PARTE SPECIALE I

- DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE-

Indice

1. I DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

La Legge 23 luglio 2009, n. 99, recante *disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia* e contenente modifiche al D. Lgs. n. 231/2001 (d'ora in poi '**Decreto**'), ha esteso la responsabilità amministrativa degli Enti ai reati in materia di proprietà intellettuale, introducendo nel Decreto, tra i reati presupposto, i 'Delitti in materia di violazione del diritto di autore' (art. 25 *novies* D. Lgs. 231/2001).

Si tratta di alcune delle fattispecie delittuose previste dalla L. 22 aprile 1941, n. 633 (*Protezione del diritto di autore e di altri diritti connessi al suo esercizio*) ed, in particolare, dei delitti di:

- messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, primo comma, lettera a-bis);
- reati di cui all'art. 171, commessi su opere altrui non destinate alla pubblicazione, qualora ne risulti offeso l'onore o la reputazione (art. 171, terzo comma);
- abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171 bis, primo comma);
- riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171 bis, secondo comma);
- abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171 ter);
- mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171 septies);
- fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di 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 (art. 171 octies).

Si fornisce, di seguito, una breve descrizione dei reati contemplati.

Art. 171, primo comma, lettera a-bis, e terzo comma, L. 633/1941

Il delitto di cui all'art. 171 primo comma, lettera a-bis, punisce (con la multa da euro 51 a euro 2.065) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa.

L'inserimento della previsione nel Decreto mira a responsabilizzare tutte quelle aziende che gestiscono server attraverso cui si mettono a disposizione del pubblico opere protette da diritto d'autore.

La norma tutela l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete.

Dal punto di vista soggettivo, basta a configurare il reato, il dolo generico, ovvero la coscienza e la volontà di porre in essere la condotta descritta dalla norma.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui l'Ente si appropri di ricerche/analisi e/o altri documenti contenenti i risultati delle attività portate avanti da ricercatori in modo da utilizzarne i contenuti o pubblicarli sul suo sito internet o su altre reti telematiche come se fossero propri.

Il delitto di cui al comma 3 dell'art. 171 è configurabile qualora sia integrata alternativamente una delle condotte menzionate dall'art. 171 (quindi sia l'ipotesi prevista dall'art. 171 lett. a bis, sopra descritta, sia le altre ipotesi indicate dalla norma, ovvero riproduzione, trascrizione, diffusione, messa in vendita, di un 'opera altrui o rivelazione del contenuto, prima che sia reso pubblico; o anche rappresentazione o diffusione di un'opera altrui) ove commesse su una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, o con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Il bene giuridico protetto dalla norma ci cui al terzo comma consiste nella protezione dei diritti personali del titolare dell'opera, ovvero il suo onore e la sua reputazione, a differenza della ipotesi criminosa precedente che mira a tutelare l'aspettativa di guadagno del titolare dell'opera.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui la Società riproduca su documenti aziendali (giornali, materiali promozionali, comunicazione via internet, ecc.) opere altrui, prima che sia reso pubblico il contenuto, usurpandone la paternità o modificandone il contenuto, con la conseguenza dell'offesa all'onore od alla reputazione dell'autore.

Art. 171 *bis,* 1 e 2 comma, L. 633/1941

Il primo comma dell'art. 171 è volto a tutelare penalmente il c.d. software, punendo l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore; ma anche l'importazione, la distribuzione, la vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; è altresì punita la predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.

La condotta può consistere anzitutto nella abusiva duplicazione, essendo prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro.

Il riferimento all'abusività della riproduzione indica che, sul piano soggettivo, il dolo dell'agente debba ricomprendere anche la conoscenza delle norme extra-penali che regolano la materia.

La seconda parte del comma indica le altre condotte che possono integrare il reato *de quo*: importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale e locazione di programmi "piratati". Si tratta di condotte caratterizzate dall'intermediazione tra il produttore della copia abusiva e l'utilizzatore finale.

Infine, nell'ultima parte del comma, il legislatore ha inteso inserire una norma volta ad anticipare la tutela penale del software, punendo condotte aventi ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Sul piano soggettivo, tutte le condotte sono caratterizzate dal dolo specifico di profitto.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui l'Ente acquisti una singola licenza per un programma e provveda alla sua duplicazione, in modo da distribuire tali programmi al proprio interno e/o commercializzare tali programmi all'esterno.

Il comma 2 dell'art. 171 bis mira alla protezione delle banche dati; la condotta, invero, si concretizza nella riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; nell'estrazione o reimpiego della banca dati; nella distribuzione, vendita o concessione in locazione di banche di dati.

Per banche dati si intendono le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo, con esclusione dei contenuti e dei diritti sugli stessi esistenti.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui la Società, attraverso l'accesso a banche dati online (organismi di farmacovigilanza, enti di ricerca, ecc.), riproduca in tutto o in parte opere, testi e/o risultati di tipo scientifico al fine di trarne un vantaggio in termini di pubblicità.

Art. 171 ter, L. 633/1941

La norma punisce l'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; la riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Perché sia integrato il reato *de quo,* oltre alla realizzazione di una delle condotte descritte dalla norma, devono ricorrere due requisiti: il primo è che le condotte siano poste in essere per fare un uso non personale

dell'opera dell'ingegno, e il secondo è il dolo specifico di lucro, che costituisce il fine ulteriore che l'agente deve avere di mira perché sia integrato il fatto tipico previsto dalla norma.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui la Società filmi/registri le discussioni e tutte le attività svolte nel corso di meeting/convegni/congressi organizzati da società competitor o da altri enti al fine di riutilizzare quanto emerso nel corso di tali occasioni per erogare formazione all'interno della Società o formazione a pagamento presso terzi.

Art. 171 septies, L. 633/1941

Il reato si configura allorquando i produttori ed importatori dei supporti non soggetti a contrassegno SIAE non comunichino alla SIAE stessa, entro 30 giorni dalla commercializzazione o dall'importazione, i dati necessari per l'univoca identificazione dei supporti medesimi nonché qualora si dichiari falsamente l'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi.

La disposizione, pertanto, è posta a tutela delle funzioni di controllo della SIAE, in un'ottica di tutela anticipata del diritto di autore. La fattispecie, di conseguenza, è un reato di ostacolo che si configura con la mera violazione dell'obbligo.

Art. 171 octies, L. 633/1941

La diposizione punisce chi, a fini fraudolenti, produce, pone in vendita, promuove, installa, modifica, utilizza per uso pubblico o privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.

Ai fini della caratterizzazione della condotta, si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dall'imposizione di un canone per la fruizione del servizio.

Dal punto di vista soggettivo oltre alla consapevolezza e volontà della condotta tipica è richiesto il perseguimento di fini fraudolenti.

2. LE AREE POTENZIALMENTE "A RISCHIO REATO". LE ATTIVITÀ "SENSIBILI". I SOGGETTI COINVOLTI. I REATI PROSPETTABILI. I CONTROLLI ESISTENTI.

In occasione dell'implementazione dell'attività di *risk mapping*, sono state individuate, nell'ambito della struttura organizzativa ed aziendale di Novo Nordisk S.p.A. (in seguito **'Novo Nordisk'** o '**Società**'):

- le **aree** considerate "**a rischio reato**", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei delitti in materia di violazione dei diritti di autore;
- nell'ambito di ciascuna area "a rischio reato", sono state individuate le relative **attività c.d. "sensibili**", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in considerazione;

- **i ruoli aziendali coinvolti nell'esecuzione di tali attività "sensibili**" e che, astrattamente, potrebbero commettere i delitti in materia di violazione dei diritti di autore; sebbene tale individuazione dei ruoli/funzioni non debba considerarsi, in ogni caso, tassativa atteso che ciascun soggetto individuato nelle procedure potrebbe in linea teorica essere coinvolto a titolo di concorso; in particolare, nell'ambito dei ruoli coinvolti, sono state riportate anche le Società che, in virtù del contratto di servizi stipulato con Novo Nordisk (si veda par. **5.2.1**. della Parte Generale), svolgono le attività sensibili nell'interesse della Società;

- in via esemplificativa, i **principali controlli procedurali previsti** con riferimento alle attività che sono poste in essere nelle aree "a rischio reato", oltre alle regole definite nel Modello di organizzazione, gestione e controllo e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.) - dirette ad assicurare la chiara definizione dei ruoli e delle responsabilità degli attori coinvolti nel processo e l'individuazione dei principi di comportamento.

Di seguito è riepilogato il quadro in precedenza esposto per ogni area a rischio reato.

Area a rischio n. 1: ACQUISTI DI BENI E SERVIZI	
Funzioni aziendali coinvolte	- Accounting Manager - Quality Manager & BAQRP - Senior Legal & Compliance Manager - Strategic Operations Director
Attività sensibili e reati astrattamente ipotizzabili	**a) Raccolta e controllo delle proposte di acquisto** **b) Richieste di offerte, valutazione delle offerte, negoziazione e gestione degli acquisti urgenti** **c) Gestione del sistema di qualificazione e selezione dei fornitori** **d) Emissione degli ordini di acquisto** **e) Stipula e gestione dei contratti** **f) Verifica delle prestazioni/beni acquistati** **g) Gestione dei conferimenti di incarichi a consulenti / professionisti esterni** *1) Art. 171, terzo comma, L. 633/1941* *2) Art. 171 bis, primo e secondo comma, L. 633/1941* *3) Art. 171 ter, L. 633/1941*

Principali controlli esistenti	− adozione di specifiche procedure volte a disciplinare il processo di acquisto di beni e servizi nonché il processo di selezione e qualifica dei fornitori; in dettaglio, sono adottate le seguenti procedure: PROCEDURA ACQUISTI, Procedura di Accreditamento degli Intermediari, Business Ethics, Business Ethics Interaction with Healthcare Professionals, Business Ethics Interaction with Third Party Representatives, Gestione Contratti in Novo Nordisk S.p.A; − chiara definizione dei ruoli e delle responsabilità delle funzioni coinvolte nel processo, nonché dei reciproci flussi informativi; − diffusione, tramite sistema aziendale interno, delle procedure a tutte le risorse/funzioni coinvolte nel processo; − ambito di applicazione delle procedure chiaramente dettagliato; − il processo di selezione, approvazione e inserimento dei fornitori nell'albo fornitori prevede la selezione del/i fornitore/i da parte del Manager di Reparto: o all'interno dell'albo; o da inserire previa formale approvazione dello Strategic Operations Director; − il processo di selezione, approvazione e inserimento dei fornitori nell'albo dei fornitori, che possono avere rapporti con la PA, prevede l'approvazione definitiva da parte del MTI, un team composto dall'Amministratore Delegato, dai Direttori Strategic Operations, People & Organization, Clinical Medical & Regulatory, Biopharm, Diabetes Sales, Diabetes Marketing & CE, External Affairs & Market Access e dal Senior Legal & Compliance Manager − il processo di selezione, approvazione e inserimento dei fornitori nell'albo dei fornitori, per i fornitori di classe A, prevede una verifica da parte del Local Due Diligence Responsible (LDDR); per i fornitori di classe B che hanno o potrebbero avere rapporti con la PA è prevista una verifica secondo quanto stabilito dalla procedura di Accreditamento degli Intermediari. Al termine del processo di Due Diligence viene emesso dal LDDR un report sui risultati dell'indagine che viene inviato al Responsabile di Reparto per la valutazione definitiva. Il reparto Accounting provvede ad inserire i fornitori all'interno dell'albo. I Manager di Reparto oltre alla selezione dei fornitori provvedono anche a fornire il benestare al pagamento; − presenza di una prassi operativa che prevede, prima di scegliere uno specifico fornitore, l'effettuazione di contatti con due o più fornitori, a seconda delle spese di importo, presenti all'interno dell'albo fornitori, al fine dell'ottenimento delle offerte; − predisposizione nelle procedure di autorizzazione delle proposte di acquisto e di criteri e modalità di assegnazione del contratto; in dettaglio, in relazione alle proposte di acquisto presentate dai Manager di Reparto, gli User generano gli ordini di acquisto che vengono approvati con doppia firma del Direttore del Manager di Reparto e dello Strategic Operations Director. La Società prevede per qualsiasi tipologia di acquisto la formalizzazione di un contratto validato da doppia firma; − previsione dello svolgimento di una gara tra i fornitori presenti nell'albo fornitori al fine di acquistare qualsiasi tipologia di beni e servizi; − predisposizione di specifiche modalità di presentazione delle offerte; in dettaglio i Manager di Reparto richiedono ai fornitori selezionati i preventivi di spesa con indicazione del dettaglio delle spese; − definizione di criteri di valutazione delle offerte ricevute e formalizzazione delle valutazioni effettuate e decisioni prese (negoziazione); in dettaglio è prevista la valutazione di preventivi di spesa richiesti ai fornitori al fine di individuare la migliore offerta in termini di economicità e di qualità dei beni e servizi offerti; − previsione di un controllo ex post sull'eventuale utilizzo di fornitori non presenti all'interno dell'albo fornitori (anche in funzione dell'importo del contratto);

	- predisposizione di specifico strumento organizzativo che definisca le modalità di qualifica, valutazione e classificazione di fornitori e contrattisti; - predisposizione di verifiche modulari su tutte le categorie di rappresentanti di terze parti (RTP) che possono agire in nome della Società; - svolgimento di adeguate attività di Due Diligence, prima della definizione degli accordi con terze parti; - predisposizione di specifiche verifiche in relazione ad eventuali conflitti di interesse dei fornitori; - processo di qualifica, per ogni nuovo fornitore, con il quale questi viene sottoposto ad una analisi volta a valutare l'affidabilità economico-finanziaria, la professionalità e il possesso dei requisiti etici e tecnico-qualitativi; - predisposizione di specifiche liste di fornitori qualificati nelle quali iscrivere i soggetti in possesso dei requisiti richiesti; in dettaglio la Società dispone di un elenco dei fornitori qualificati che viene pubblicato su Globeshare. L'elenco viene aggiornato costantemente dal LDDR man mano che vengono effettuati o rinnovati i singoli processi di Due Diligence propedeuticamente all'utilizzo di un nuovo fornitore o al riutilizzo di un fornitore già esistente; - garanzia che per acquisti (singoli o cumulati) al di sopra di un valore soglia definito sia richiesto, per la qualifica del fornitore (e degli eventuali subappaltatori utilizzati), la richiesta di un'autocertificazione sul casellario giudiziale e sui carichi pendenti, effettuata nel processo di Due Diligence; - predisposizione di una black list per i fornitori con la definizione delle relative modalità di gestione (criteri di inserimento, aggiornamento e storicizzazione); inoltre i nominativi dei fornitori valutati come non idonei vengono inseriti all'interno di specifico documento nella sezione Legal di Globeshare; - predisposizione di specifiche verifiche sui fornitori in relazione a liste di terrorismo e riciclaggio; - svolgimento di una sistematica attività di analisi dei fornitori registrati al fine di disattivare fornitori non più utilizzati da un determinato lasso di tempo o doppi; - svolgimento di specifiche verifiche su eventuali cambi nella ragione sociale delle Società fornitrici e/o nella relativa compagine societaria; in dettaglio, nel caso di Fornitori di Categoria A, viene aggiornato annualmente il processo di Due Diligence attraverso il modulo di Certificazione annuale. Nel caso di cambi di ragione sociale il fornitore è obbligato alla compilazione di specifico modulo con le nuove specifiche societarie; - svolgimento di specifiche verifiche su variazioni in merito a dati bancari dei fornitori e/o consulenti; - adozione di un Codice di Comportamento rivolto ai fornitori che contenga regole etico-sociali atte a disciplinare i rapporti con l'impresa; - svolgimento con cadenza periodica di una verifica di riqualifica dei fornitori selezionati, anche, ad esempio, attraverso un questionario; - svolgimento di una valutazione delle attività e dei servizi sulla base dei principi di congruità o di criteri di FMV (Fair Market Value); - svolgimento di specifici audit al fine di verificare l'adeguatezza dei sistemi utilizzati ed il rispetto delle norme previste dalla legge presso i seguenti fornitori: "distribution", "External Call Center" e "Società di Archiviazione"; - formalizzazione degli accordi con il fornitore selezionato (OdA per i Fornitori di classe C o contratto per i fornitori di classe A e B); - previsione di un monitoraggio degli ordini aperti al fine di evitare il rischio di registrazione di transazioni improprie; in dettaglio è previsto un monitoraggio costante degli ordini fino alla conclusione del processo di acquisto al fine di evitare il rischio di registrazione di transazioni improprie; - previsione di modalità di gestione e relative approvazioni per eventuali

	modifiche/integrazioni dei PO; - identificazione di previsioni contrattuali standardizzate in relazione a natura e tipologie di contratto, contemplando clausole contrattuali finalizzate all'osservanza di principi di controllo nella gestione delle attività da parte del terzo e le attività da seguirsi nel caso di eventuali scostamenti; tutti i contratti con gli RTP di categoria A e B devono includere le clausole contrattuali globali di Etica Aziendale, con allegati i "Principi Chiave di etica Aziendale di Novo Nordisk", e una descrizione dettagliata dei servizi che verranno forniti o delle attività che saranno intraprese dai RTP; - previsione, negli schemi contrattuali/ordini utilizzati, di una clausola risolutiva del contratto in caso di mancato rispetto di quanto previsto dal modello ex D.Lgs. 231/01; - predisposizione di allegati ai contratti con i fornitori di clausole di Business Ethics; - raccolta di una dichiarazione sostitutiva del fornitore attestante l'assenza di provvedimenti a carico dell'ente o dei suoi apicali per reati della specie di quelli previsti dal decreto 231/01 (con particolare riferimento all'art 24-ter); - predisposizione di una clausola risolutiva espressa per il caso in cui l'impresa fornitrice non rispetti le norme di qualificazione etica, di autoregolamentazione o l'obbligo di denunciare i reati subiti direttamente o dai propri familiari e/o collaboratori; - raccolta di una dichiarazione sostitutiva del fornitore attestante il rispetto delle norme contributive, fiscali, previdenziali e assicurative verso i dipendenti e collaboratori; - raccolta di una dichiarazione sostitutiva del fornitore attestante il rispetto degli obblighi di tracciabilità finanziaria; - previsione che l'ente/soggetto destinatario del servizio certifichi (beni/servizi) formalmente la corrispondenza tra quanto richiesto e quanto effettivamente erogato (consegnato/prestato); - previsione di limiti relativamente alle spese vive da fatturare all'azienda (trasporto, vitto e alloggio) sostenute dal consulente per l'esecuzione dell'incarico; in dettaglio è previsto che le eventuali spese sostenute dal consulente per l'esecuzione dell'incarico, direttamente o tramite un'Agenzia selezionata, debbano essere indicate preventivamente nei contratti di consulenza; - predisposizione di controlli sui collaboratori esterni e sulla congruità delle provvigioni pagate rispetto a quelle praticate normalmente nell'area geografica di riferimento; - definizione dei passaggi operativi necessari per la finalizzazione di un acquisto, mediante l'utilizzo dei sistemi gestionali aziendali; - definizione formale degli acquisti eseguiti in eccezione alla procedura; - definizione dei limiti di importo in base ai quali applicare specifici flussi approvativi degli acquisti.

Area a rischio n. 2: GESTIONE SISTEMI INFORMATIVI/INFORMATION TECHNOLOGY	
Funzioni aziendali coinvolte	- Client Support Manager - Novo Nordisk IT
Attività sensibili e reati	**a) Gestione della sicurezza informatica sia a livello fisico che a livello logico**

astrattamente ipotizzabili	**b) Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio** **c) Gestione dell'attività di manutenzione dei sistemi esistenti e gestione dell'attività di elaborazione dei dati** **d) Gestione e protezione delle reti** **e) Attività di back-up dei dati e degli applicativi** **f) Gestione banche dati e software della società** *1) Art. 171, primo comma, lettera a-bis, L. 633/1941* *2) Art. 171, terzo comma, L. 633/1941* *3) Art. 171- bis, primo comma, L. 633/1941* *4) Art. 171- bis, secondo comma, L. 633/1941* *5) Art. 171 ter, L. 633/1941*
Principali controlli esistenti	− svolgimento delle attività relative alla gestione dei servizi IT da parte di Novo Nordisk Region Europe, in virtù di apposito contratto di servizio che ne disciplina condizioni e modalità; − adozione di apposite procedure volte a disciplinare che disciplinano la regolamentazione delle attività in cui si esplica il processo di gestione dei sistemi informativi; in dettaglio la Società è dotata di un Quality Management System che definisce i requisiti e gli standard per la documentazione di tutti i processi IT . Le procedure sono soggette a processo di revisione ed approvazione e poi archiviate nel sistema di archiviazione. La Società ha adottato procedure emesse dalla Capogruppo in relazione al processo di gestione dei sistemi informativi per i sistemi informativi gestiti dalla Capogruppo. La Società dispone anche di procedure volta a disciplinare il processo di gestione cambiamenti sui sistemi informativi. Inoltre la Società dispone di una procedura volta a disciplinare il processo di gestione del sito internet. Infine la Società si è dotata di una procedura volta alla gestione/archiviazione delle informazioni aziendali; − chiara identificazione dei ruoli e delle responsabilità delle funzioni coinvolte nel processo di gestione dei sistemi informativi; − diffusione delle procedure aziendali attraverso un sistema aziendale interno; − chiara segregazione di funzioni e responsabilità nelle attività relative alla gestione della rete, all'amministrazione dei sistemi e allo sviluppo/manutenzione degli applicativi; in dettaglio la Società fornisce i servizi IT alla Novo Nordisk Region Europe; il processo prevede il coinvolgimento della Capogruppo, presso cui sono detenuti tutti i server delle Società del Gruppo Novo Nordisk (gestiti da un fornitore esterno), e di un Gruppo europeo di cui il Client Support Manager fa parte; − adozione di procedure, emanate e gestite a livello centralizzato, per la gestione delle credenziali di accesso ai sistemi ed il loro monitoraggio periodico; − adozione di specifica procedura nella quale sono definiti criteri per le attribuzioni degli accessi ai dati e che identifica i soggetti aventi parte nel processo di richiesta, verifica ed autorizzazione degli accessi; − predisposizione di una procedura che disciplini la rimozione dei diritti di accesso al

	termine del rapporto di lavoro; - predisposizione di procedure di batch; - segregazione delle funzioni, nell'ambito della creazione/profilazione delle utenze, in relazione ad eventuali ulteriori incarichi ricoperti all'interno del Gruppo; in dettaglio è previsto un processo volto ad accertare la segregazione delle funzioni all'interno dei singoli processi tramite la revisione della richiesta dello specifico ruolo da parte del manager del dipartimento e dal "System Owner" ovvero il gestore dello specifico sistema informativo; - separazione delle competenze garantita da una separazione degli accessi ai sistemi informativi; - esecuzione delle fasi di creazione/cancellazione delle utenze in accordo con l'area delle Risorse Umane; - effettuazione delle fasi di modifica delle utenze in accordo con l'Ente richiedente; - svolgimento a livello centralizzato della gestione delle configurazioni dei PC e del loro monitoraggio; - predisposizione di operazioni di intervento e ripristino delle configurazioni dei sistemi in caso di anomalia; - identificazione di tutti gli utenti attraverso una user ID personale tramite il quale accedono ai vari applicativi; - definizione di criteri minimi di robustezza per la scelta delle password (ogni password è alfanumerica e contiene almeno un carattere maiuscolo e almeno un segno di interpunzione); - rinnovo periodico e obbligatorio delle password; - inibizione dell'utilizzo della medesima password per più di una volta; - obbligo del cambio della password al primo login; - divieto di lasciare attiva una sessione di lavoro in caso di allontanamento dal PC; - necessità di nuovo login con password dopo diversi minuti di inattività; - predisposizione di misure per un'adeguata protezione delle apparecchiature incustodite; - mappatura e monitoraggio dei sistemi stand alone; - predisposizione di adeguato riscontro delle password di abilitazione per l'accesso ai Sistemi Informativi della PA, possedute, per ragioni di servizio, da determinati dipendenti appartenenti a specifiche funzioni/strutture aziendali; in dettaglio i dipendenti provvedono in autonomia alla creazione di profili per comunicare/inviare documentazione alla PA. Il dipartimento Quality, con il supporto dell'IT, provvede a mappare tali sistemi qualora le aree aziendali ne diano comunicazione. Per ogni sistema utilizzato viene richiesto al "System Manager" su base annuale la produzione e la revisione di documentazione (BIA - Business Impact Assessment, SIA - System Impact Assessment, Personal Data LyfeCycle Sheet) di riferimento per ogni sistema censito. La funzione QA coordina e supervisiona questo processo. Infine il Servizio IT prevede attività di training ed aggiornamento i al fine di sensibilizzare i dipendenti della Società in relazione ai predetti aspetti. Tutti i dipendenti ricevono ogni anno alcune procedure IT da rivedere e firmare, identificate dalla funzione QA; - utilizzo della firma digitale per la trasmissione della documentazione alla PA da parte delle funzioni preposte a tale attività; - adozione di misure di protezione dei documenti elettronici (es. Firma digitale); - obbligo, per gli utenti, di corsi di formazione on-line, organizzati dalla Società, finalizzati alla sensibilizzazione all'uso appropriato degli strumenti informatici ed alle misure di sicurezza; - adozione di direttive e norme di carattere etico, dirette ai singoli utenti, riguardanti tutti i processi legati all'Information Technology e finalizzate alla sensibilizzazione in tale ambito;

	- previsione di apposite disposizioni nelle procedure volte a prevedere: limitazione dell'utilizzo dei sistemi informatici o telematici ai soli fini lavorativi; accesso alle informazioni societarie solo previa autorizzazione da un livello manageriale adeguato; accesso alle informazioni societarie solo mediante gli strumenti concessi ed autorizzati dalla società; riservatezza delle informazioni societarie; elaborazione dei dati nel rispetto delle modalità previste dalle procedure societarie; integrità dei dati elaborati; impossibilità di installare sui sistemi informatici/telematici societari software o hardware non autorizzati; impossibilità di introdurre in società dispositivi hardware/software non autorizzati; - predisposizione di clausole, negli accordi con terzi e nei contratti di lavoro, di non divulgazione delle informazioni; - predisposizione di ambienti dedicati per quei sistemi che sono considerati "sensibili" sia per il tipo di dati contenuti sia per il valore di business; - definizione formale dei criteri per l'identificazione dei soggetti proprietari dei dati e per la loro classificazione; - regolamentazione di una procedura per il trasferimento dei dati sensibili mediante supporti esterni o rimovibili; - predisposizione di una procedura che prescriva, per il dipendente, la richiesta di autorizzazioni per esportare dati all'esterno; - adozione di una procedura nella quale è definita la modalità di crittografia che i dipendenti devono adottare per lo scambio dati; - esplicito riferimento, nelle procedure adottate dalla Società, della responsabilità dei dipendenti nei confronti delle informazioni loro affidate; - predisposizione di una procedura che disciplini lo smarrimento/compromissione/alterazione dei dati aziendali; - istituzione, nella sede della Società, di un Centro Elaborazione Dati il cui accesso a è riservato esclusivamente al personale autorizzato; - formalizzazione in procedura del processo di assegnazione degli asset della Società; - formalizzazione, all'interno delle procedure, delle regole per il corretto utilizzo dei beni societari destinati allo scambio ed elaborazione di dati (PC desktop, laptop, cellulari, ecc.) che sono sottoscritte da tutti i dipendenti, contractors, fornitori autorizzati, partner commerciali e altri fornitori di servizi che utilizzano beni della Società; - espressi ed inequivocabili richiami ad un corretto utilizzo degli strumenti informatici in possesso dei dipendenti; - allestimento di misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro della Società; - predisposizione di accessi da remoto verso la rete aziendale solo tramite VPN crittografata; - divieto assoluto di accesso ai siti a pagamento, a quelli contenenti materiale osceno ovvero collegato, a qualsiasi titolo, ad attività illecite; - divieto di configurare Client di posta non aziendali; - previsione di limitazioni nell'utilizzo di dispositivi elettronici che prescrivono che l'accesso ad Internet sia consentito per finalità attinenti l'attività lavorativa mentre viene tollerato il moderato utilizzo per fini personali purché lo stesso, direttamente o indirettamente, non costituisca reato; - centralizzazione a livello globale del coordinamento delle attività legate alla sicurezza; - adeguata comunicazione e delle procedure di sicurezza informatica (fisica/logica) (es.: utilizzo di password, ID number, sistemi antincendio, sistemi di allarmi, ecc.), nonché periodicamente testate;

	- presenza di personale tecnico preparato e preposto principalmente a garantire il buon funzionamento dei sistemi informativi; - predisposizione di specifici controlli su: rete aziendali e informazioni che vi transitano; instradamento (routing) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza; installazione di SW sui sistemi operativi; - utilizzo di software antivirus che controllano il traffico di rete in entrata ed in uscita e sensibilizzazione, digitalmente tracciata, sul tema nei confronti degli gli utenti; - predisposizione di misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema accessibile al pubblico, al fine di prevenire modifiche non autorizzate; - periodico aggiornamento dei sistemi informativi; - installazione di un proxy server e/o firewall che effettui il monitoraggio del traffico di dati segnalando eventuali anomalie e mantenendone traccia; - predisposizione di procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi; - adozione di un sistema di Software/hardware Inventory che monitora singolarmente ogni PC/Utente; - inventariazione dei software e hardware per ogni singolo Utente segnalando eventuali anomalie; - redazione di file Log per le varie attività dei sistemi informativi; - tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali; - adozione di una procedura di change management che regoli ogni tipo di cambiamento riguardante sistemi ed infrastrutture, definendo vari sub-processi ed i corrispondenti responsabili; - predisposizione di un controllo periodico volto a riconciliare il numero di licenze acquistate vs il numero di utenti autorizzati; - predisposizione di un elenco dei SW aziendali e dei relativi amministratori di sistema; in dettaglio è prevista una mappatura periodica dei sistemi aziendali. Per ogni sistema viene definito un System Manager (amministratore lato tecnico) e un System Owner (lato funzionale). Attualmente la Società dispone di sistemi suddivisi in: Sistemi globali; Sistemi europei; Sistemi Locali. Nel caso di integrazione di nuovi sistemi è necessaria l'approvazione da parte del Comitato europeo; - adeguata archiviazione della documentazione relativa al ciclo di approvazione delle modifiche/cancellazioni/integrazioni dei siti internet; - predisposizione di ambienti di sviluppo, collaudo e produzione; - utilizzo di dispositivi hardware e software specifici per il salvataggio degli applicativi e per il salvataggio dei dati; - adeguato tracciamento del processo di aggiornamento degli applicativi/DB; - formalizzazione di una procedura per il back up dei dati, gestita a livello centrale; - formale definizione della frequenza dei back-up, le modalità e i tempi di conservazione dei supporti per i dati; - necessaria autorizzazione formale a procedere in caso sia necessario effettuare un restore dei dati di back-up; - predisposizione di appositi registri per documentare le attività di back-up e i restore effettuati; - custodia dei back-up in luogo protetto da furti e incendi nonché diverso rispetto a quello in cui sono custoditi i dati; - predisposizione di procedure a livello globale per la gestione degli incidenti che definiscono ruoli, modalità operative e urgenze per tutte le fasi della gestione degli incidenti, tramite un sistema di gestione dei ticket; - predisposizione di un piano di Disaster Recovery System; - predisposizione di un processo di autorizzazione della direzione per le strutture di

	elaborazione delle informazioni; - pedissequo rispetto, da parte della Società, della normativa sulla privacy; - predisposizione di procedure per l'etichettatura e il trattamento delle informazioni in base allo schema di classificazione adottato; - predisposizione di apposite verifiche sui mezzi di comunicazione interni ed esterni al fine di prevenire la diffusione di informazioni sensibili.

Area a rischio n. 3: ATTIVITÀ DI COMUNICAZIONE ESTERNA/PUBLIC AFFAIRS	
Funzioni aziendali coinvolte	- Digital & New Media Marketing Project Manager - Government Affairs & External Relation Director
Attività sensibili e reati astrattamente ipotizzabili	**a) Gestione dei rapporti con i mass media, compresi:** **- contatti con giornalisti e/o rappresentanti dei mass media (giornali, radio, televisione)** **- gestione delle iniziative con i mass media (giornali, radio, televisione)** **b) Scelta e pubblicazione dei testi/immagini e di qualsiasi altro contenuto suscettibile di essere protetto da diritti di proprietà industriale/intellettuale** *1) Art. 171, primo comma, lettera a-bis, L. 633/1941* *2) Art. 171 bis, secondo comma, L. 633/1941* *3) Art. 171, terzo comma, L. 633/1941* *4) Art. 171 ter, L. 633/1941*
Principali controlli esistenti	- definizione, approvazione e aggiornamento di una procedura che disciplina il processo di gestione del sito internet e twitter; - definizione formale dei ruoli, delle responsabilità, dei flussi informativi tra le varie funzioni aziendali coinvolte e diffusione formale della procedura attraverso la pubblicazione sul sistema aziendale interno; - chiara segregazione delle funzioni coinvolte nel processo; in particolare, il sito internet è gestito dal Digital & New Media Marketing Project Manager, inoltre è previsto un Editorial Board che provvede ad approvare e verificare i contenuti presenti sul sito internet formato dal Regulatory Affairs Manager e dal Senior Legal & Compliance Manager; - definizione di ruoli e responsabilità deputate ad intrattenere rapporti con i mass media; - svolgimento di un monitoraggio periodico dei siti internet al fine di verificare che la loro gestione avvenga secondo le linee guida stabilite; - definizione del Responsabile della gestione del sito internet aziendale,; - chiara identificazione, nel sito internet predisposto, della fonte di tutte le informazioni riportate sul sito stesso, nonché i destinatari di tali informazioni e gli obiettivi; - specifico coinvolgimento dell'area medica nel caso in cui il materiale prodotto per la comunicazione abbia contenuti scientifici; - i contenuti ed il materiale sviluppati per la pubblicazione sul sito web della società di carattere promozionale sono riservati agli operatori previsti dalla normativa di riferimento e dal Codice Deontologico;

	− definizione di uno specifico iter di approvazione dei contenuti e del materiale da pubblicare attraverso il sito web, al fine di verificare la coerenza dei contenuti con gli obiettivi e le aree di intervento della Società; − deposito presso l'AIFA del materiale diffuso via internet, salvo che non sia già stato preventivamente autorizzato; − svolgimento di procedure autorizzative per comunicati stampa, strutturate in vari controlli sulle successive bozze dei comunicati fino alla versione definitiva attraverso il coinvolgimento delle funzioni responsabili e dei soggetti preposti alle verifiche contabili; − svolgimento di una gestione conforme alle disposizioni previste dal Codice Deontologico di Farmindustria in relazione ai trasferimenti di valore effettuati direttamente o indirettamente con gli Operatori Sanitari e con le Organizzazioni Sanitarie − Definzione delle responsabilità in materia di pubblicazione dei contenuti tramite twitter..

Area a rischio n. 4: GESTIONE DEI MATERIALI PROMOZIONALI	
Funzioni aziendali coinvolte	- Clinical, Medical & Regulatory Director - Regulatory Affairs Manager - Degludec Franchise Marketing Manager - Biopharm Director
Attività sensibili e reati astrattamente ipotizzabili	**a) Offerta e distribuzione di materiale scientifico/omaggi quali, ad es., brand reminder e supporti cartacei e/o elettronici e/o informatici ecc.** **b) Diffusione e distribuzione di materiale scientifico/omaggi quali, ad es., brand reminder e supporti cartacei e/o elettronici e/o informatici ecc., suscettibili di essere protetti dal diritto d'autore** *1) art. 171 bis, primo e secondo comma, L. 633/1941* *2) art. 171, terzo comma, L. 633/1941* *3) art. 171 ter, L. 633/1941*
Principali controlli esistenti	− definizione, approvazione ed aggiornamento di una serie di procedure che disciplinano la regolamentazione delle attività in cui si esplica il processo di gestione del materiale informativo/promozionale; identificazione chiara dei ruoli aziendali responsabili delle funzioni coinvolte nel processo; − diffusione formale a tutte le risorse/funzioni coinvolte nel processo attraverso la pubblicazione sul sistema aziendale interno; − chiara segregazione delle funzioni coinvolte nelle attività relative alle fasi di progettazione, approvazione, esecuzione, chiusura e rendicontazione della gestione del materiale informativo/promozionale; in dettaglio, il materiale promozionale viene predisposto dalla Capogruppo ed inviato alla Società, la quale adatta il materiale alle normative e alle esigenze di marketing nazionali; il processo prevede il coinvolgimento del Dipartimento Marketing per le attività relative alla gestione degli adattamenti del materiale, del Responsabile del Servizio Scientifico

	per la verifica e approvazione dell'idoneità del materiale, del Regulatory Affairs Manager per la verifica e approvazione della conformità del materiale alle normative vigenti, del Medical Department per la verifica delle referenze e delle informazioni scientifiche del materiale, nonché dell'Autore del Materiale per la trasmissione del Materiale all'AIFA o al Ministero della Salute per l'approvazione; - distribuzione ai medici di omaggi promozionali di un valore economico percepito trascurabile, infungibili e acquistati direttamente dall'azienda a livello centrale; - attinenza dei materiali informativo/promozionali alle attività esercitate dal medico; - contenuti dell'informazione sempre aggiornata e documentata; - adeguata e formale approvazione dei materiali informativi/promozionali da un punto di vista scientifico e con l'indicazione del prezzo; - monitoraggio del valore dei materiali informativo/promozionali (brand reminder e materiali di supporto alla diagnosi e terapia) distribuiti al medico, al fine di rispettare i limiti previsti dalla normative regionali; - previsione del flusso di distribuzione e aggiornamento dei materiali informativi/promozionali alla Field Force nonché rispetto dei 10 gg. di legge prima della distribuzione del materiale informativo/promozionale alla Field Force; - cessione a titolo gratuito del materiale informativo di consultazione scientifica o di lavoro solamente alle strutture sanitarie pubbliche (ad eccezione del materiale con valore < 25 euro); - donazione a titolo gratuito solo alle strutture pubbliche dei documenti con indirizzo medico-scientifico disciplinati dall'art 123, comma 2, D.lgs. 219/2006 e D.M. 14 Aprile 2008 (a) libri e monografie professionali; b) abbonamenti a riviste; c) iscrizioni a newsletter online; d) cd, dvd o password); - netta separazione tra informazione e pubblicità, nel rispetto della regola della trasparenza, in merito alla pubblicità su giornali e riviste, garantendo sempre al lettore l'immediata riconoscibilità del messaggio promozionale in qualunque sua forma, sia essa redazionale che tabellare; - disciplina attraverso procedure/linee guida del richiamo del materiale informativo/promozionale in caso di blocco divulgativo/sospensione del materiale obsoleto; - attività di controllo volto a verificare che quanto inviato dal fornitore di beni (stampa, brand reminder) risulti coerente con il materiale informativo/promozionale richiesto; - archiviazione di tutta la documentazione relativa ai materiali informativo/promozionali sviluppati; - previsione ed apposizione di modifiche sul materiale informativo/promozionale acquisito dalla Capogruppo, al fine di allinearlo alle esigenze di marketing e alla normativa vigenze nazionale; - selezione delle agenzie che si occupano di sviluppare la creazione dei materiali informativi/promozionali all'interno di un albo fornitori e attraverso una gara tra almeno due fornitori; - disciplina formale dei rapporti con i fornitori di materiali informativi/promozionali attraverso la stipula di contratti; in particolare, i suddetti contratti vengono redatti secondo form contrattuali standard stilati dalla funzione legale; - definizione di un'apposita clausola risolutiva all'interno dei contratti in caso di violazione del Modello ex D.Lgs. 231/01; - approvazione di un contratto da parte di un soggetto dotato di idonea procura (nei limiti e negli ambiti consentiti); - invio all'AIFA per l'approvazione di tutti i mezzi informativo/promozionale; - conformità delle informazioni contenute nel materiale informativo/promozionale con la documentazione presentata ai fini dell'AIC.

3. I PRINCIPI GENERALI DI COMPORTAMENTO

Nell'espletamento della propria attività per conto di Novo Nordisk, i responsabili della funzione coinvolta nell'area "a rischio reato" sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico.

A tutti i soggetti i destinatari del Modello è fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dall'art. 25 *novies* del Decreto;
- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- di duplicare, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale, o comunque per trarne profitto, senza averne diritto, programmi per elaboratori, banche dati protette ovvero qualsiasi opera protetta dal diritto d'autore e da diritti connessi, incluse opere a contenuto letterario, musicale, multimediale, cinematografico, artistico;
- di diffondere tramite reti telematiche - senza averne diritto - un'opera dell'ingegno o parte di essa;
- di mettere in atto pratiche di file sharing, attraverso lo scambio e/o la condivisione di qualsivoglia tipologia di file attraverso piattaforme di tipo peer to peer.

È, inoltre, necessario:

- che tutte le attività e le operazioni svolte per conto di Novo Nordisk – ivi incluso per ciò che attiene i contatti relativi a rapporti con società del Gruppo - siano improntate al massimo rispetto delle leggi vigenti, con particolare riferimento alle norme vigenti in materia di violazione del diritto di autore, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- che sia rispettato il principio di separazione di ruoli e responsabilità nelle fasi dei processi interni dell'Ente;
- che sia assicurata la massima rispondenza tra i comportamenti effettivi e quelli richiesti dalle procedure interne, prestando una particolare attenzione per ciò che concerne lo svolgimento delle attività "sensibili" nelle aree ''a rischio reato" indicate nel par. 2.;
- che coloro che svolgono una funzione di controllo e supervisione in ordine agli adempimenti connessi all'espletamento delle suddette attività ''sensibili'' pongano particolare attenzione all'attuazione degli adempimenti stessi e riferiscano immediatamente all'Organismo di Vigilanza (di seguito, anche 'OdV') eventuali situazioni di irregolarità.

Inoltre, ai fini dell'attuazione dei comportamenti di cui sopra, Novo Nordisk:

- ha inserito nelle norme di comportamento (o Codice Etico) adottate dall'Ente specifiche previsioni riguardanti i delitti in materia di violazione dei diritti d'autore;
- ha previsto sanzioni in caso di violazione del Modello anche con riferimento alle fattispecie di cui alla presente Parte Speciale;
- ha previsto la realizzazione di una adeguata attività di comunicazione e formazione sui contenuti del Codice Etico e del Modello di organizzazione, gestione e controllo;
- dispone di regole sull'utilizzo di materiale protetto da diritto d'autore;
- ha previsto la formalizzazione di contratti di ricerca e di clausole specifiche per la gestione dei diritti d'autore;
- ha previsto il divieto di installazione e utilizzo non autorizzato di sistemi di file sharing.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.