l'efficace attuazione dei Modelli di organizzazione e gestione della salute e sicurezza sul lavoro, come previsto dal comma 5bis del D.lgs. 81/2008.

Le piccole e medie imprese, come Terni Reti possono così utilizzare la modulistica allegata al Decreto e quella che sarà pubblicata sul sito www.lavoro.gov.it alla sezione "sicurezza sul lavoro", fermo restando l'integrale applicazione di quanto previsto dall'art. 30 del D.lgs. 81/2008.

L'articolo 30 stabilisce che il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa degli enti di cui al D.lgs. n. 231/2001, deve assicurare l'adozione di un sistema di gestione per l'adempimento di tutti gli obblighi giuridici[9], prevedere idonei sistemi di registrazione dell'avvenuta effettuazione degli stessi e un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo (riesame) sull'attuazione stessa del modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

Sistema di controllo interno: Terni Reti sta progettando il proprio sistema di gestione della sicurezza sul lavoro sulla base delle procedure semplificate di cui al DM del 13.2.2014 del Ministero del Lavoro e delle Politiche, tratte da linee guida UNI – INAIL, ritenuto idoneo dall'art.

[9] Gli obblighi giuridici relativi alla sicurezza, che un sistema di gestione idoneo deve garantire, sono:
a. rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b. valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c. attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
d. attività di sorveglianza sanitaria;
e. attività di informazione e formazione dei lavoratori;
f. attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
g. acquisizione di documentazioni e certificazioni obbligatorie di legge;
h. periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

30 del D.lgs.81/2008, avvalendosi della consulenza della società Ambiente e Lavoro di Terni (conferimento incarico del 22.09.2015).

La gestione della sicurezza sul lavoro sarà strutturata secondo le fasi di valutazione dei rischi, di progettazione delle misure di prevenzione, di attuazione delle misure e di raccolta delle evidenze documentali e di attuazione del modello, come documentato dal DVR e dagli allegati.

VI.4.2 Adempimenti organizzativi (art 30 comma 3)

Gli adempimenti organizzativi previsti dal D.lgs. 81/2008 riguardano la formale individuazione, tenendo conto della complessità dell'organizzazione aziendale, dei diversi ruoli e responsabilità in materia di salute e sicurezza: Datore di Lavoro (DL); dirigenti (se presenti); preposti, (se presenti); Responsabile del Servizio di Prevenzione e Protezione (RSPP) - nei casi in cui i compiti del Servizio di Prevenzione e Protezione non siano svolti direttamente dal DL; Addetti al Servizio di Prevenzione e Protezione (se presenti); Addetti alle Emergenze ed al Primo Soccorso; Medico competente (MC); Rappresentante dei Lavoratori per la Sicurezza/RLS Territoriale.

A seconda della tipologia di attività svolta può essere necessario individuare i ruoli e le responsabilità, in materia di salute e sicurezza, di ulteriori figure (come previsto, ad esempio, dal titolo IV del D.lgs. 81/08 "Cantieri temporanei e mobili" e s.m.i. o dal DPR 77/2011).

Sistema dei controlli esistente: Il Datore di lavoro è l'Amministratore Unico *pro tempore* di Terni Reti che con procura rilasciata il 04.05.2016 con repertorio n. 65327 del notaio Pasqualini registrata il 26.05.2016 ha delegato il Direttore Generale allo svolgimento di tutte le funzioni delegabili del "datore di lavoro".

La nomina del RSPP esterno, formalizzata ed accettata, è stata fatta dal Datore di Lavoro in data 30 settembre 2016, e le nomine del Medico competente, dei preposti, degli Addetti al Primo soccorso e antincendio sono fatte dal Dirigente Delegato, formalizzate e accettate dai nominati.

Avendo frequentato specifici corsi nel precedente rapporto di lavoro con USI Spa, i Responsabili di Area sono stati nominati "preposti". Inoltre sono preposti il responsabile Aviosuperficie e due addetti alle squadre di verifica parcheggi.

Il Medico Competente cura anche la sorveglianza sanitaria (incarico prot. 81del 30 settembre 2015).

Al RLS, eletto il 18 gennaio 2016, è stata erogato un corso di formazione di base il 26 ottobre del 2009 e successivi aggiornamenti il 14 novembre 2011, il 28 maggio 2013 e 22 gennaio 2016.

Infine, con Determina n. 70/AU del 01.12.2016 è stata approvata la Disposizione Organizzativa riguardante "L'ORGANIZZAZIONE DELLA SALUTE E SICUREZZA SUL LAVORO in Terni Reti S.r.l. Unipersonale".

VI.4.3 Politica di sicurezza sul lavoro e piano di miglioramento

La politica per la salute e la sicurezza sul lavoro (SSL) deve essere definita e documentata dal vertice aziendale nell'ambito della politica generale dell'azienda.

La politica ha la finalità di indicare la visione, i valori essenziali e le convinzioni dell'azienda sul tema della SSL e serve a definire la direzione, i principi d'azione e i risultati a cui tendere.

La politica esprime cioè l'impegno del vertice aziendale nel promuovere nel personale la conoscenza degli obiettivi, la consapevolezza dei risultati a cui tendere, l'accettazione delle responsabilità e le motivazioni ed aiuta a dimostrare l'impegno concreto dell'azienda alla tutela della salute e sicurezza dei lavoratori.

A fronte di quanto riportato nella politica aziendale sono definiti gli obiettivi di miglioramento di cui va pianificata la realizzazione attraverso uno specifico piano di miglioramento.

Il Piano di miglioramento della sicurezza trae, quindi, fondamento dal Documento di valutazione dei Rischi (DVR) ed è adeguatamente finanziato dal Budget aziendale. Gli interventi di miglioramento vengono programmati in base alla loro priorità, tenendo conto della rilevanza del rischio emersa dal processo di valutazione.

È compito del Datore di Lavoro definire le modalità di monitoraggio e controllo di funzionalità, efficacia e puntualità di realizzazione del piano di miglioramento.

Sistema dei controlli esistente: la politica di SSL della Società è enunciata nel Codice Etico al § 3.3 "Eticità nella gestione della sicurezza sul lavoro e della tutela ambientale" in cui è richiamato l'impegno di Terni reti a "*operare, a tutti i livelli, al fine di garantire l'integrità fisica e morale dei propri dipendenti e collaboratori, condizioni di lavoro rispettose della dignità individuale ed ambienti di lavoro sicuri e salubri, nel pieno rispetto della normativa vigente in materia, in conformità ai principi indicati dall'articolo 15 del D.lgs. 81/2008. Si impegna, quindi, a mettere a disposizione risorse umane, strumentali ed economiche, atte a perseguire tali obiettivi come primari, considerando la gestione della sicurezza e salute sul lavoro parte integrante della propria attività*".

Azione programmata: Nell'ambito dell'aggiornamento del DVR aziendale, a seguito dei nuovi servizi, sarà definita la "politica della sicurezza" in cui sono enunciati i principi ispiratori e l'impegno dell'azienda per il miglioramento delle condizioni di salute e sicurezza sul lavoro, indicando le linee di sviluppo per realizzarlo[10].
Inoltre, sarà predisposto il "Piano di miglioramento della sicurezza" (annuale o pluriennale), conforme alla modulistica ministeriale, in cui saranno individuate: le responsabilità, le tempistiche,

[10] I contenuti della politica aziendale di salute e sicurezza comprendono l'impegno dell'alta direzione: a rispettare e applicare integralmente la legislazione in materia di SSL; a prevenire infortuni e malattie professionali e a migliorare nel tempo le condizioni di SSL, attraverso l'individuazione di aree di miglioramento; a verificare periodicamente e ad aggiornare la Politica.

le priorità degli interventi da realizzare e le risorse umane, strumentali e finanziarie necessarie alla loro realizzazione.
Infine, quale intervento specifico, saranno migliorate le condizioni di sicurezza dell'area di servizio presso l'Aviosuperficie.

VI.4.4 Obblighi giuridici in materia di sicurezza (art. 30 co. 1 lettera a e b)

ATTIVITÀ DI VALUTAZIONE DEI RISCHI

La Valutazione dei Rischi ex art. 28 del D.lgs. 81/2008 è un processo di valutazione documentata di tutti i rischi per la salute e la sicurezza dei lavoratori presenti in azienda a delle persone che accedono ai luoghi di lavoro dell'azienda, con la finalità di individuare adeguate misure di prevenzione e protezione e di elaborare il programma di miglioramento.

Il processo di valutazione è condotto sotto la responsabilità (non delegabile) del Datore di Lavoro, formalizzato nel DVR elaborato in collaborazione con il RSPP e il Medico Competente, previa consultazione del Rappresentante dei lavoratori per la sicurezza (RLS).

La valutazione dei rischi è aggiornata, utilizzando le informazioni ottenute dalle attività di monitoraggio e, comunque, ogni volta che intervengano cambiamenti significativi di processo produttivo o di organizzazione del lavoro, cambiamenti legislativi o in seguito ad eventi quali emergenze, infortuni, incidenti.

Azione Programmata:

L'elaborazione dell'aggiornamento del DVR aziendale è stata affidata alla società Ambiente e Lavoro di Terni (protocollo n. 77 conferimento incarico del 22.09.2015).

STANDARD TECNICO STRUTTURALI E DI LEGGE

Il MOG deve assicurare un sistema di gestione idoneo a garantire il rispetto degli standard tecnico strutturali fissati dalla legge e dalle norme di riferimento per le attrezzature, gli impianti, i luoghi di lavoro, l'esposizione ad agenti chimici, fisici e biologici, per i dispositivi di protezione individuale (DPI), per le macchine, i materiali e materie utilizzati e per gli impianti, sia in fase di acquisto sia per il mantenimento della conformità nel tempo.

La Società, quindi, deve predisporre modalità che garantiscano l'aggiornamento tempestivo alle prescrizioni legislative applicabili alla propria realtà aziendale e l'utilizzo di risorse interne o esterne per la consultazione delle fonti di aggiornamento e l'identificazione della normativa applicabile.

La Società deve, quindi, individuare le funzioni aziendali competenti che devono far effettuare i controlli periodici previsti dalla legge, vigilare sul mantenimento dei dispositivi di sicurezza e sul

buono stato di attrezzature, macchine ed impianti e attuare tempestivi interventi manutentivi a seguito delle segnalazioni di non conformità o di guasti.

Azione programmata: Il DVR in fase di elaborazione riporterà nel prospetto delle "Manutenzioni Obbligatorie da effettuare" un elenco esaustivo, conforme alla modulistica ministeriale, delle attrezzature, impianti, macchinari, materiali e materie, DPI, esistenti ed utilizzati[11] in Azienda in cui saranno indicate le norme di riferimento e la frequenza delle verifiche.

Inoltre, si prevede di elaborare un "disciplinare tecnico" da allegare al Contratto di affidamento delle funzioni di RSSP in cui specificare l'obbligo della Società contraente di "*garantire un adeguato presidio in merito alla normativa da applicare per impianti ed attrezzature utilizzate in merito all'attuazione delle verifiche periodiche e agli interventi manutentivi necessari*" e prevedere "*un idoneo flusso informativo volto ad assicurare la vigilanza e il monitoraggio del Dirigente Delegato e del Datore di lavoro*".

VI.4.5 Emergenze e primo soccorso, appalti e consultazione RLS (art.30 co. 1 lett c)

GESTIONE DELLE EMERGENZE

La gestione delle emergenze si caratterizza come l'insieme delle misure straordinarie da attuare in caso di pericolo grave e immediato. È necessario, quindi, individuare le possibili situazioni di emergenza che possono creare danni alle persone e alle cose e definire le azioni da mettere in atto per fronteggiare ciascuna di esse.

Il Datore di Lavoro o un suo incaricato, individua le possibili emergenze e le relative modalità di gestione e pianifica la gestione delle emergenze come segue:

- designa i lavoratori incaricati dell'attuazione delle misure di prevenzione e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio e di primo soccorso;
- definisce le misure organizzative e gestionali da attuare in caso di emergenza per la messa in sicurezza del personale individuando le vie di esodo, i punti di raccolta, le raccomandazioni rispetto agli atteggiamenti da tenere durante l'evacuazione e redige il relativo Piano di emergenza;
- organizza le modalità di comunicazione con i servizi pubblici competenti in materia di primo soccorso, salvataggio, lotta antincendio e gestione delle emergenze;
- stabilisce le modalità di diramazione dell'allarme (es.: sonoro, vocale, luminoso ecc.);
- informa i lavoratori circa le misure predisposte e i comportamenti da adottare;
- garantisce la presenza di planimetrie chiare, con l'indicazione delle vie di fuga e dei presìdi

[11] Sistema antincendio, Lampade di emergenza, Quadri elettrici, Gruppi elettrogeni (Sala server e per piano di antincendio), Ascensori e Montacarichi, Sistema di riscaldamento e condizionamento, DPI rischio elettrocuzione e caduta (gli addetti ai lavori elettrici in altezza).

antincendio
- organizza esercitazioni con cadenza periodica, simulando le emergenze possibili, identificate e riportate, ove presente, nel piano di emergenza.

Sistema dei controlli esistente:

Le nomine del personale incaricato per la gestione delle emergenze sono complete e aggiornate (Coordinatore squadre di emergenza e n. 1 sostituto, n. 8 componenti squadre antincendio, n. 8 componenti squadre di primo soccorso).

Le istruzioni operative sono riportate nel documento "Linee guida per il Coordinatore delle squadre di emergenza".

È competenza del Comune di Terni, proprietario dell'immobile in cui sono ubicati gli uffici di Terni Reti, l'approvazione del piano generale di emergenza, a cui sono stati comunicati il 14.10.2016 i nominativi del RSPP, dei Coordinatori e degli addetti alle squadre antincendio e primo soccorso, nonché il Nominativo e numero telefonico dell'Addetto al posto di chiamata (APC) presente in sede.

Azione programmata: aggiornamento dei Piani di Emergenza per le aree operative Aviosuperficie, Parcheggio S. Francesco; implementazione dei ruoli di addetti antincendio presso Aviosuperficie, mediante abilitazione di nuovi addetti ai sensi del DM 06.08.2014.

GESTIONE DEGLI APPALTI

Il Datore di Lavoro (DL) o un suo incaricato deve assicurarsi, nella selezione degli appaltatori e nella gestione degli appalti, che vengano applicati i principi di salvaguardia della sicurezza e della salute dei lavoratori.

Per la selezione degli appaltatori il DL o suo incaricato deve pertanto procedere come segue:
- selezionare gli appaltatori, sia lavoratori autonomi sia imprese, previa verifica dell'idoneità tecnico professionale;
- se i lavori ricadono nel campo d'applicazione del art. 26 del D.lgs. 81/08 redigere il DUVRI, ovvero avvalersi, nei casi previsti dallo stesso articolo, della possibilità di individuare un incaricato responsabile della cooperazione e del coordinamento;
- attivare le procedure di cui al Titolo IV del D.lgs. 81/08 nel caso si tratti di cantieri temporanei e mobili;
- comunicare all'appaltatore o agli appaltatori la propria politica di sicurezza e, se necessario, il soggetto di riferimento per l'attività oggetto dell'appalto.

Sistema dei controlli esistente: il Regolamento per l'acquisizione dei beni e servizi in economia tratta in modo dettagliato e completo le modalità di verifica dell'idoneità tecnico-professionale di fornitori e appaltatori negli artt. 5 e 6 del Titolo II "Disciplina degli operatori economici".

Azione programmata: stesura dei DUVRI [12] (Documento di Valutazione dei Rischi da Interferenze) per la gestione delle attività affidate in appalto presso le aree operative Aviosuperficie, Parcheggio S. Francesco;
previsione nei contratti di appalto dell'ottemperanza degli adempimenti riguardanti la sicurezza sul lavoro e della clausola risolutiva in caso di violazione del Codice Etico.

RIUNIONI PERIODICHE E CONSULTAZIONE RLS

Il Datore di Lavoro o un suo incaricato gestisce le comunicazioni interne ed esterne relativamente alle tematiche di salute e sicurezza, coinvolgendo quando opportuno i lavoratori dell'azienda, anche attraverso i loro RLS, come previsto dalla legislazione vigente e dai contratti collettivi di lavoro, raccogliendo osservazioni, commenti e proposte dai lavoratori e dagli altri soggetti interessati (enti locali, cittadini, dipendenti diretti e indiretti, clienti e fornitori, ecc.).

Azione programmata: organizzare la riunione periodica ex art. 15 D.lgs.81/2008 in modo tale da assolvere anche alla finalità di riesame del sistema di gestione della SSL adottato.

VI.4.6 Sorveglianza sanitaria (art. 30 comma 1 lettera d)

Il Datore di Lavoro o un suo incaricato nomina il Medico Competente (MC) per l'effettuazione della sorveglianza sanitaria nei casi previsti dal decreto legislativo n. 81/2008 e s.m.i., verificando il possesso dei titoli necessari per legge (art. 38 e 39 del decreto legislativo n. 81/2008 e s.m.i.) e fornendo al MC medesimo tutte le informazioni necessarie allo svolgimento dell'incarico.

Il MC, oltre a collaborare con il DL ed il RSPP alla valutazione dei rischi, programma ed effettua la sorveglianza sanitaria attraverso protocolli sanitari definiti in funzione dei rischi specifici; la periodicità dei controlli di sorveglianza sanitaria tiene conto delle normative applicabili nonché dei livelli di rischio.

Il MC visita almeno una volta all'anno (o con cadenza differente, stabilita in funzione della valutazione dei rischi) gli ambienti di lavoro dell'azienda; il sopralluogo prevede la redazione di un apposito verbale.

Il MC partecipa alla riunione periodica, nei casi in cui è prevista (art. 35 del decreto legislativo n. 81/2007 e s.m.i.).

La cartella sanitaria e di rischio, istituita ed aggiornata dal MC, per ogni lavoratore sottoposto a sorveglianza sanitaria, è custodita, con salvaguardia del segreto professionale e della privacy, presso il luogo concordato col Datore di Lavoro o con un suo incaricato al momento della nomina.

[12] Il documento riporta i rischi specifici di interferenza per tutti gli appalti stabili ed è parte integrante del contratto di appalto unitamente all'allegato, compilato e sottoscritto dalle parti, in cui sono riportati gli elementi di verifica dell'idoneità tecnico professionale in relazione all'appalto e le informazioni da parte del Committente sui rischi specifici dell'ambiente di lavoro oggetto dell'appalto, sui rischi interferenziali e sulle misure di prevenzione e di emergenza.

Sistema dei controlli esistente: la sorveglianza sanitaria è affidata al MC e riguarda la quasi totalità dei dipendenti per il rischio videoterminali (VDT).
Le cartelle sanitarie sono custodite dal MC.
Il certificato di idoneità al lavoro è conservato all'interno della cartella del dipendente presso l'Ufficio Segreteria.

Azione programmata: formalizzare in un contratto il rapporto economico prestazionale con il medico competente anche con riferimento agli adempimenti privacy.

VI.4.7 Informazione e formazione (art. 30 co. 1 lett. e)

Il Datore di lavoro o un suo incaricato definisce le modalità per un efficace e corretta gestione delle attività di informazione e formazione dei lavoratori.

In base alle risultanze della valutazione dei rischi ed in conformità con la legislazione vigente ed i contratti collettivi di lavoro applicati, tenendo conto delle capacità e delle condizioni dei lavoratori, il DL o suo incaricato pianifica, predispone ed attua il "Programma annuale di formazione, informazione e addestramento" per tutte le figure aziendali e lo aggiorna all'occorrenza in occasione della revisione della valutazione dei rischi, nel caso di modifiche legislative, di nuove assunzioni, di cambiamenti nelle mansioni, nei cambiamenti di attività o processi (nuove macchine, attrezzature, impianti, nuove modalità operative, ecc.).

Al termine degli interventi formativi deve essere verificato il grado di apprendimento, sia per i corsi organizzati dal DL stesso che per quelli erogati presso soggetti esterni, e deve essere registrata la presenza dei partecipanti (ai sensi degli accordi Stato regioni: 21 dicembre 2011 e 12 febbraio 2012).

Azioni programmate:

- aggiornamento e completamento della formazione dei lavoratori sulla base delle nuove mansioni oltre alla formazione aggiuntiva per i preposti;
- abilitazione di nuovi addetti antincendio per l'Aviosuperficie ai sensi del DM 06.08.2014
- elaborazione di un disciplinare tecnico allegato al contratto del RSPP in cui sia previsto che la formazione e informazione è seguita e monitorata dal RSPP esterno che si avvale di uno scadenziario, condiviso dal Responsabile dell'Area Amministrazione, relativo alla formazione obbligatoria in materia di sicurezza; inoltre, l'RSPP, all'occorrenza, provvederà alla distribuzione di documenti e manuali informativi.

Il responsabile dell'Area Amministrazione dovrà assicurare che la formazione erogata sia registrata e gli attestati di partecipazione e di merito siano archiviati nella cartella personale del dipendente.

VI.4.8 Vigilanza sull'osservanza delle procedure di sicurezza (art. 30 co. 1 lett. f)

Il Datore di lavoro (DL) deve dare direttive per la realizzazione di un sistema di controllo sul rispetto delle procedure e delle istruzioni di sicurezza da parte dei lavoratori e vigilare sulla loro corretta attuazione.

La vigilanza del rispetto delle disposizioni aziendali è distribuita, secondo le competenze di ciascuno, tra DL, dirigente delegato (ove presente) e preposto; il DL deve quindi individuare le figure del sistema di sicurezza, conferire i relativi incarichi e responsabilità e comunicarli ai lavoratori ed ai soggetti interessati.

L'eventuale utilizzo della delega di funzioni non esclude l'obbligo di vigilanza in capo al delegante in relazione al corretto espletamento da parte del delegato delle funzioni trasferite.

Sistema dei controlli esistente: nell'atto di nomina dei preposti è fatto riferimento all'obbligo di vigilanza sull'operato dei collaboratori e subordinati.

Azioni programmate: negli atti di nomina dei preposti sarà espressamente indicato che le violazioni riscontrate nell'ambito delle attività di vigilanza dovranno essere tempestivamente comunicate agli organi preposti per l'irrogazione della relativa sanzione secondo il sistema disciplinare del MOG - Parte Generale.

Inoltre il RSPP esterno predisporrà una scheda di monitoraggio ad uso dei preposti, quale guida all'attività di vigilanza sui comportamenti dei sottoposti.

VI.4.9 Documenti e certificazioni obbligatorie (art. 30 co. 1 lett. g)

Il Datore di lavoro (DL) o un suo incaricato deve adeguatamente gestire e custodire i documenti e le certificazioni obbligatorie per legge (esempi non esaustivi: DVR, DUVRI, POS; agibilità dell'immobile; conformità impianti elettrici L.46/90; conformità impianti elevatore, termico, di condizionamento e antincendio; certificazione CE, libretti uso e manutenzione macchine e attrezzature; autocertificazioni degli appaltatori).

La gestione di tale documentazione riguarda i seguenti aspetti:

- le modalità di emissione e divulgazione della documentazione
- il sistema di conservazione e controllo
- le modalità di revisione, necessarie specialmente in caso di cambiamenti organizzativi, tecnici, strutturali, dei processi, ecc.
- la figura/e in azienda che ne ha/hanno responsabilità

Sistema dei controlli esistente: Il sistema di protocollo e di gestione documentale adottato da Terni Reti come descritto nel Cap. II.8 "Trasparenza e tracciabilità" del MOG – Parte Generale, consente la registrazione e l'acquisizione in formato digitale, nonché la corretta archiviazione

cartacea ed informatica di tutta la documentazione prodotta e acquisita in materia di sicurezza sul lavoro, nonché le certificazioni e i libretti d'uso e manutenzione. La gestione è affidata all'Ufficio Segreteria che si avvale del sistema informatico denominato ""**Isharedoc"** e di un archivio meccanizzato.

Azione programmata: riportare in un documento conforme al modello ministeriale, in modo dettagliato ed esaustivo, l'elenco della documentazione rilevante riguardante la sicurezza, indicando per ogni documento i dati di emissione e di revisione e la relativa responsabilità.

VI.4.10 Verifiche di effettività e adeguatezza del MOG SSL (art. 30 co. 1 lett. h)

Le verifiche periodiche riguardanti l'applicazione e l'efficacia delle procedure e del modello adottati costituiscono un requisito essenziale per l'efficacia esimente del MOG.

Il processo di verifica dell'applicazione delle procedure/modelli si realizza in diverse fasi che possono essere riconducibili essenzialmente a sorveglianza, misurazione o monitoraggio, tenendo conto degli esiti della valutazione dei rischi.

La verifica di efficacia delle procedure/modelli deve tener conto degli infortuni e degli incidenti che si sono verificati nel periodo considerato e la gestione delle "non conformità" rilevate.

Tali attività sono svolte a vari livelli da risorse interne dell'azienda, dai preposti, dal DL o da un suo incaricato in virtù delle rispettive attribuzioni e competenze e, per aspetti specialistici si può ricorrere a risorse esterne.

Le attività di verifica devono essere registrate e i risultati confrontati con gli obiettivi prefissati.

Qualora a seguito delle attività di sorveglianza/monitoraggio e misurazione si rilevino non conformità, l'azienda deve attivare il processo di gestione delle non conformità e di pianificazione e di attuazione delle azioni correttive e preventive e successivamente verificarne l'efficacia, secondo modalità predefinite.

Gli esiti del monitoraggio sono oggetto del Riesame.

Azione programmata: In relazione agli esiti della valutazione dei rischi e all'andamento di infortuni e incidenti, saranno eseguiti audit indipendenti periodici sul sistema di gestione per la sicurezza adottato.

Nel caso in cui tale attività sia affidata a Terzi, il relativo contratto dovrà indicare in dettaglio le finalità e gli aspetti da verificare, nonché la struttura del report da produrre.

VI.4.11 Registrazione delle attività di cui al co. 1 dell'art.30 - MOG

Il Datore di lavoro (DL) o un suo incaricato deve definire le modalità con cui gestire e custodire la documentazione, per fornire l'evidenza del funzionamento del MOG al fine di disporre di documenti comprensibili, corretti, aggiornati.

La definizione delle modalità di gestione riguarda i seguenti aspetti: le modalità di redazione ed approvazione della documentazione; le modalità di invio della documentazione alle funzioni interessate; il sistema di conservazione e controllo; le modalità di revisione, necessarie specialmente in caso di cambiamenti organizzativi, tecnici, strutturali, dei processi, ecc. e le relative responsabilità; la data di emissione e di aggiornamento.

Sistema dei controlli esistente:

Il MOG – Parte Generale - Cap. II.10 "Organismo di vigilanza" descrive le funzioni, i poteri e i compiti dell'organismo di vigilanza (OdV).

L'OdV si avvarrà del sistema di protocollo e di gestione documentale adottato da Terni Reti, come descritto nel Cap. II.8 "Trasparenza e tracciabilità" del MOG – Parte Generale.

Azione programmata:

L'OdV, una volta nominato, proporrà al CdA una procedura dei "flussi informativi" e dovrà emanare un "Regolamento delle attività dell'OdV", in cui saranno trattati gli aspetti riguardanti le registrazioni e il controllo della documentazione prodotta o acquisita dallo stesso.

VI.5 LE AREE SENSIBILI E IL SISTEMA DEI CONTROLLI ESISTENTI – TUTELA AMBIENTALE

VI.5.12 Trattamento di rifiuti speciali (consumabili per la stampa)

I consumabili per la stampa si qualificano come “rifiuti speciali” e devono essere avviati al recupero o allo smaltimento in base alla normativa in vigore (D.lgs. 4/2008).

Tuttavia, Terni Reti ha affidato alla ditta Pucciufficio s.r.l. un global service per la fornitura di apparati stampa, materiali di consumo (carta e toner), assistenza tecnica ed ogni altro onere connesso al servizio; pertanto anche la responsabilità oltreché l’onere di smaltimento ricade in capo dell’appaltatore.

Tutti gli altri rifiuti prodotti sono rifiuti urbani e come tali presi in carico dal servizio pubblico di raccolta dei rifiuti urbani.

VI.5.13 Adempimenti di tutela ambientale presso l’Aviosuperficie.

IMPIANTO DI DEPURAZIONE

Temi Reti ha commissionato alla Ecol Service s.r.l. il servizio di manutenzione ordinaria dell'impianto di depurazione, sito presso l'Aviosuperficie "A. Leonardi" in Temi (TR) - Loc. Maratta "Le Sore". L'impianto smaltisce le acque reflue assimilabili alle domestiche derivanti dai servizi igienici e dalle attività turistico-ricettive presenti nell'area, effettuandone il trattamento attraverso il ciclo di depurazione biologico comprensivo di trattamento con fitodepurazione e la canalizzazione delle acque depurate verso un fosso superficiale.

Sono esclusi dall'oggetto dell'appalto le attività necessarie per l‘assolvimento degli obblighi previsti dal D. Lgs.152 /2006 tra cui le analisi chimiche, in particolare quel e per la caratterizzazione dei fanghi e dei rifiuti generati dal processo di depurazione che Terni Reti gestisce direttamente.

I rischi di reato ex art. 25 undecies del D.lgs. 231/2001 sono i seguenti:

- superamento dei limiti tollerati di concentrazione di cui alla Tabella 3 allegato V del D.lgs. 152/06, in relazione alle sostanze indicate alla Tabella 5 del D.lgs. 152/2006, art. 137, co. 5;
- alterazione di alcuni valori della “caratterizzazione di base” non in linea con quanto stabilito dall’articolo 2 del D.M. 27 settembre 2010 per il conferimento dei rifiuti in discarica;
- alterazione di alcuni valori del certificato di analisi non in linea con i limiti di legge;
- realizzazione di una discarica non autorizzata, destinata allo smaltimento dei rifiuti pericolosi, D.lgs. 152/2006, art. 256, co 3, primo e secondo periodo.

Sistema dei controlli esistenti: Codice Etico - §§. 2.1 "Integrità e Legalità". 2.5 "Responsabilità sociale", 3.3."Eticità nella gestione della sicurezza sul lavoro e della tutela ambientale".

Inoltre, il Responsabile dell'Area Aviosuperficie è tenuto ad assicurare la vigilanza sul corretto funzionamento dell'impianto e si impegna a comunicare tempestivamente alla Società incaricata della manutenzione eventuali malfunzionamenti, sbalzi di energia elettrica, e qualsivoglia anomalia che si manifesti nel ciclo di smaltimento.

Azioni programmate: tenuta dello scadenzario delle analisi di controllo da eseguire sui fanghi di fitodepurazione; esame dei certificati emessi da Laboratorio fiduciario della Società in seguito alle analisi eseguite sui reflui per la verifica del rispetto dei parametri previsti nella tabella 3 – All. V al D.lgs. 152/06 o da eventuali prescrizioni dell'Ente competente al rilascio dell' AUA: Autorizzazione Unica Ambientale (Regione Umbria).

IMPIANTO DI DISTRIBUZIONE CARBURANTE

L'Aviosuperficie è dotata di una stazione di rifornimento, soggetta a manutenzione periodica, dotata di vasche di stoccaggio pompe e misuratori.

Le "acque reflue di dilavamento" sono definite " acque reflue industriali" in relazione alla potenziale presenza di oli o idrocarburi nelle acque meteoriche che cadono nell'area esterna sottesa all'impianto di rifornimento carburante. L'obbligo del trattamento dei reflui è assolto dalla presenza di un "dissabbiatore" e "disolatore" che consente la separazione dei liquidi leggeri (ad esempio benzina, petrolio e derivati).

A valle del processo di disoleazione le acque reflue industriali sono canalizzate verso un fosso (acque superficiali); mentre oli e idrocarburi sono trattenuti e periodicamente aspirati e smaltiti come rifiuti speciali. Lo scarico di acque reflue industriali in acque superficiali è soggetto ad Autorizzazione Unica Ambientale (AUA).

I rischi di reato ex art. 25 undecies del D.lgs. 231/2001 sono i seguenti:

- scarico di acque reflue industriali senza autorizzazione, con autorizzazione sospesa con autorizzazione revocata, art 137.c 1 del D.lgs. 152/06;
- superamento dei limiti tollerati di concentrazione di cui alla Tabella 3 allegato V del D.lgs. 152/06, in relazione alle sostanze indicate alla tabella 5 del D.lgs. 152/2006, art. 137, co. 5;
- alterazione di alcuni valori della "caratterizzazione di base" non in linea con quanto stabilito dall'articolo 2 del D.M. 27 settembre 2010 per il conferimento dei rifiuti in discarica.

Sistema dei controlli esistenti: Codice Etico - §§. 2.1 "Integrità e Legalità". 2.5 "Responsabilità sociale", 3.3."Eticità nella gestione della sicurezza sul lavoro e della tutela ambientale".

ALLEGATO AL MOG PARTE SPECIALE D

PIANO DI AZIONE – AREA SICUREZZA SUL LAVORO

#	Descrizione dell'azione pianificata	Responsabile	Data pianificata	Data attuazione
MOG-D. 1	Approvazione con determina dell'AU del documento organizzativo della sicurezza in cui sono riportati i diversi ruoli assegnati e il relativo organigramma. (VI.4.2)	Datore di Lavoro Dirigente Delegato	30.11.2016	01.12.2016
MOG-D. 2	Definizione della Politica della Società in materia di SSL indicandone le linee di sviluppo (da riportare nel DVR in fase di aggiornamento (VI.4.3)	RSPP	30.11.2016	
MOG-D. 3	Predisposizione del Piano di sicurezza e miglioramento annuale secondo la modulistica ministeriale da riportare nel DVR (VI.4.3)	Datore di Lavoro RSPP	30.11.2016	
MOG-D. 4	Miglioramento delle condizioni di sicurezza dell'area di servizio presso l'Aviosuperficie. (VI.4.3)	Dirigente Delegato RSPP	31.03.2017	
MOG-D. 5	Elaborazione ed emissione del DVR aziendale affidata a Ambiente Lavoro Srl di Terni, previa consultazione con Medico Competente e RLS (VI.4.4)	Datore di lavoro RSPP	30.11.2016	
MOG-D. 6	Elaborazione del prospetto delle "Manutenzioni Obbligatorie da effettuare" un elenco esaustivo, conforme alla modulistica ministeriale, da riportare nel DVR (VI.4.4)	Datore di lavoro RSPP	31.12.2016	
MOG-D. 7	Predisporre un Disciplinare Tecnico da allegare al contratto che includa nelle responsabilità del RSPP esterno "il presidio normativo" (VI.4.4)	Datore di Lavoro RSPP	Dicembre 2016	
MOG-D. 8	Riportare nei contratti di appalto (Aviosuperficie) gli adempimenti di sicurezza a carico degli appaltatori e il rispetto di principi e valori del Codice etico. (VI.4.5)	Resp. Area Acquisti	Dicembre 2016	
MOG-D. 9	Stesura dei DUVRI (Documento di Valutazione dei Rischi da Interferenze) per la gestione delle attività affidate in appalto presso le aree operative Aviosuperficie, Parcheggio S. Francesco; (VI.4.5)	Datore di Lavoro RSPP	30.11.2016	

#	Descrizione dell'azione pianificata	Responsabile	Data pianificata	Data attuazione
MOG-D. 10	Organizzare la riunione periodica ex art 35 D.lgs.81/2008 con la finalità anche di riesame del sistema di gestione della sicurezza (VI.4.5)	Datore di Lavoro RSPP	Dicembre 2016	
MOG-D.11	Formalizzare con un contratto l'incarico al Medico Competente per regolare i rapporti economici e prestazionali nonché gli adempimenti ex D.lgs. 196/2003 VI.4.6	Resp. Area Acquisti	Dicembre 2016	
MOG-D. 12	Indicare espressamente negli atti di nomina dei preposti l'obbligo di vigilanza nei confronti dei collaboratori e la sanzionabilità della mancata verifica. VI.4.8	Datore di Lavoro RSPP	Dicembre 2016	
MOG-D.13	Adottare un modello di scheda di monitoraggio ad uso dei preposti VI.4.8	Datore di Lavoro RSPP	Febbraio 2017	
MOG-D.14	Riportare in una procedura/documento organizzativo le modalità di registrazione, controllo e archiviazione dei documenti di sicurezza + allegato di rintracciabilità. VI.4.9	Datore di Lavoro RSPP	Giugno 2017	
MOG-D. 15	I contratti di audit indipendenti sul sistema SSL devono prevedere un programma di lavoro ed uno schema di report di volta in volta approvato dal Datore di Lavoro/OdV	Resp. Area Acquisti RSPP	Luglio 2017	
MOG-D. 16	(L'OdV una volta nominato) proporre al CdA la procedura dei flussi informativi ed emettere il regolamento dell'OdV in cui dovranno essere trattati aspetti riguardanti la registrazione e l'archiviazione della documentazione acquisita e prodotta. VI.4.11	OdV	Giugno 2017	

PIANO DI AZIONE – AREA TUTELA AMBIENTALE

#	Descrizione dell'azione pianificata	Responsabile	Data pianificata	Data attuazione
MOG – D.17	Tenuta dello scadenzario delle analisi di controllo da eseguire sui fanghi di fitodepurazione VI.45.2 - Depuratore	Direttore Generale	Dicembre 2017	
MOG – D.18	Esame dei certificati emessi da Laboratorio fiduciario della Società in seguito alle analisi eseguite sui reflui per la verifica del rispetto dei parametri previsti nella tabella 5 – All. V al D.lgs. 152/06 o da eventuali prescrizioni dell'Autorità d'Ambito VI.5.2 - Depuratore	Direttore Generale	All'occorrenza	