MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del Decreto legislativo 8 giugno 2001, n. 231)

Parte Speciale

Approvato dal Consiglio di Amministrazione
Di Careapt S.r.l. in data7/03/2022

Sommario

PARTE SPECIALE A REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E IL SUO PATRIMONIO, REATO DI CORRUZIONE FRA PRIVATI E REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA 5

FUNZIONE DELLA PARTE SPECIALE A 6

FATTISPECIE DI REATO RILEVANTI 6

A.1 Reati contro la Pubblica Amministrazione ed il suo patrimonio (artt. 24 e 25 D.lgs. 231/2001) 6

A.2 Reato di corruzione tra privati 9

A.3 Delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria 9

PRINCIPALI AREE DI RISCHIO 10

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO 10

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 28

SANZIONI 28

PARTE SPECIALE B 29

DELITTI INFORMATICI, TRATTAMENTO ILLECITO DI DATI E REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE 29

FUNZIONE DELLA PARTE SPECIALE B 30

FATTISPECIE DI REATO RILEVANTI 30

PRINCIPALI AREE A RISCHIO 38

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO 39

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 42

SANZIONI 42

PARTE SPECIALE C 43

REATI SOCIETARI E REATI TRIBUTARI 43

FUNZIONE DELLA PARTE SPECIALE C 44

FATTISPECIE DI REATO RILEVANTI 44
C.1 Reati societari (art. 25-ter D.lgs. 231/2001) 44
C.2 Reati tributari (art. 25-quinquiesdecies D.lgs. 231/2001) 46

PRINCIPALI AREE A RISCHIO 48

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO 49

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 55

SANZIONI 55

PARTE SPECIALE D 56

DELITTI DI CRIMINALITA' ORGANIZZATA E REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO 56

FUNZIONE DELLA PARTE SPECIALE D 57

FATTISPECIE DI REATO RILEVANTI 57
D.1 Delitti di criminalità organizzata (art. 24-ter D.lgs. 231/2001) 57
D.2 Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies D.lgs. 231/2001) 57

PRINCIPALI AREE DI RISCHIO 58

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO 59

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 61

SANZIONI 61

PARTE SPECIALE E 62

DELITTI DI OMICIDIO COLPOSO E LESIONI PERSONALI COLPOSE GRAVI E GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME A TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO 62

FUNZIONE DELLA PARTE SPECIALE E 63

FATTISPECIE DI REATO RILEVANTI 63
E.1 Delitti di omicidio colposo e lesioni personali colpose gravi e gravissime commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro (art. 25-septies D.lgs. 231/2001) 63

PRINCIPALI AREE DI RISCHIO 64

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO 64

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 68

SANZIONI 68

PARTE SPECIALE F 69

DELITTI CONTRO LA PERSONALITA' INDIVIDUALE E REATO DI IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE 69

FUNZIONE DELLA PARTE SPECIALE F 70

FATTISPECIE DI REATO RILEVANTI 70

F.1 Delitti contro la personalità individuale 70

F.2 Delitto di impiego di cittadini di stati terzi il cui soggiorno è irregolare 71

PRINCIPALI AREE DI RISCHIO 71

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO 72

PARTE SPECIALE A

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E IL SUO PATRIMONIO, REATO DI CORRUZIONE FRA PRIVATI E REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA

FUNZIONE DELLA PARTE SPECIALE A

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i "Destinatari" del Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato richiamate dagli artt. 24, 25, 25-*ter* (limitatamente al reato di corruzione tra privati) e 25-*decies* del D.lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione, nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di definire:

- i principi di comportamento che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- i flussi informativi all'Organismo di Vigilanza.

FATTISPECIE DI REATO RILEVANTI

Di seguito vengono riportate le fattispecie di reato ritenute rilevanti per Careapt ai sensi degli artt. 24, 25, 25-*ter* (come sopra specificato) e 25-*decies* del Decreto.

A.1 Reati contro la Pubblica Amministrazione ed il suo patrimonio (artt. 24 e 25 D.lgs. 231/2001)

Malversazione a danno dello Stato (art. 316-*bis* c.p.)

Il reato si configura nel caso in cui, dopo avere legittimamente ricevuto finanziamenti o contributi da parte dello Stato italiano o da altro Ente Pubblico o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta; nessun rilievo assume il fatto che l'attività programmata si sia comunque svolta).

Indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* c.p.)

Il reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri Enti pubblici o dalla Unione Europea.

A nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Questa ipotesi di reato è residuale rispetto alla più grave fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa aggravata per il percepimento di erogazioni pubbliche.

Frode nelle pubbliche forniture (art. 356 c.p.)

Il reato si configura nel caso in cui venga commessa una frode nella esecuzione dei contratti di fornitura o nell'adempimento degli obblighi contrattuali che derivano da un contratto di fornitura concluso con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità.

Truffa a danno dello Stato o di altro Ente pubblico (art. 640, comma 2, n. 1, c.p.)

Il reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente pubblico o all'Unione Europea).

Il reato può realizzarsi, ad esempio, nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (per esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.)

Il reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.

Questa fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-*ter* c.p.)

Il reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro Ente Pubblico. È prevista un'aggravante nel caso in cui il fatto sia commesso con furto o indebito utilizzo dell'identità digitale.

Concussione (art. 317 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale, abusando della propria posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli.

Tale forma di reato potrebbe ravvisarsi nell'ipotesi in cui un Dipendente od un agente della società, concorra nel reato commesso dal pubblico ufficiale, il quale, approfittando di tale sua qualità, richieda a terze prestazioni non dovute (sempre che tale comportamento sia posto in essere nell'interesse, anche non esclusivo, della società).

Corruzione per l'esercizio della funzione (artt. 318 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

Ai fini della consumazione non è necessaria l'identificazione di uno specifico atto quale oggetto dell'accordo illecito e la tipicità del reato riposa nel fatto che la consegna del denaro o di altra utilità venga effettuata semplicemente in ragione delle funzioni esercitate dal pubblico ufficiale e per retribuirne i favori.

La fattispecie di cui trattasi potrebbe concretizzarsi mediante l'assunzione di personale segnalato dal pubblico ufficiale, mediante il riconoscimento a quest'ultimo (o a terzi al medesimo riconducibili) di compensi non in linea con la prestazione/fattura erogata oppure ancora mediante l'assegnazione di beni fittiziamente a titolo di omaggio o liberalità.

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve per sé o per un terzo, in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa.

Circostanze aggravanti (art. 319-*bis* c.p.)

La circostanza aggravante di cui trattasi ricorre nelle ipotesi in cui la corruzione per un atto contrario ai doveri d'ufficio abbia per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi.

Corruzione in atti giudiziari (art. 319-*ter*, comma 2, e 321 c.p.)

Il reato si potrebbe configurare nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario). Il reato in parola è punito più gravemente della corruzione semplice.

Induzione indebita a dare o promettere utilità (art. 319- *quater* c.p.)

La norma punisce il pubblico ufficiale o l'incaricato di pubblico servizio che abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità, salvo che il fatto costituisca più grave reato.

La punibilità è estesa anche al soggetto privato che è indotto al pagamento o alla sua promessa (che diventa dunque soggetto attivo concorrente).

Ai fini dell'integrazione della fattispecie di cui trattasi debbono sussistere i seguenti elementi:

- una condotta del soggetto attivo che deve tradursi in un'attività di induzione;
- un evento incarnato da due condotte del soggetto passivo (promessa o dazione indebita di denaro o altra utilità);
- un nesso eziologico tra induzione ed evento finale;
- la rappresentazione e volizione della propria azione antigiuridica.

Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)

Le disposizioni degli artt. 318 e 319 c.p. si applicano anche all'incaricato di un pubblico servizio.

Pene per il corruttore (art. 321 c.p.)

Le pene stabilite agli art. 318, comma 1, 319, 319-*bis*, 319-*ter* e 320 c.p. in relazione alle ipotesi degli art. 318 e 319 c.p., si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità.

Istigazione alla corruzione (art. 322 c.p.)

Vi incorre chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri qualora l'offerta o la promessa non sia accettata.

Vi incorre chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, se l'offerta o la promessa è fatta per indurre ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, qualora l'offerta o la promessa non sia accettata.

La pena si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri.

Traffico di influenze illecite (art.346-*bis* c.p.)

Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-*ter* e nei reati di corruzione di cui all'articolo 322-*bis*, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322- *bis*, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-*bis*, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri, è punito con la pena della reclusione da un anno a quattro anni e sei mesi.

A.2 Reato di corruzione tra privati

Corruzione fra privati (art. 2635 c.c.)

La norma punisce amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori (anche per interposta persona), i quali, sollecitino o ricevano, per sé o per altri, denaro o altra utilità non dovuti, o ne accettino la promessa, per compiere od omettere un atto, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

Istigazione alla corruzione tra privati (art. 2635-*bis* c.c.)

La norma punisce chiunque offra o prometta denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.

A.3 Delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.)

Il reato si configura allorquando taluno, con violenza, minaccia, con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere, davanti alla autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale, quando questa ha facoltà di non rispondere[1], salvo che il fatto costituisca più grave reato.

[1] Si tratta di soggetti che rivestono la qualifica di indagato (o imputato), dei loro prossimi congiunti a cui la legge conferisce la facoltà di non rispondere, ai sensi dell'art. 199 c.p.p. e dei soggetti che assumono la veste di indagato (o imputato) di reato connesso o collegato, sempre che gli stessi non abbiano già assunto l'ufficio di testimone.

PRINCIPALI AREE DI RISCHIO

Le principali aree di rischio della Società, con riferimento ai reati contro la Pubblica Amministrazione e il suo Patrimonio, al reato di corruzione fra privati ed al delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, sono riconducibili a:

- *Gestione delle attività commerciali;*
- *Gestione degli adempimenti amministrativi ed attività ispettive;*
- *Gestione dei rapporti con l'Autorità Giudiziaria e dei contenziosi;*
- *Selezione e gestione del personale e del sistema di incentivazione;*
- *Gestione delle note spese;*
- *Gestione dei rapporti con Operatori Sanitari ed Organizzazioni Sanitarie;*
- *Gestione delle attività di comunicazione e sponsorizzazione;*
- *Gestione degli omaggi;*
- *Gestione degli studi clinici;*
- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*
- *Gestione dei rapporti Intercompany;*
- *Gestione dei flussi finanziari.*

I Destinatari sono tenuti ad adeguare il proprio comportamento a quanto esposto nel presente documento.

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari, come definiti nella Parte Generale del presente Modello.

In generale, **è fatto obbligo** di assicurare che lo svolgimento delle predette attività avvenga nell'assoluto rispetto di:

- leggi e normative vigenti;
- principi di lealtà, correttezza e chiarezza;
- Codice Etico.

In generale, **è fatto divieto** di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di cui agli artt. 24, 25, 25-*ter* (come sopra specificato) e 25-*decies* del D.lgs. 231/2001 innanzi richiamate.

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alle seguenti attività:

- ***Gestione delle attività commerciali.***

La gestione delle attività commerciali potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, un soggetto sottoposto o apicale della Società offra o prometta denaro od altra utilità ad un pubblico ufficiale, ad un incaricato di pubblico servizio o a soggetti da questi indicati, al fine di compiere un'azione corruttiva o comunque per ottenere trattamenti di favore nell'ambito delle responsabilità del pubblico ufficiale.

La gestione delle attività commerciali potrebbe presentare profili di rischio in relazione al **reato di corruzione fra privati** nell'ipotesi in cui, ad esempio, un soggetto sottoposto o apicale della Società offra o prometta denaro od altra utilità ad una controparte privata al fine di ottenere la stipula di un contratto per la vendita di un prodotto ad un prezzo superiore a quello di mercato ovvero a condizioni particolarmente sfavorevoli rispetto agli standard normalmente in uso a danno della controparte.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione della predetta attività **è fatto obbligo** di:

- garantire che i rapporti con le controparti avvengano nell'assoluto rispetto di leggi, normative vigenti e principi di lealtà, correttezza, chiarezza e trasparenza;
- mantenere elevati *standard* di integrità in tutte le interazioni con soggetti pubblici e privati, adottando comportamenti trasparenti e responsabili;
- assicurarsi che i rapporti con la clientela siano gestiti da soggetti specificamente individuati e muniti di idonei poteri;
- garantire adeguata segregazione tra i soggetti incaricati di gestire i rapporti con la clientela e quelli incaricati di definire i prezzi del servizio, nonché i termini e le condizioni di pagamento;
- assicurarsi che la definizione dei prezzi sia effettuata da soggetti muniti di idonei poteri;
- garantire che le condizioni per l'erogazione del servizio di teleassistenza infermieristica siano stipulate all'interno di specifici contratti;
- assicurare che qualsiasi impegno contrattuale che genera diritti e/o obblighi in capo alla Società, sia sottoscritto da soggetti dotati di idonei poteri;
- verificare la regolarità della fatturazione nei confronti della clientela;
- garantire che tutta la documentazione relativa al processo di gestione delle attività commerciali sia archiviata a cura delle funzioni aziendali coinvolte nel processo;
- comunicare, senza ritardo, al proprio responsabile gerarchico o al management della Società e, contestualmente, all'Organismo di Vigilanza eventuali comportamenti posti in essere da quanti operano per la controparte, rivolti ad ottenere favori, elargizioni illecite di danaro od altre utilità, anche nei confronti dei terzi, nonché qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- promettere o concedere denaro o altre utilità a controparti pubbliche o private o a persone a queste vicine, anche per il tramite di soggetti terzi, al fine di favorire la stipula di un contratto di fornitura;
- effettuare prestazioni o pagamenti in favore di soggetti terzi che operino per conto della Società nell'ambito delle attività disciplinate dal presente protocollo, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- stipulare contratti di fornitura con prezzi e condizioni stabilite secondo parametri non oggettivi;
- presentare offerte non sottoposte all'approvazione dei soggetti dotati di idonei poteri;
- presentare dichiarazioni non veritiere esibendo documenti in tutto o in parte non corrispondenti alla realtà od omettendo l'esibizione di documenti veri;
- esibire documenti o dati falsi o alterati ovvero rendere informazioni non corrispondenti al

vero.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione degli adempimenti amministrativi ed attività ispettive***.

La gestione degli adempimenti amministrativi e delle attività ispettive potrebbe presentare profili di rischio in relazione ai **reati contro la PA** nell'ipotesi in cui, ad esempio, nell'ambito di relazioni intercorrenti con la Pubblica Amministrazione per il rilascio di certificazioni, autorizzazioni o permessi, un soggetto apicale o sottoposto della Società induca in errore la Pubblica Amministrazione non semplicemente presentando dichiarazioni o documenti falsi o attestanti circostanze non vere, ma ponendo in essere ulteriori malizie quali, ad esempio, allegazioni di fatture per operazioni inesistenti, al fine di conseguire indebitamente, per sé o per altri, un'autorizzazione o un permesso.

La gestione degli adempimenti amministrativi e delle attività ispettive potrebbe presentare profili di rischio in relazione al **reato di corruzione** per il compimento di un atto contrario ai doveri d'ufficio nell'ipotesi in cui, ad esempio, in caso di verifiche ed ispezioni da parte della PA (Guardia di Finanza, ASL, ATS, ecc.), un soggetto apicale o sottoposto della Società consegni o prometta denaro o altra utilità ad un soggetto pubblico al fine di indurlo a determinare il buon esito della verifica

Ai Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione della succitata attività **è fatto obbligo** di:

- garantire che i rapporti con i soggetti pubblici avvengano nell'assoluto rispetto di leggi, normative vigenti e principi di lealtà, correttezza, chiarezza e trasparenza;
- mantenere elevati standard di integrità in tutte le interazioni con soggetti pubblici, adottando comportamenti trasparenti e responsabili;
- gestire gli adempimenti nei confronti della Pubblica Amministrazione e delle Autorità di Vigilanza, nonché la predisposizione della relativa documentazione nel rispetto delle previsioni di legge esistenti in materia e dei principi generali e delle regole di comportamento richiamate nel Codice Etico e nella presente Parte Speciale;
- provvedere tempestivamente agli adempimenti richiesti nei confronti delle Autorità di Vigilanza con la massima diligenza e professionalità, fornendo informazioni chiare, accurate, complete, fedeli e veritiere ed evitando situazioni di conflitto di interesse;
- assicurare che i rapporti con funzionari della Pubblica Amministrazione siano gestiti esclusivamente da soggetti dotati di idonei poteri, preventivamente identificati ed autorizzati ovvero da soggetti da questi appositamente e formalmente delegati;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da questi esercitate;
- garantire che la documentazione da inviare alla Pubblica Amministrazione e alle Autorità di Vigilanza sia predisposta dalle persone competenti in materia e sottoscritta da soggetti dotati di idonei poteri;
- assicurare che gli adempimenti nei confronti della Pubblica Amministrazione siano effettuati con la massima diligenza e professionalità, in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere, in modo da evitare situazioni di conflitto di

interesse e darne comunque informativa tempestivamente e con le modalità ritenute più idonee;

- individuare i soggetti cui è attribuito il potere di rappresentare la Società presso la Pubblica Amministrazione ovvero di inoltrare comunicazioni di qualsiasi natura alla stessa;
- assicurare che i rapporti con funzionari della Pubblica Amministrazione siano gestiti esclusivamente da soggetti dotati di idonei poteri e che ne sia verificata la validità, completezza e veridicità;
- assicurare la tracciabilità dei rapporti intrattenuti con la Pubblica Amministrazione, nonché dell'evidenza di tutte le richieste ricevute, mediante la predisposizione di report periodici e l'archiviazione di tutte le comunicazioni, sia in entrata che in uscita;
- in caso di visite ispettive, garantire che agli incontri partecipino, ove possibile, almeno due risorse in forza della Società;
- assicurare la piena collaborazione con i Pubblici Ufficiali in occasione di eventuali verifiche ispettive;
- comunicare tempestivamente alla Pubblica Amministrazione ogni variazione significativa che potrebbe avere impatto sull'ottenimento/mantenimento di autorizzazioni, licenze, ecc.;
- provvedere agli obblighi di trasmissione alle Autorità competenti dei dati e documenti previsti dalle norme in vigore ovvero specificamente richiesti dalle suddette Autorità;
- comunicare, senza ritardo, al proprio responsabile gerarchico o al management della Società e contestualmente all'Organismo di Vigilanza, eventuali comportamenti posti in essere da quanti operano con la controparte pubblica, rivolti ad ottenere favori, elargizioni illecite di danaro o altre utilità, anche nei confronti di terzi, nonché qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la Pubblica Amministrazione;
- assicurare che tutta la documentazione da inviare alla Pubblica Amministrazione sia raccolta ed archiviata a cura delle funzioni coinvolte nel processo.

Nell'ambito dei succitati comportamenti **è fatto divieto** di:

- effettuare promesse o indebite elargizioni di denaro o altra utilità a controparti pubbliche o a persone a queste vicine, anche per il tramite di terze parti;
- intrattenere rapporti con Funzionari della Pubblica Amministrazione o pubblici ufficiali o rappresentanti delle Autorità di Vigilanza senza la presenza di almeno un'altra persona, ove possibile, e senza garantire la tracciabilità, come sopra specificato;
- cedere a raccomandazioni o pressioni provenienti da soggetti pubblici o incaricati di pubblico servizio;
- presentare dichiarazioni non veritiere esibendo documenti in tutto o in parte non corrispondenti alla realtà o omettendo l'esibizione di documentazione;
- tenere condotte ingannevoli nei confronti della Pubblica Amministrazione tali da indurre quest'ultima in errori di valutazione;
- tenere comportamenti comunque intesi ad influenzare impropriamente le decisioni dei funzionari che trattano o prendono decisioni per conto della Pubblica Amministrazione;
- presentare dichiarazioni non veritiere alle Autorità di Vigilanza, esibendo documenti in tutto o in parte non corrispondenti alla realtà;

- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza cui è soggetta l'attività aziendale, nonché di trasmettere dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;
- esporre, nelle predette comunicazioni, fatti non rispondenti al vero, ovvero occultare fatti rilevanti;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio dei funzionari pubblici e delle Autorità di Vigilanza, anche in sede di ispezioni.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione dei rapporti con l'Autorità Giudiziaria e dei contenziosi.***

La gestione del contenzioso potrebbe presentare profili di rischio in relazione al **reato di corruzione in atti giudiziari** (sia direttamente che per il tramite di consulenti legali) in occasione dei rapporti con l'Autorità Amministrativa e Giudiziaria nell'ipotesi in cui, ad esempio, la Società proceda al pagamento di compensi illeciti in favore delle controparti al fine di ottenere il buon esito del contenzioso pur in assenza dei presupposti.

La gestione del contenzioso potrebbe presentare profili di rischio in relazione alla configurazione del **reato di corruzione per il compimento di un atto contrario ai doveri del proprio ufficio** qualora, ad esempio, un soggetto sottoposto o apicale della Società ceda denaro ad un Giudice al fine di compensarlo per il favorevole esito di un processo.

La gestione dei rapporti con l'Autorità Giudiziaria potrebbe presentare profili di rischio in relazione al **reato di induzione e non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria** nell'ipotesi in cui, ad esempio, un soggetto apicale o sottoposto della Società imputato o indagato in un procedimento penale venga indotto a rendere false dichiarazioni (o ad astenersi dal renderle) per evitare che la Società sia dichiarata responsabile.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione dei rapporti con l'Autorità Giudiziaria e del contenzioso **è fatto obbligo** di:

- operare nel pieno rispetto di leggi, normative vigenti, *standard* di condotta e principi di lealtà, correttezza, chiarezza e trasparenza;
- garantire che i rapporti con la P.A. siano intrattenuti esclusivamente da parte di soggetti preventivamente identificati e autorizzati dalla Società;
- assicurare che la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità delle informazioni e delle decisioni assunte, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate;
- assicurare che tutta la documentazione e gli atti prodotti nell'ambito della gestione dei contenziosi e rapporti con l'Autorità Giudiziaria sia sottoscritta da soggetti dotati di idonei poteri;
- garantire che il processo di selezione di eventuali professionisti esterni (consulenti, legali, ecc.), sia effettuato da soggetti dotati di idonei poteri valutando la professionalità e onorabilità della controparte;

- assicurarsi che i rapporti con i consulenti legali siano definiti nell'ambito di contratti/lettere d'incarico formalizzati riportanti clausole che specifichino:
  - che la terza parte dichiari di rispettare i principi di cui al D.lgs. 231/2001, nonché di attenersi ai principi del Codice Etico adottato dalla Società;
  - che la terza parte dichiari di aver posto in essere tutti i necessari adempimenti e cautele finalizzati alla prevenzione dei reati sopra indicati, avendo dotato – ove possibile – la propria struttura aziendale di procedure interne e di sistemi del tutto adeguati a tale prevenzione;
  - che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto ai sensi dell'art. 1456 c.c.;
- garantire che tutta la documentazione sia archiviata a cura delle funzioni coinvolte nel processo.

Nell'ambito dei succitati comportamenti **è fatto divieto** di:

- effettuare prestazioni o pagamenti in favore di legali esterni, consulenti, periti o altri soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- adottare comportamenti contrari alle leggi e al Codice Etico in sede di incontri formali ed informali, anche a mezzo di legali esterni e consulenti, per indurre Giudici o Membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio) a favorire indebitamente gli interessi della Società;
- adottare comportamenti contrari alle leggi e al Codice Etico in sede di ispezioni/controlli/verifiche da parte degli Organismi pubblici o periti d'ufficio, per influenzarne il giudizio/parere nell'interesse della Società, anche a mezzo di legali esterni e consulenti.

Nell'espletamento di tutte le operazioni attinenti alla gestione dei rapporti con l'Autorità Giudiziaria, oltre al complesso di regole di cui al presente Modello, ai Destinatari **è fatto obbligo** di conoscere e rispettare quanto di seguito riportato:

- nei rapporti con l'Autorità Giudiziaria, i Destinatari sono tenuti a prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaustivamente rappresentative dei fatti;
- nei rapporti con l'Autorità Giudiziaria i Destinatari e, segnatamente, coloro i quali dovessero risultare indagati o imputati in un procedimento penale anche connesso, inerente all'attività lavorativa prestata nella Società, sono tenuti ad esprimere liberamente le proprie rappresentazioni dei fatti o ad esercitare la facoltà di non rispondere accordata dalla legge;
- tutti i Destinatari devono tempestivamente avvertire, attraverso gli strumenti di comunicazione esistenti all'interno della Società (oppure con qualsivoglia strumento di comunicazione, purché nel rispetto del principio di tracciabilità), l'Organismo di Vigilanza di ogni atto, citazione a testimoniare e procedimento giudiziario (civile, penale o amministrativo) che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente;
- l'Organismo di Vigilanza deve poter ottenere una piena conoscenza del procedimento in corso, anche attraverso la partecipazione ad incontri inerenti i relativi procedimenti o comunque preparatori all'attività difensiva del Destinatario medesimo, anche nelle ipotesi in cui i predetti incontri prevedano la partecipazione di consulenti esterni.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- coartare od indurre, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse della Società, la volontà dei Destinatari di rispondere all'Autorità Giudiziaria o di avvalersi della facoltà di non rispondere;
- accettare, nei rapporti con l'Autorità Giudiziaria, denaro o altre utilità, anche attraverso consulenti della Società medesima;
- promettere o offrire denaro o qualsivoglia utilità ovvero ricorrere all'uso di violenza o minaccia, al fine di indurre un soggetto chiamato a testimoniare a non rilasciare dichiarazioni ovvero a rilasciare dichiarazioni false davanti all'Autorità Giudiziaria, qualora tali dichiarazioni possano essere utilizzate all'interno di un processo penale.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione degli acquisti di beni e servizi (incluse le consulenze).***

La gestione degli acquisti di beni e servizi potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nel caso in cui, ad esempio, un soggetto apicale o sottoposto della Società stipuli contratti fittizi o a valori volutamente non congrui al fine di costituire provviste da utilizzare a fini corruttivi.

La gestione degli acquisti di beni e servizi potrebbe presentare profili di rischio in relazione al **reato di corruzione fra privati** nel caso in cui, ad esempio, un soggetto apicale o sottoposto della Società consegni denaro o altra utilità (es. omaggi, liberalità, assunzioni, ecc.) al responsabile dell'Ufficio Acquisti di una società fornitrice al fine di ottenere la fornitura di un bene o di un servizio ad un prezzo inferiore a quello di mercato ovvero a condizioni particolarmente favorevoli rispetto agli standard normalmente in un uso.

Nella gestione degli acquisti di beni e servizi, i rapporti con i fornitori devono essere formalizzati con accordi che prevedano, tra gli altri:

- che l'impresa dichiari di rispettare i principi di cui al D.lgs. 231/2001, nonché di attenersi ai principi del Codice Etico adottato dalla Società;
- in caso di contratti d'appalto, d'opera o di somministrazione, che l'impresa interessata dichiari di impiegare alle proprie dipendenze esclusivamente personale assunto con regolare contratto di lavoro, nel pieno rispetto della normativa vigente in materia previdenziale, fiscale, assicurativa e sulla disciplina dell'immigrazione;
- che l'impresa interessata dichiari di essere dotata delle autorizzazioni richieste dalla legge per lo svolgimento della propria attività;
- che l'impresa dichiari di aver posto in essere tutti i necessari adempimenti e cautele finalizzati alla prevenzione dei reati sopra indicati, avendo dotato – ove possibile – la propria struttura aziendale di procedure interne e di sistemi del tutto adeguati a tale prevenzione;
- che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto ai sensi dell'art. 1456 c.c..

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella predetta attività **è fatto obbligo** di:

- garantire che i rapporti con fornitori e consulenti avvengano nell'assoluto rispetto di

leggi, normative vigenti e principi di lealtà, correttezza, chiarezza e trasparenza;

- assicurare il rispetto di regole, procedure e linee guida interne in materia di selezione e qualifica dei fornitori;
- prevedere l'attuazione di processi di qualifica dei fornitori che prevedano, tra le altro, la verifica della solidità finanziaria, dell'attendibilità commerciale, tecnico-professionale ed etica degli stessi anche tramite autodichiarazioni prodotte dalla controparte - ad esempio, autodichiarazioni in merito all'eventuale coinvolgimento in procedimenti giudiziari - ed ogni altra informazione utile (anche attraverso attività di *googling*).
- verificare l'esistenza delle specifiche autorizzazioni dei fornitori che svolgono attività per le quali le stesse sono richieste;
- garantire la tracciabilità dell'iter di selezione del fornitore, attraverso la formalizzazione e archiviazione della relativa documentazione di supporto;
- garantire, ove possibile sulla base dell'organizzazione aziendale, un'adeguata segregazione delle funzioni nel processo di gestione dei rapporti con fornitori e consulenti;
- verificare e valutare potenziali conflitti di interesse con il fornitore. In caso di incarichi a persone fisiche verificare l'assenza di incompatibilità legate, ad esempio, allo status di ex dipendente pubblico al fine di garantire la conformità a quanto previsto dal D.lgs. 165/2001, art.53, comma 16-ter (introdotto dalla Legge 190/2012 in materia di "Anticorruzione");
- garantire la tracciabilità dell'iter di selezione del fornitore, attraverso la formalizzazione e archiviazione della relativa documentazione di supporto;
- in caso di servizi in appalto:
  - in caso di utilizzo da parte della terza parte di personale proveniente da paesi extra UE, verificare la validità dei relativi permessi di soggiorno;
  - garantire che la terza parte sia soggetta ad iter di qualificazione che preveda, tra l'altro, la raccolta di documentazione di supporto: DURC, autocertificazione sul possesso dei requisiti di idoneità tecnico-professionale, documentazione richiesta dalle norme in materia di salute e sicurezza sui luoghi di lavoro, DVR, Visura Camerale, autodichiarazione di regolarità contributiva del personale dipendente dell'appaltatore, autodichiarazione di non essere oggetto di provvedimenti di sospensione o interdittivi;
  - assicurarsi che l'ingresso ai locali aziendali sia consentito al solo personale dell'appaltatore specificamente autorizzato, munito di tessera di riconoscimento, che si sia opportunamente registrato ed abbia dichiarato di uniformarsi ai regolamenti interni aziendali;
- garantire che tutti i rapporti con i fornitori o consulenti/professionisti siano formalizzati tramite specifici accordi scritti, sottoscritti da soggetti muniti di idonei poteri;
- verificare la congruità tra quanto ordinato e quanto ricevuto nonché la conformità delle prestazioni effettuate da consulenti e fornitori rispetto a quanto previsto a livello contrattuale;
- assicurare che tutti i pagamenti siano effettuati se adeguatamente supportati da contratto o ordine e solamente a seguito di un iter autorizzativo interno predefinito;

- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatario/ordinanti e controparti effettivamente coinvolte;
- assicurare l'effettivo svolgimento delle attività previste da fornitori e terze parti;
- comunicare, senza ritardo, al proprio responsabile gerarchico e al management della Società e contestualmente all'Organismo di Vigilanza per quanto di sua competenza, eventuali criticità emerse nella gestione delle attività di acquisto di beni e servizi.

Nell'ambito dei predetti comportamenti **è fatto divieto** di:

- effettuare pagamenti su conti correnti cifrati o non intestati al fornitore/consulente o diversi da quelli previsti dal contratto;
- effettuare pagamenti in paesi diversi da quello di residenza del fornitore/consulente;
- effettuare pagamenti non adeguatamente documentati;
- autorizzare pagamenti legati ad operazioni inesistenti o non effettuate dal consulente/fornitore;
- creare fondi a fronte di pagamenti non giustificati (in tutto o in parte);
- impegnare la Società con ordini/contratti verbali;
- effettuare prestazioni in favore di consulenti che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e riconoscere loro compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- effettuare qualsiasi operazione commerciale o finanziaria, sia in via diretta che per interposta persona, con soggetti (persone fisiche o giuridiche) i cui nominativi siano contenuti nelle Liste disponibili presso la Banca d'Italia, o da soggetti da questi ultimi controllati, quando tale rapporto di controllo sia noto;
- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati da rappresentanti della Pubblica Amministrazione come condizione per lo svolgimento di successive attività.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alle seguenti attività:

- ***Selezione e gestione del personale e del sistema di incentivazione;***
- ***Gestione delle note spese.***

L'attività di selezione e gestione del personale potrebbe presentare profili di rischio in relazione al **reato di corruzione** nell'ipotesi in cui, ad esempio, sia scelto - in assenza dei requisiti - un candidato "vicino" o indicato da un pubblico ufficiale al fine di ottenere un indebito vantaggio per la Società.

La gestione del sistema di incentivazione potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, la Società, tramite la gestione del sistema di incentivazione, eroghi ad una risorsa premi/incentivi in denaro volutamente non proporzionati al proprio ruolo/competenze, al fine di dotare il dipendente di una provvista da utilizzare per azioni corruttive.

La gestione delle note spese potrebbe presentare profili di rischio in relazione ai **reati di corruzione**, nell'ipotesi in cui, ad esempio, un soggetto sottoposto o apicale della Società, al

fine di dotare i dipendenti di provviste da utilizzare a fini corruttivi, rimborsi spese fittizie o spese non rientranti nella normale attività del dipendente.

Con riferimento alle attività sopra previste, di seguito si indicano i principi specifici di comportamento.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella gestione delle predette attività **è fatto obbligo** di:

- operare nel pieno rispetto di leggi, normative vigenti, Codice Etico e principi di lealtà, correttezza, chiarezza e trasparenza;
- assicurare che l'assunzione sia approvata secondo l'iter approvativo interno;
- garantire che i processi sopra individuati avvengano sempre nel rispetto di quanto disciplinato dalle regole interne;
- effettuare attività di selezione atte a garantire che la scelta dei candidati sia effettuata sulla base di considerazioni oggettive delle caratteristiche professionali e personali necessarie all'esecuzione del lavoro da svolgere evitando favoritismi di ogni sorta;
- operare nel rispetto del criterio di meritocrazia e delle pari opportunità, senza nessuna discriminazione basata sul sesso, l'origine razziale ed etnica, la nazionalità, l'età, le opinioni politiche, le credenze religiose, lo stato di salute, l'orientamento sessuale, le condizioni economico-sociali, in relazione alle reali esigenze della Società;
- garantire la segregazione del processo di selezione assicurando, altresì, la tracciabilità del processo di valutazione del candidato tramite compilazione e archiviazione di una scheda di valutazione;
- assumere personale solo ed esclusivamente con regolare contratto di lavoro e con retribuzione coerente con il Contratto Collettivo applicato;
- assicurare che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti assegnati ed approvata da soggetti dotati di idonei poteri;
- garantire che sia effettuata la verifica dell'esistenza di possibili conflitti di interessi e dell'eventuale *status* di ex dipendente pubblico del candidato, al fine di garantire la conformità a quanto previsto dal D.lgs.165/2001, art.53, comma 16-*ter* (introdotto dalla Legge 190/2012 in materia di "Anticorruzione");
- per il personale proveniente da Paesi Extra-UE, verificare la validità del permesso di soggiorno ed il monitoraggio dello stesso nel corso della durata del rapporto di lavoro;
- curare che siano assicurate, all'interno della Società, condizioni di lavoro rispettose della dignità personale, delle pari opportunità ed un ambiente di lavoro adeguato, nel rispetto della normativa contrattuale collettiva del settore e della normativa previdenziale, fiscale ed assicurativa;
- verificare che gli orari di lavoro siano applicati nel rispetto della normativa vigente;
- assicurare che al momento dell'assunzione al dipendente sia consegnata copia del Codice Etico, del presente Modello e di tutta la documentazione relativa all'assunzione e che questi si impegni formalmente al pieno rispetto dei principi in essi contenuti;
- garantire un adeguato processo formativo al neo-assunto che preveda, tra le altre, un'adeguata informativa in merito al Modello ed al Codice Etico adottato dalla Società;

- assicurare che siano organizzate specifiche sessioni formative a favore di tutto il personale dipendente;
- assicurare che, per il personale infermieristico, siano previsti *training* specifici sia tramite lezioni frontali che tramite attività di affiancamento a personale sul campo;
- ove le attività siano svolte con il supporto di terze parti, garantire che il processo di selezione delle stesse, avvenga sempre nel rispetto di quanto disciplinato nella sezione "Gestione degli acquisti di beni e servizi (incluse le consulenze)" della presente Parte Speciale e venga effettuato valutando la professionalità e onorabilità della controparte;
- garantire che la contrattualistica sia sottoscritta da soggetti dotati di idonei poteri;
- predisporre le note spese nel rispetto di quanto previsto dalle regole e procedure interne, utilizzando gli strumenti aziendali a disposizione;
- garantire che il rimborso delle note spese avvenga solo a seguito di approvazione delle stesse a cura di soggetti dotati di idonei poteri, sulla base di un processo segregato, e solo in presenza di regolari giustificativi;
- verificare che le spese sostenute siano inerenti lo svolgimento dell'attività lavorativa ed adeguatamente documentate tramite l'allegazione di giustificativi fiscalmente validi;
- assicurare che il rimborso delle spese avvenga solo in presenza di regolari giustificativi;
- garantire, in caso di spese anomale o non supportate da opportuno giustificativo, che le stesse non siano rimborsate;
- assicurare la completa archiviazione della documentazione relativa alla gestione del personale e delle note spese a cura delle funzioni coinvolte nei succitati processi;
- comunicare, senza ritardo, al proprio responsabile gerarchico o al management della Società e contestualmente all'Organismo di Vigilanza eventuali comportamenti rivolti ad ottenere un vantaggio illecito per la Società.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- operare secondo logiche di favoritismo;
- tollerare forme di lavoro irregolare o minorile o di sfruttamento della manodopera;
- assumere personale, anche per contratti temporanei, senza il rispetto delle normative vigenti (ad esempio in termini di contributi previdenziali ed assistenziali, permessi di soggiorno, ecc.);
- promettere assunzioni/avanzamenti di carriera a risorse vicine o gradite a funzionari pubblici o controparti private (ad esempio competitors, fornitori, ecc.) quando questo non sia conforme alle reali esigenze dell'azienda e non rispetti il principio della meritocrazia con il fine di produrre un vantaggio illecito per la Società;
- assumere o promettere l'assunzione ad impiegati della Pubblica Amministrazione (o loro parenti, affini, amici, ecc.) che abbiano partecipato a processi autorizzativi della Pubblica Amministrazione o ad atti ispettivi, nei confronti della Società;
- effettuare rimborsi spese che:
  - non siano stati preventivamente autorizzati;
  - non trovino giustificazione in relazione al tipo di attività svolta;
  - non siano supportati da giustificativi fiscalmente validi o non siano esposti in nota spese.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione dei rapporti* Intercompany*;***
- ***Gestione dei flussi finanziari.***

La gestione dei rapporti *Intercompany* potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, la Società utilizzi le risorse finanziarie in operazioni con società del Gruppo al fine di creare provviste da utilizzare a fini corruttivi.

La gestione dei flussi finanziari ed in particolare la gestione poco trasparente delle risorse finanziarie potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, la Società, anche per il tramite di rapporti con soggetti terzi, consenta l'accantonamento di fondi da utilizzare a fini corruttivi.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nelle predette attività **è fatto obbligo** di:

- autorizzare alla gestione ed alla movimentazione dei flussi finanziari solo soggetti preventivamente identificati e dotati di necessari poteri/procure;
- prevedere limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative;
- assicurare il rispetto delle regole e delle istruzioni operative interne in materia di gestione dei flussi finanziari;
- effettuare i pagamenti a fronte di fatture registrate corredate dai relativi ordini e comunque approvate dalle funzioni competenti che ne attestano l'avvenuta prestazione, secondo i termini e le modalità pattuite, e conseguentemente autorizzano il pagamento;
- assicurare che le operazioni che comportano l'utilizzo o l'impiego di risorse economiche o finanziarie abbiano una causale espressa, siano motivate dal soggetto richiedente e siano documentate e opportunamente registrate in conformità ai principi di correttezza professionale e contabile;
- assicurare che tutte le disposizioni sui conti correnti bancari intestati alla Società, nonché i pagamenti con modalità differenti (ad es. carte di credito aziendali), siano adeguatamente documentate ed autorizzate secondo il sistema di deleghe in vigore;
- effettuare le movimentazioni di flussi finanziari con strumenti che ne garantiscano la tracciabilità;
- garantire la periodica riconciliazione dei conti correnti bancari;
- per la gestione dei flussi in entrata e in uscita, utilizzare esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea o enti creditizi/finanziari situati in uno Stato extracomunitario che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- eseguire un controllo di coerenza tra il soggetto cui è intestata la fattura e l'intestatario del servizio/prodotto;
- garantire che gli incassi e i pagamenti della Società, nonché i flussi di denaro siano sempre tracciabili e provabili documentalmente;

- garantire, compatibilmente con la struttura organizzativa esistente, un'adeguata segregazione tra i soggetti autorizzati a caricare le distinte di pagamento, i soggetti approvatori e coloro che gestiscono i dati sensibili all'interno delle anagrafiche fornitori;
- in caso di utilizzo di denaro contante rispettare le regole ed i limiti di utilizzo del contante di cui alla normativa vigente;
- in caso di utilizzo di carte di credito aziendali assicurare il rispetto delle regole adottate dalla Società nonché le tipologie di spese ammesse;
- assicurare la presenza dei giustificativi relativi alle spese effettuate con carte di credito aziendali;
- garantire la corretta e completa archiviazione della documentazione a cura delle funzioni coinvolte nel processo.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella gestione dei rapporti *Intercompany* **è altresì fatto obbligo** di:

- garantire che i rapporti *Intercompany* siano regolati tramite specifici contratti disciplinanti, tra gli altri:
  - il dettaglio delle attività oggetto di contratto ed i servizi erogati;
  - i ruoli e le responsabilità delle parti;
  - i compensi pattuiti ed i relativi parametri per la determinazione dei corrispettivi;
- assicurarsi che i contratti stipulati con Società del Gruppo siano sottoscritti da soggetti dotati di idonei poteri;
- garantire la tracciabilità di tutte le operazioni con le Società del Gruppo mediante l'archiviazione di tutta la documentazione rilevante;
- verificare l'effettivo svolgimento delle attività previste da parte delle Società del Gruppo;

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- effettuare pagamenti in contanti per importi superiori ai limiti normativi o con mezzi di pagamento non tracciabili;
- effettuare pagamenti su conti correnti cifrati o conti correnti non intestati al fornitore;
- effettuare pagamenti su conti correnti diversi da quelli previsti contrattualmente;
- effettuare pagamenti non adeguatamente documentati;
- procedere al pagamento di fatture *intercompany* relative ad operazioni inesistenti in tutto o in parte;
- creare fondi a fronte di pagamenti non giustificati (in tutto o in parte), anche per il tramite di rapporti con società facenti parte del Gruppo;
- ricevere pagamenti da soggetti che non abbiano nessun rapporto commerciale/contrattuale con la Società;
- effettuare trasferimenti di denaro rispetto ai quali non vi sia piena coincidenza tra i destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nelle transazioni;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione dei rapporti con Operatori Sanitari ed Organizzazioni Sanitarie.***

La gestione dei rapporti con Operatori Sanitari ed Organizzazioni Sanitarie potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, un soggetto sottoposto o apicale della Società stipuli contratti fittizi o a valori volutamente non congrui con Operatori Sanitari pubblici o privati ed Organizzazioni Sanitarie, anche per il tramite di agenzie esterne, al fine di ottenere, in cambio, un vantaggio illecito per la Società.

La gestione dei rapporti con Operatori Sanitari potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, un soggetto sottoposto o apicale della Società stipuli contratti fittizi o a valori volutamente non congrui con consulenti (Operatori Sanitari pubblici o privati), anche per il tramite di agenzie esterne incaricate dell'organizzazione di *advisory board*, allo scopo di costruire provviste da utilizzare ai fini corruttivi.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella predetta attività **è fatto obbligo** di:

- garantire che i rapporti con gli Operatori Sanitari e le Organizzazioni Sanitarie avvengano nell'assoluto rispetto di leggi, normative vigenti e principi di lealtà, correttezza, chiarezza e trasparenza, mantenendo elevati standard di integrità;
- assicurare che i compensi riconosciuti agli operatori sanitari siano determinati sulla base dell'equo valore di mercato della prestazione;
- garantire che i consulenti operatori sanitari siano selezionati in base ai requisiti di professionalità, indipendenza e competenza;
- garantire che la selezione sia effettuata sulla base della verifica del possesso delle competenze necessarie allo svolgimento dell'incarico (analisi e raccolta del *curriculum vitae* del consulente e di ogni altra informazione/documentazione utile);
- prima di procedere all'assegnazione di un incarico di consulenza ad un operatore sanitario, valutare l'assenza di potenziali conflitti di interesse o incompatibilità (legati a normativa nazionale e regionale, regolamenti e codici di comportamento degli Enti di appartenenza, ruoli ed attività svolte dal consulente quali, ad esempio, l'appartenenza a commissioni aggiudicatrici nell'ambito di processi di gara, ecc.);
- prevedere che tutti gli incarichi di consulenza siano formalizzati tramite specifici contratti/lettere d'incarico, sottoscritti a cura di soggetti dotati di idonei poteri;
- garantire che l'incarico sia conferito prima che l'attività sia svolta e la formalizzazione dell'incarico preveda l'indicazione del compenso pattuito, del contenuto della prestazione nonché l'impegno previsto per ciascuna attività in termini di ore o giornate;
- garantire che i pagamenti dei compensi pattuiti in sede di contratto quadro siano vincolati all'effettiva esecuzione delle attività previste;
- garantire la tracciabilità delle attività svolte dai consulenti attraverso l'archiviazione della documentazione rilevante
- procedere al pagamento dei compensi all'operatore sanitario solo a fronte di una fattura ragionevolmente dettagliata che corrisponda alla descrizione contrattuale dei servizi resi nonché a seguito di verifica dell'effettivo svolgimento dell'incarico

consulenziale;

- in caso di utilizzo di terze parti nell'ambito di organizzazione di consulenze ovvero Advisory Board, assicurare che siano qualificate e selezionate nel rispetto di quanto disciplinato nella sezione "Gestione degli acquisti di beni e servizi" della presente Parte Speciale e che i rapporti con le stesse siano disciplinati tramite specifici contratti riportanti clausole che specifichino:
  - che la terza parte dichiari di rispettare i principi di cui al D.lgs. 231/2001, nonché di attenersi ai principi del Codice Etico adottato dalla Società;
  - che la terza parte dichiari di aver posto in essere tutti i necessari adempimenti e cautele finalizzati alla prevenzione dei reati sopra indicati, avendo dotato – ove possibile – la propria struttura aziendale di procedure interne e di sistemi del tutto adeguati a tale prevenzione;
  - che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto ai sensi dell'art. 1456 c.c.;
- comunicare, senza ritardo, al management aziendale e contestualmente all'Organismo di Vigilanza per quanto di sua competenza, eventuali criticità emerse nello svolgimento di incarichi di consulenza.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- effettuare pagamenti in contanti, su conti correnti cifrati o non intestati al consulente o diversi da quelli previsti dal contratto;
- effettuare pagamenti in paesi diversi da quello di residenza del consulente;
- effettuare pagamenti non adeguatamente documentati;
- creare fondi a fronte di pagamenti non giustificati (in tutto o in parte);
- organizzare o effettuare, nell'ambito delle iniziative, attività ludico, sociali, ricreative o procedere al sostenimento di spese di ospitalità in favore di eventuali accompagnatori che eccedano i limiti previsti dalle normative, dai codici di categoria e dalle procedure aziendali.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione delle attività di comunicazione e sponsorizzazione.***

La gestione delle attività di comunicazione e sponsorizzazione potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, la Società offra o prometta denaro od altra utilità ad un soggetto pubblico o privato, in occasione delle attività di comunicazione e informazione, al fine di ottenere, in cambio, un vantaggio illecito per la Società.

La gestione delle attività di comunicazione e sponsorizzazione potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, la Società sponsorizzi eventi tramite soggetti terzi riconoscendo a questi compensi non congrui al fine di dotarli di provviste da utilizzare a fini corruttivi nei confronti di controparti pubbliche o private.

La gestione delle attività di comunicazione e sponsorizzazione potrebbe presentare profili di rischio in relazione al **reato di traffico di influenze illecite** nell'ipotesi in cui, ad esempio, la Società, nell'ambito delle attività di sponsorizzazione, accetti di avvalersi di agenzie esterne che, nella gestione delle attività organizzative ad esse demandate, intendano sfruttare

relazioni con pubblici ufficiali al fine di far ottenere indebiti vantaggi, e vengano pertanto remunerate a fronte di tale mediazione illecita.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella predetta attività **è fatto obbligo** di:

- assicurare che la gestione delle sponsorizzazioni e la partecipazione ad eventi avvenga nell'assoluto rispetto di leggi, normative vigenti, e principi di lealtà, correttezza, chiarezza e trasparenza;
- procedere alla sottoscrizione di specifici contratti di sponsorizzazione da parte dei soggetti dotati di idonei poteri;
- garantire che la partecipazione e/o organizzazione di eventi congressuali siano esclusivamente motivate e connesse all'attività aziendale e siano, oltre che mirate ad attività lecite ed etiche, anche autorizzate, giustificate e documentate;
- garantire che ogni attività relativa all'organizzazione e/o partecipazione ad eventi congressuali e le eventuali relative comunicazioni ad Enti Pubblici avvenga in accordo con le disposizioni normative applicabili;
- procedere alla raccolta ed all'archiviazione di tutta documentazione relativa al processo di sponsorizzazione;
- assicurare il rispetto delle limitazioni stabilite della normativa, regolamenti e Codici di Comportamento con riferimento all'invito ed il sostenimento di eventuali spese sostenute in favore di Operatori Sanitari invitati alle manifestazioni in qualità di discenti;
- assicurare un corretto uso delle opere d'ingegno nell'ambito della gestione di tutte le attività finalizzate alle attività di comunicazione e sponsorizzazione.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- procedere alla sottoscrizione di contratti di sponsorizzazione a valori volutamente non congrui al fine di fornire un'indebita utilità ad una controparte pubblica o privata;
- procedere all'organizzazione o sponsorizzazione di un evento o di un congresso che non sia conforme alla normativa di riferimento;
- organizzare o contribuire ad iniziative di tipo sociale, culturale, turistiche, ludiche o cene di gala nell'ambito di manifestazioni congressuali;
- effettuare pagamenti in contanti, su conti correnti cifrati o intestati a soggetti diversi da quelli previsti contrattualmente;
- effettuare pagamenti non adeguatamente documentati o per prestazioni non eseguite (in tutto o in parte).

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione degli omaggi.***

La gestione degli omaggi potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, un soggetto apicale o sottoposto della Società concede omaggi di valore significativo a controparti pubbliche o private, al fine di compiere azioni corruttive e ottenere benefici illeciti.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella predetta attività **è fatto obbligo** di:

- garantire che gli omaggi siano di valore ragionevole, legati a contesti istituzionali e ad uno scopo commerciale predefinito.
- garantire che il valore, la natura e lo scopo dell'omaggio, sia considerato eticamente corretto, ovvero tale da non compromettere l'immagine della Società;
- garantire che il valore degli omaggi destinati alla Pubblica Amministrazione rispettino i limiti indicati dal D.P.R. 16 aprile 2013, n. 62 e dai Codici di Comportamento adottati dalle singole ASL;
- assicurare che gli omaggi siano stati debitamente autorizzati;
- garantire la tracciabilità del processo decisionale e di spesa.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- promettere o effettuare omaggi a pubblici funzionari italiani o stranieri per finalità diverse da quelle istituzionali e di servizio;
- offrire o promettere omaggi al di fuori di quanto previsto dalla prassi aziendale ed eccedenti le normali pratiche di cortesia;
- accordare vantaggi di qualsiasi natura in favore di rappresentanti della Pubblica Amministrazione italiana o straniera (a titolo esemplificativo: assunzioni, conferimenti di incarichi di natura professionale, commerciale o tecnica a persone particolarmente vicine alla Pubblica Amministrazione) che possano determinare le stesse conseguenze previste al precedente punto.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione degli studi clinici.***

La gestione degli studi clinici potrebbe presentare profili di rischio in relazione ai **reati di corruzione** nell'ipotesi in cui, ad esempio, la Società eroghi un contributo ad uno sperimentatore indipendente nell'ambito di uno studio spontaneo che non viene in tutto o in parte eseguito, al fine di ottenere un vantaggio illecito.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella predetta attività **è fatto obbligo** di:

- sostenere esclusivamente studi clinici i cui contenuti siano attinenti all'ambito di interesse della Società;
- assicurare che i rapporti con operatori sanitari, organizzazioni sanitarie e centri sperimentatori, nell'ambito di gestione degli studi clinici avvengano nel pieno rispetto di leggi, normative vigenti e principi di lealtà, correttezza, chiarezza e trasparenza;
- garantire un adeguato processo di valutazione, scientifica ed economica, della sperimentazione clinica;
- mantenere elevati standard di integrità in tutte le interazioni con i soggetti pubblici, adottando comportamenti trasparenti e responsabili;
- garantire il rispetto delle normative, regolamenti e dei Codici di Comportamento degli Enti di appartenenza degli operatori sanitari coinvolti nella realizzazione di studi clinici;
- corrispondere alle strutture sanitarie coinvolte nello studio compensi ragionevoli in linea con il valore di mercato per analoghe prestazioni medico-sanitarie;
- formalizzare i rapporti con i centri sperimentatori ed eventuali ulteriori terze parti

coinvolte nella gestione di studi clinici tramite appositi contratti scritti contenti clausole che specifichino:

  - che la terza parte dichiari di rispettare i principi di cui al D.lgs. 231/2001, nonché di attenersi ai principi del Codice Etico della Società;
  - che la terza parte dichiari di aver posto in essere tutti i necessari adempimenti e cautele finalizzati alla prevenzione dei reati sopra indicati, avendo dotato – ove possibile – la propria struttura aziendale di procedure interne e di sistemi del tutto adeguati a tale prevenzione;
  - che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto ai sensi dell'art. 1456 c.c.;

- assicurare che la sottoscrizione dei contratti sia effettuata a cura di soggetti dotati di idonei poteri;
- comunicare, senza ritardo, al management aziendale e contestualmente all'Organismo di Vigilanza, eventuali comportamenti posti in essere da quanti operano con la controparte pubblica, rivolti ad ottenere favori, elargizioni illecite di danaro o altre utilità, anche nei confronti di terzi, nonché qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la Pubblica Amministrazione.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- effettuare promesse o indebite elargizioni di denaro o altra utilità a controparti pubbliche o a persone a queste vicine, anche per il tramite di terze parti;
- presentare dichiarazioni non veritiere esibendo documenti in tutto o in parte non corrispondenti alla realtà o omettendo l'esibizione di documenti veri;
- effettuare pagamenti su conti correnti cifrati o non intestati alle terze parti (Centri Sperimentatori, ecc.) coinvolte nella gestione degli studi clinici;
- effettuare pagamenti su conti correnti diversi da quelli previsti contrattualmente;
- effettuare pagamenti non adeguatamente documentati;
- creare fondi a fronte di pagamenti non giustificati (in tutto o in parte).

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Destinatari del presente Modello che, nello svolgimento della propria attività, si trovino a dover gestire attività rilevanti ai sensi degli artt. 24, 25 e 25-*ter* (come sopra specificato) e 25-decies del D.lgs. 231/2001, provvedono a comunicare tempestivamente all'Organismo di Vigilanza, in forma scritta, qualsiasi informazione concernente deroghe o violazioni dei principi di controllo e comportamento previsti al presente capitolo.

Inoltre, a titolo esemplificativo, i Destinatari sono tenuti a trasmettere all'Organismo:

- i provvedimenti o le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità dai quali si evinca lo svolgimento di attività di indagine per i reati rilevanti ai fini del Decreto, avviate anche nei confronti di ignoti;
- le richieste di assistenza legale in caso di avvio di procedimento giudiziario a proprio carico per i reati rilevanti ai fini del Decreto;
- le notizie evidenzianti i procedimenti disciplinari svolti e le eventuali sanzioni irrogate, i provvedimenti assunti ovvero i provvedimenti motivati di archiviazione di procedimenti disciplinari a carico del personale aziendale;
- le informazioni rilevanti in ordine ad eventuali violazioni delle regole di cui al Modello.

SANZIONI

In caso di violazione delle disposizioni contenute nella presente Parte Speciale, trovano applicazione le sanzioni disciplinari previste nel Modello di Organizzazione, Gestione e Controllo della Società, conformemente al CCNL applicato o al contratto di volta in volta sottoscritto.

Ogni violazione delle prescrizioni ivi contenute ovvero i comportamenti elusivi delle stesse da parte di soggetti terzi è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole inserite nei relativi contratti.

PARTE SPECIALE B

DELITTI INFORMATICI, TRATTAMENTO ILLECITO DI DATI E REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

FUNZIONE DELLA PARTE SPECIALE B

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i "Destinatari" del presente Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dagli artt. 24-*bis* e 25-*novies* del D.lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di definire:

- i principi di comportamento che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- i flussi informativi all'Organismo di Vigilanza.

FATTISPECIE DI REATO RILEVANTI

Di seguito vengono riportate le fattispecie di reato ritenute rilevanti per Careapt ai sensi degli artt. 24-*bis* e 25-*novies* del Decreto.

B.1 I reati informatici e trattamento illecito di dati (art. 24-bis D.lgs. 231/2001)

Documenti informatici (art. 491-*bis* c.p.)

La norma sanziona le condotte di falso sui documenti informatici pubblici aventi efficacia probatoria estendendo, attraverso un espresso rinvio, l'applicazione delle disposizioni sulla falsità in atti (falso materiale e ideologico) alle ipotesi di falso su documento informatico.

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

Tale ipotesi di reato punisce chiunque si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Nel primo caso si mira dunque a punire colui che abusivamente si introduce in un sistema informatico o telematico protetto. Più precisamente, l'introduzione nel sistema informatico deve realizzarsi mediante un accesso non autorizzato al sistema stesso, intendendosi come tale l'inizio di un'interazione con il software della macchina che supporta il sistema cui abusivamente si accede (cd. accesso logico). La condotta di introduzione si realizza nel momento in cui l'agente oltrepassi abusivamente le barriere di protezione sia dell'hardware che del software. La legge non richiede che l'agente abbia preso conoscenza di tutti o di una parte cospicua dei dati memorizzati nel sistema violato. E' sufficiente, per la consumazione del reato, che abbia superato le barriere di protezione e che abbia iniziato a conoscere i dati in esso contenuti.

Nel caso del mantenimento, invece, si punisce la condotta di colui che permane nel sistema informatico/telematico contro la volontà di chi ha il diritto di escluderlo. Si tratta di casi in cui l'introduzione nel sistema avviene originariamente in modo legittimo, ma diviene poi illecita in un secondo tempo, a causa del superamento dei limiti di permanenza nel sistema.

Per "sistema informatico" deve intendersi qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compiono l'elaborazione automatica di dati.

Per "sistema telematico" si intende un sistema combinato di apparecchiature, idoneo alla trasmissione a distanza di dati e informazioni, attraverso l'impiego di tecnologie dedicate alle comunicazioni.

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

La condotta incriminata consiste alternativamente nel procurarsi, ovvero acquistare in qualsiasi modo la disponibilità (è del tutto irrilevante che il codice di accesso al sistema informatico altrui, oggetto di cessione, sia stato ottenuto illecitamente) riprodurre, ovvero effettuare la copia in uno o più esemplari, diffondere ovvero divulgare, comunicare, ovvero portare a conoscenza materialmente a terzi, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure nel fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza.

La norma prevede un aggravamento di pena nelle ipotesi in cui il fatto sia commesso:

in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica utilità;

da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema.

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

La norma intende preservare il corretto funzionamento delle tecnologie informatiche. Essa sanziona la condotta di chiunque si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altre apparecchiature, dispositivi o programmi informatici, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o a esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, l'alterazione del suo funzionamento.

Il riferimento è, tra l'altro, ai c.d. *virus*, programmi capaci di modificare o cancellare i dati di un sistema informatico.

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

La norma in esame tutela la riservatezza delle comunicazioni informatiche ovvero il diritto all'esclusività della conoscenza del contenuto di queste ultime, sia nei confronti di condotte di indebita captazione, sia di rivelazione di contenuti illecitamente appresi.

Tale fattispecie di reato può configurarsi attraverso due distinte modalità: l'ipotesi in cui un soggetto fraudolentemente intercetti, interrompa o impedisca, con interruzioni provocate da qualsiasi forma di ingresso nel sistema, le comunicazioni intercorrenti tra soggetti terzi per il tramite di sistemi informatici o telematici, oppure l'ipotesi in cui un soggetto diffonda il contenuto di comunicazioni informatiche o telematiche fraudolentemente intercettate tramite un mezzo di comunicazione al pubblico.

Per intercettazione deve intendersi la presa di conoscenza del contenuto di comunicazioni informatiche o telematiche, che deve essere attuata con modalità fraudolente, l'impedimento è la privazione della possibilità di iniziare una comunicazione, l'interruzione consiste creare ostacoli tali da rendere impossibile la prosecuzione della comunicazione già iniziata, mentre rivelazione è qualsiasi forma di divulgazione delle comunicazioni.

Il terzo comma della fattispecie in esame prevede delle circostanze aggravanti per i casi in cui il fatto sia commesso a danni di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da altra impresa esercente servizi pubblici o di pubblica necessità, o

da pubblico ufficiale o incaricato di pubblico servizio con abuso di potere, o con abuso della qualità di operatore di sistema, o da chi esercita la professione di investigatore privato.

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

La norma tutela il bene giuridico della riservatezza delle informazioni o notizie trasmesse per via telematica o elaborate da singoli sistemi informatici.

Questa ipotesi di reato si configura nel caso in cui vengano istallate apparecchiature volte a consentire al soggetto agente o ad altro soggetto di intercettare, interrompere o impedire comunicazioni informatiche o telematiche.

La condotta sanzionata è quella dell'installazione, nel senso che il complesso delle apparecchiature deve essere posto in condizione di poter svolgere le funzioni richieste dalla norma, ovvero "intercettare, impedire o interrompere".

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

La norma punisce chiunque, salvo che il fatto costituisca più grave reato, distrugge, deteriora, cancella, altera o sopprime informazioni dati e programmi informatici.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia, ovvero con abuso della qualità di operatore di sistema.

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

La norma, salvo che il fatto costituisca più grave reato, sanziona la condotta di chiunque ponga in essere atti volti a distruggere, deteriorare, cancellare, alterare o a sopprimere informazioni dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità.

La pena è aumentata qualora dal fatto consegua la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o programmi informatici o se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore di sistema.

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

La fattispecie di cui trattasi risulta integrata laddove sia cagionato il danneggiamento di un sistema informatico o telematico mediante la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o programmi ovvero tramite l'introduzione o la trasmissione di dati, informazioni o programmi.

La distinzione tra il danneggiamento di dati (punito dall'art. 635-*bis* c.p.) e il danneggiamento del sistema è pertanto legata alle conseguenze che la condotta assume: laddove la soppressione o l'alterazione di dati informazioni e programmi renda inservibile, o quantomeno ostacoli gravemente il funzionamento del sistema, ricorrerà la più grave fattispecie del danneggiamento di sistemi informatici o telematici, prevista appunto dall'art. 635-*quater* c.p.

Anche in questo caso il legislatore ha previsto un aggravamento di pena nelle ipotesi in cui il fatto sia commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore di sistema.

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

La norma sanziona la stessa condotta di cui al punto precedente nel caso in cui il fatto è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

La pena è aumentata se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile e se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

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

La norma sanziona il soggetto, che nell'esercizio dei propri servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare un danno, viola gli obblighi di legge per il rilascio di un certificato qualificato.

Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, del D.L. 21 settembre 2019, n.105)

La norma punisce chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2[2] lettera b), o al comma 6[3], lettera a), o delle attività ispettive

[2] Con Decreto del Presidente del Consiglio dei Ministri del 30 luglio 2020, n.131, è stato adottato, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), il Regolamento in materia di sicurezza nazionale cibernetica. Con tale provvedimento, pubblicato nella Gazzetta Ufficiale Serie Generale n. 261 del 21 ottobre 2020 ed entrato in vigore in data 5 novembre 2020, ai sensi dell'art. 1 comma 2 del D.L 105/2019 "*a) sono definiti modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; ai fini dell' individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla Legge 3 agosto 2007, n. 124, si procede sulla base dei seguenti criteri: 1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato; 2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici; 2-bis) l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alla specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall' interruzione, anche parziali, ovvero dall' utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti; b) sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità, che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-bis predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della Legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; entro sei mesi dalla data della comunicazione, prevista dal comma 2-bis, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al comma 2-bis trasmettono tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico; la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico inoltrano gli elenchi di rispettiva pertinenza al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del Decreto-Legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla Legge 31 luglio 2005, n. 155*".

[3] Con Decreto del Presidente del Consiglio dei Ministri del 30 luglio 2020, n.131, è stato adottato, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), il Regolamento in materia di sicurezza nazionale cibernetica. Con tale provvedimento, pubblicato nella Gazzetta Ufficiale Serie Generale n. 261 del 21 ottobre 2020 ed entrato in vigore in data 5 novembre 2020, ai sensi del comma 6 dell'art. 1 del D.L. 105/2019: "*[…]sono disciplinati le procedure, le modalità e i termini con cui: a) i soggetti di cui al comma 2-bis, ovvero le centrali di committenza alle quali essi fanno ricorso ai sensi dell'articolo 1, comma 512, della Legge 28 dicembre 2015, n. 208, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), appartenenti a categorie*

e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni e all'ente, responsabile ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote.

---

individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, […], ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico; la comunicazione comprende anche la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego. Entro quarantacinque giorni dalla ricezione della comunicazione, prorogabili di quindici giorni, una sola volta, in caso di particolare complessità, il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere anche in collaborazione con i soggetti di cui al comma 2-bis, secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In caso di imposizione di condizioni e test di hardware e software, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. I test devono essere conclusi nel termine di sessanta giorni. Decorso il termine di cui al precedente periodo, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In relazione alla specificità, delle forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'interno e del Ministero della difesa, individuati ai sensi del comma 2, lettera b), i predetti Ministeri, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dal presente decreto, possono procedere, con le medesime modalità e i medesimi termini previsti dai periodi precedenti, attraverso la comunicazione ai propri Centri di valutazione accreditati per le attività di cui al presente decreto, ai sensi del comma 7, lettera b), che impiegano le metodologie di verifica e di test definite dal CVCN. Per tali casi i predetti Centri informano il CVCN con le modalità stabilite con il decreto del Presidente del Consiglio dei ministri, di cui al comma 7, lettera b). Non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni, sistemi e servizi ICT per le quali sia indispensabile procedere in sede estera, fermo restando, in entrambi i casi, l'utilizzo di beni, sistemi e servizi ICT conformi ai livelli di sicurezza di cui al comma 3, lettera b), salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati; b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici di cui al comma 2, lettera b), assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, ai Centri di valutazione operanti presso i Ministeri dell'interno e della difesa, di cui alla lettera a) del presente comma, la propria collaborazione per l'effettuazione delle attività di test di cui alla lettera a) del presente comma, sostenendone gli oneri; il CVCN segnala la mancata collaborazione al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati, o alla Presidenza del Consiglio dei ministri, in caso di fornitura destinata a soggetti pubblici ovvero a quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82; sono inoltrate altresì alla Presidenza del Consiglio dei ministri le analoghe segnalazioni dei Centri di valutazione dei Ministeri dell'interno e della difesa, di cui alla lettera a); c) la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-bis, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma, svolgono attività di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera b), dal comma 3, dal presente comma e dal comma 7, lettera b) , impartendo, se necessario, specifiche prescrizioni; ((nello svolgimento delle predette attività di ispezione e verifica l'accesso, se necessario, a dati o metadati personali e amministrativi è effettuato in conformità a quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196;)) per le reti, i sistemi informativi e i servizi informatici di cui al comma 2, lettera b), connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica sono svolte, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché, nei casi in cui siano espressamente previste dalla legge, in tema di prevenzione e di contrasto del crimine informatico, delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza."

B.2 I reati in materia di violazione del diritto d'autore (art. 25-novies D.lgs. 231/2001)

Si tratta di reati previsti dalla L. 633/1941 a tutela del diritto d'autore. Segnatamente:

Protezione penale dei diritti di utilizzazione economica e morale (art. 171, comma 1, lett. a-*bis*] e comma 3 della L. 633/1941)

Tale norma reprime la condotta di chi, 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.

È previsto un aggravio di pena se la condotta è commessa sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Ai sensi del secondo comma, è possibile estinguere il reato pagando, prima dell'apertura del dibattimento o prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena pecuniaria stabilita dal comma primo, oltre alle spese del procedimento.

Tale articolo incrimina il c.d. "*peer-to-peer*[4]", indicando però solamente l'immissione in internet di opere dell'ingegno protette, e non anche le condotte successive di condivisione e diffusione mediante le quali chiunque può accedere alle opere inserite nella rete telematica.

L'oggetto della tutela è rappresentato dalle opere dell'ingegno protette, da intendersi, secondo le definizioni:

- dell'art. 1 della L. 633/1941, secondo cui "Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione. Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore[5]";

[4] Il peer-to-peer è lo scambio di opere protette che avviene nei sistemi di file-sharing, nei quali ciascun utente è sia downloader che uploader poiché automaticamente condivide i file scaricati anche durante la fase di download.

[5] L'art. 2 specifica quali opere sono oggetto della tutela, disponendo che "In particolare sono comprese nella protezione: 1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto se in forma scritta quanto se orale; 2) le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originale; 3) le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti; 4) le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia; 5) i disegni e le opere dell'architettura; 6) le opere dell'arte cinematografica, muta o sonora, sempreché non si tratti di semplice documentazione protetta ai sensi delle norme del capo quinto del titolo secondo; 7) le opere fotografiche e quelle espresse con procedimento analogo a quello della fotografia sempre che non si tratti di semplice fotografia protetta ai sensi delle norme del capo V del titolo II; 8) i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso; 9) le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto; 10) le opere del disegno industriale che presentino di per sé carattere creativo e valore artistico".

- dell'art. 2575 c.c., per il quale "Formano oggetto del diritto di autore[6] le opere dell'ingegno di carattere creativo che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia qualunque ne sia il modo o la forma di espressione".

Tutela penale del software e delle banche dati (art. 171-*bis*, comma 1, L. 633/1941)

La norma in esame prevede due ipotesi di reato:

- al primo comma, viene punita la condotta di chi duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE). È altresì perseguito penalmente il medesimo comportamento se inerente a 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;
- al secondo comma, viene punita la condotta di chi, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati o esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di legge, ovvero distribuisce, vende o concede in locazione una banca di dati.

Tutela penale delle opere audiovisive (art. 171-*ter* L. 633/1941)

Il comma primo della norma in esame punisce una serie di condotte se realizzate per un uso non personale e a fini di lucro; nello specifico sono sanzionate:

- l'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero di ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
- l'abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento, di opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
- fuori dai casi di concorso nella duplicazione o riproduzione, l'introduzione nel territorio dello Stato, la detenzione per la vendita o la distribuzione, la distribuzione, la messa in commercio, la concessione in noleggio o la cessione a qualsiasi titolo, la proiezione in pubblico, la trasmissione a mezzo della televisione con qualsiasi procedimento, la trasmissione a mezzo della radio, il far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui sopra;
- la detenzione per la vendita o la distribuzione, la messa in commercio, la vendita, il noleggio, la cessione a qualsiasi titolo, la proiezione in pubblico, la trasmissione a mezzo della radio o della televisione con qualsiasi procedimento, di videocassette,

[6] Il contenuto del diritto d'autore è definito dall'art. 2577 c.c., che dispone che "L'autore ha il diritto esclusivo di pubblicare l'opera e di utilizzarla economicamente in ogni forma e modo, nei limiti e per gli effetti fissati dalla legge. L'autore, anche dopo la cessione dei diritti previsti dal comma precedente, può rivendicare la paternità dell'opera e può opporsi a qualsiasi deformazione, mutilazione o altra modificazione dell'opera stessa, che possa essere di pregiudizio al suo onore o alla sua reputazione" e dall'art. 12 della L. 633/1941, il quale prevede che l'autore abbia il diritto esclusivo di pubblicare l'opera e di utilizzare economicamente l'opera nei limiti fissati dalla legge.

musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o altro supporto per il quale è prescritta, ai sensi della legge sul diritto d'autore, l'apposizione di contrassegno da parte della SIAE, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

- la ritrasmissione o diffusione con qualsiasi mezzo di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato, in assenza di accordo con il legittimo distributore;
- l'introduzione nel territorio dello Stato, la detenzione per la vendita o la distribuzione, la distribuzione, la vendita, la concessione in noleggio, la cessione a qualsiasi titolo, la promozione commerciale, l'installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;
- la fabbricazione, l'importazione, la distribuzione, la vendita, il noleggio, la cessione a qualsiasi titolo, la pubblicizzazione per la vendita o il noleggio, la detenzione per scopi commerciali di attrezzature, prodotti o componenti ovvero la prestazione di servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di prevenzione ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure;
- l'abusiva rimozione o alterazione delle informazioni elettroniche che identificano l'opera o il materiale protetto, nonché l'autore o qualsiasi altro titolare dei diritti ai sensi della legge sul diritto d'autore, ovvero la distribuzione, l'importazione a fini di distribuzione, la diffusione per radio o per televisione, la comunicazione o la messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le suddette informazioni elettroniche.

Il secondo comma della norma in esame invece punisce:

- l'abusiva riproduzione, duplicazione, trasmissione, diffusione, vendita, messa in commercio, cessione a qualsiasi titolo o importazione di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;
- la comunicazione al pubblico a fini di lucro e in violazione delle disposizioni sul diritto di comunicazione al pubblico dell'opera, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa[7];
- la realizzazione di un comportamento previsto dal comma 1 da parte di chi esercita in forma imprenditoriale attività di riproduzione, distribuzione, vendita, commercializzazione o importazione di opere tutelate dal diritto d'autore e da diritti connessi;
- la promozione o l'organizzazione delle attività illecite di cui al comma primo.

Il terzo comma prevede un'attenuante se il fatto è di particolare tenuità, mentre il comma quarto prevede alcune pene accessorie, ovvero la pubblicazione della sentenza di condanna, l'interdizione da una professione o da un'arte, l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese e la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività

[7] Tale condotta risulta assai simile a quella prevista dall'art. 171, comma 1, lett. a-bis), ma si distingue da quest'ultima in quanto prevede il dolo specifico del fine di lucro e la comunicazione al pubblico in luogo della messa a disposizione dello stesso.

produttiva o commerciale.

Responsabilità penale relativa ai supporti (art. 171-*septies* L. 633/1941)

La norma in analisi prevede l'applicazione della pena comminata per le condotte di cui al comma 1 dell'art. 171-ter anche per:

- i produttori o importatori dei supporti non soggetti al contrassegno SIAE, i quali non comunicano alla medesima entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;
- chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi.

Responsabilità penale relativa a trasmissioni audiovisive ad accesso condizionato (art. 171-*octies* L. 633/1941)

La norma in esame reprime la condotta di chi, a fini fraudolenti, produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

PRINCIPALI AREE A RISCHIO

La principale area a rischio della Società, con riferimento ai delitti informatici e trattamento illecito di dati ed ai reati in materia di violazione del diritto d'autore è riconducibile a:

- *Gestione delle attività di comunicazione e sponsorizzazione;*
- *Gestione della sicurezza informatica.*

I Destinatari sono tenuti ad adeguare il proprio comportamento a quanto esposto nel presente documento.

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari, come definiti nella Parte Generale del presente Modello.

In generale, **è fatto obbligo** di assicurare che la gestione della sicurezza informatica, l'acquisto e l'utilizzo di opere dell'ingegno protette dal diritto d'autore avvengano nell'assoluto rispetto di:

- leggi e normative vigenti;
- principi di lealtà, correttezza e chiarezza;
- Codice Etico.

In generale, **è fatto divieto** di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di cui agli artt. 24-*bis* e 25-*novies* del D.lgs. 231/2001 innanzi richiamate.

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- **Gestione delle attività di comunicazione e sponsorizzazione.**

La gestione delle attività di comunicazione e sponsorizzazione potrebbe presentare profili di rischio potenziale in relazione ai **reati di violazione in materia di diritto d'autore** nell'ipotesi in cui, ad esempio, la Società utilizza materiale informativo, quali pubblicazioni protette, senza provvedere all'acquisto dei relativi diritti.

Per quanto attiene alla gestione delle attività di comunicazione e sponsorizzazione si rimanda ai principi di comportamento di cui alla Parte Speciale A "*Reati contro la Pubblica Amministrazione e il suo patrimonio, reato di corruzione tra privati e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*" del presente Modello di Organizzazione, Gestione e Controllo.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- **Gestione della sicurezza informatica**

La gestione della sicurezza informatica potrebbe presentare profili di rischio in relazione alla configurazione dei **reati informatici**, nell'ipotesi in cui, ad esempio, un soggetto apicale o sottoposto della Società, utilizzi gli strumenti informatici messi a disposizione della Società per commettere uno dei reati richiamati dall'art.24-*ter* del D.lgs. 231/2001.

La gestione della sicurezza informatica potrebbe presentare profili di rischio in relazione alla configurazione dei **reati informatici**, nell'ipotesi in cui, ad esempio un soggetto apicale o sottoposto della Società alteri documenti aventi efficacia probatoria, la gestione degli accessi ai sistemi informativi interni o di concorrenti terzi e la diffusione di virus o programmi illeciti.

La gestione della sicurezza informatica potrebbe presentare profili di rischio in relazione alla configurazione dei **reati in materia di violazione del diritto d'autore** nell'ipotesi in cui, ad esempio, un soggetto apicale o sottoposto della Società, al fine di ottenere risparmi economici, installi software senza averne acquisito le relative licenze.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione della sicurezza informatica **è fatto obbligo**, in via generale, di:

- osservare rigorosamente le norme poste dalla legge in merito alla sicurezza dei sistemi informativi dell'azienda ed al trattamento di qualsivoglia dato personale;
- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino le fattispecie di reato di cui agli artt. 24-*bis* e 25-*novies* del D.lgs. 231/2001.

Ai predetti Destinatari è altresì **fatto obbligo** di:

- operare nel rispetto delle disposizioni disciplinanti la sicurezza dei sistemi IT;
- garantire che i server siano ospitati in locali dedicati e messi in sicurezza e che l'accesso ai suddetti locali sia riservato al solo personale autorizzato;
- astenersi da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati aziendali e altrui;
- garantire che l'accesso logico ai sistemi informativi sia limitato e protetto da strumenti di autenticazione;
- definire i criteri e le modalità per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (es. lunghezza minima della password, regole di complessità, scadenza);
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione;
- garantire che le nuove utenze siano attivate solo previa richiesta predisposta dalla Funzione Marketing & Operations e siano definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- assicurare che i profili amministratori siano gestiti esclusivamente da soggetti dotati di specifici poteri e la loro attività sia adeguatamente tracciata;
- utilizzare esclusivamente software di cui si possiede regolare licenza;
- assicurare che i software siano istallati dai soli soggetti con profilo di amministratore;
- effettuare controlli periodici sull'effettiva attività degli account e, in caso di inattività dell'utenza, procedere al blocco degli stessi;
- promuovere il corretto uso di tutte le opere dell'ingegno;
- ove per la gestione della sicurezza informatica si faccia ricorso a consulenti esterni, garantire che i rapporti con i suddetti siano formalizzati tramite contratti scritti riportanti clausole che specifichino:
    - che la terza parte dichiari di rispettare i principi di cui al D.lgs. 231/2001, nonché di attenersi ai principi del Codice Etico adottato dalla Società;
    - che la terza parte dichiari di aver posto in essere tutti i necessari adempimenti e cautele finalizzati alla prevenzione dei reati sopra indicati, avendo dotato – ove possibile – la propria struttura aziendale di procedure interne e di sistemi del tutto adeguati a tale prevenzione;
    - che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto ai sensi dell'art. 1456 c.c.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- utilizzare le risorse informatiche (es. personal computer fissi o portatili) e di rete assegnate dalla Società per scopi personali ovvero per finalità diverse da quelle lavorative;
- intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;
- alterare documenti elettronici, pubblici o privati, con finalità probatoria;
- accedere, senza averne la autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai sistemi informativi interni che l'accesso ai sistemi informativi di Enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o industriali);
- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza;
- procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, l'alterazione del suo funzionamento (il divieto include la trasmissione di virus con lo scopo di danneggiare i sistemi informativi di Enti concorrenti);
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici (il divieto include l'intrusione non autorizzata nel sistema informativo di società concorrente, con lo scopo di alterare informazioni e dati di quest'ultima);
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui o ostacolarne gravemente il funzionamento;
- distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ostacolarne gravemente il funzionamento;
- installare software/programmi aggiuntivi rispetto a quelli esistenti e/o autorizzati.

I presidi di controllo sopra indicati sono applicati dalla Società anche ai fini della prevenzione dei delitti in materia di violazione del diritto d'autore.

Nell'ambito dei citati comportamenti è, infatti, **fatto divieto** di:

- porre in essere, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse della Società, comportamenti di qualsivoglia natura atti a ledere
- duplicare, importare, distribuire, vendere, concedere in locazione,

diffondere/trasmettere al pubblico, detenere a scopo commerciale - o comunque per trarne profitto - programmi per elaboratori, banche dati, opere a contenuto letterario, musicale, multimediale, cinematografico, artistico per i quali non siano stati assolti gli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi al suo esercizio.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Destinatari del presente Modello che, nello svolgimento della propria attività, si trovino a dover gestire attività rilevanti ai sensi degli artt. 24-*bis* e 25-*novies* del D.lgs. 231/2001, provvedono a comunicare tempestivamente all'Organismo di Vigilanza, in forma scritta, qualsiasi informazione concernente deroghe o violazioni dei principi di controllo e comportamento previsti al presente capitolo.

Inoltre, i Destinatari sono altresì tenuti a trasmettere all'Organismo eventuali diffide, lettere o comunicazioni di terzi che segnalano violazioni del diritto d'autore.

SANZIONI

In caso di violazione delle disposizioni contenute nella presente Parte Speciale, trovano applicazione le sanzioni disciplinari previste nel Modello di Organizzazione, Gestione e Controllo della Società, conformemente al CCNL applicato o al contratto di volta in volta sottoscritto.

Ogni violazione delle prescrizioni ivi contenute ovvero i comportamenti elusivi delle stesse da parte di soggetti terzi è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole inserite nei relativi contratti.

PARTE SPECIALE C

REATI SOCIETARI E REATI TRIBUTARI

FUNZIONE DELLA PARTE SPECIALE C

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i "Destinatari" del presente Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato previste dagli artt. 25-*ter*[8] e 25-*quinquiesdecies* del D.lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di definire:

- i principi di comportamento che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- i flussi informativi all'Organismo di Vigilanza.

FATTISPECIE DI REATO RILEVANTI

Di seguito vengono riportate le fattispecie di reato ritenute rilevanti per Careapt ai sensi degli artt. 25-*ter* e 25-*quinquiesdecies* del Decreto.

C.1 Reati societari (art. 25-ter D.lgs. 231/2001)

False comunicazioni sociali (art. 2621 c.c.)

Le false comunicazioni sono costituite dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazione ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Società in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionando un danno patrimoniale alla società, ai soci o ai creditori. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Fatti di lieve entità (art. 2621-*bis* c.c.)

Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'art. 2621 c.c. sono di lieve entità tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'art. 2621 c.c. riguardano società che non superano i limiti indicati dal secondo comma dell'art. 1 del R.D. 267/1942. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

Impedito controllo (art. 2625 c.c.)

[8] Per quanto attiene ai reati di corruzione tra privati ed istigazione alla corruzione tra privati si rimanda alla Parte Speciale A del presente Modello di Organizzazione, Gestione e Controllo.

Il reato di impedito controllo si verifica nell'ipotesi in cui, attraverso l'occultamento di documenti o altri idonei artifici, si impedisca o semplicemente si ostacoli lo svolgimento delle attività di controllo legalmente attribuite ai soci e ad altri organi sociali[9].

Il reato si considera imputabile alla società unicamente nell'ipotesi in cui l'impedimento, o il semplice ostacolo abbia cagionato un danno ai soci, stante l'esplicito riferimento al solo secondo comma di tale disposizione, contenuto nel D. Lgs. 231/2001.

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

Riguarda la condotta di amministratori i quali, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli riducendo l'integrità ed effettività del capitale sociale a garanzia dei diritti dei creditori e dei terzi.

Illegale ripartizione di utili e riserve (art. 2627 c.c.)

Il reato riguarda la condotta degli amministratori, i quali ripartiscono utili, o acconti sugli utili, che non sono stati effettivamente conseguiti, o che sono destinati per legge a riserva.

La fattispecie potrebbe verificarsi inoltre attraverso la ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite.

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

Il reato è costituito dalla condotta degli amministratori mediante l'acquisto o la sottoscrizione, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della società controllante in modo tale da procurare una lesione all'integrità del capitale sociale e delle riserve non distribuibili per legge.

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

Le operazioni in pregiudizio dei creditori sono costituite dalla condotta degli amministratori i quali, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.

Omessa comunicazione del conflitto di interessi (art. 2629-*bis* c.c.)

Il reato in esame si configura allorché un componente del consiglio di amministrazione o del consiglio di gestione di una società - con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del Testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al D. Lgs. 58/ 1998, ovvero di un soggetto sottoposto a vigilanza ai sensi del Testo unico delle leggi in materia bancaria e creditizia, di cui al D. Lgs. 385/1993, del citato testo unico di cui al D. Lgs. 58/1998, della L. 576/1982, o del D. Lgs. 124/1993 - violando la disciplina in materia di interessi degli amministratori prevista dal codice civile, rechi alla stessa o a terzi un danno.

Più in specifico, la norma rimanda all'art. 2391 c.c., primo comma, che impone ai membri del consiglio di amministrazione di comunicare (agli altri membri del consiglio e ai sindaci) ogni interesse che i medesimi, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata.

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

[9] Così come modificato dall'art. 37, comma 35, lett. a) D.lgs. 39/2010. La fattispecie di impedito controllo alle società di revisione è disciplinata dall'art 29 D.lgs. 39/2010 non espressamente richiamato dal D.lgs. 231/2001.

Il reato riguarda la condotta degli amministratori e dei soci conferenti i quali, anche in parte, formano o aumentano in modo fittizio il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

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

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, che cagioni un danno ai creditori. Soggetti attivi sono i liquidatori e costituisce una modalità di estinzione del reato il risarcimento del danno ai creditori prima del giudizio.

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

Il reato si perfeziona quando chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

È opportuno ricordare che la responsabilità dell'ente è configurabile solo quando la condotta prevista dall'articolo in esame sia realizzata nell'interesse dell'Ente. Ciò rende difficilmente ipotizzabile il reato in questione che, di norma, viene realizzato per favorire interessi di parte e non dell'"ente".

Aggiotaggio (art. 2637 c.c.)

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

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

Il reato si realizza nel caso in cui determinati soggetti (amministratori, direttori generali, sindaci, liquidatori di società o Enti e, in generale, i soggetti sottoposti alle autorità pubbliche di vigilanza ex lege) espongano, in occasione di comunicazioni alle autorità pubbliche di vigilanza, cui sono tenuti in forza di legge, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che erano tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi In tale ipotesi il reato si perfeziona nel caso in cui la condotta criminosa sia specificamente volta ad ostacolare l'attività delle autorità pubbliche di vigilanza.

C.2 Reati tributari (art. 25-quinquiesdecies D.lgs. 231/2001)

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 co. 1 e co. 2 *bis* del D.lgs. 74/2000)

La norma punisce chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi. La pena è diminuita se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila.

Dichiarazione fraudolenta mediante altri artifici (art. 3 del D.lgs. 74/2000)

La fattispecie in esame punisce chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 co. 1 e 2 *bis* del D.lgs. 74/2000)

La norma punisce chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti. La pena è diminuita se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Occultamento o distruzione di documenti contabili (art. 10 del D.lgs. 74/2000)

La fattispecie in esame punisce chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Sottrazione fraudolenta al pagamento di imposte (art. 11 del D.lgs. 74/2000)

La norma punisce chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. La pena è aumentata se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila.

La norma punisce altresì chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. La pena è aumentata se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila.

PRINCIPALI AREE A RISCHIO

Le principali aree a rischio della Società, con riferimento ai reati societari e ai reati tributari, sono riconducibili a:

- *Gestione delle attività commerciali;*
- *Gestione degli adempimenti amministrativi ed attività ispettive;*
- *Selezione e gestione del personale e del sistema incentivante;*
- *Gestione delle note spese;*
- *Gestione dei rapporti con Operatori Sanitari ed Organizzazioni Sanitarie;*
- *Gestione delle attività di comunicazione e sponsorizzazione;*
- *Gestione degli omaggi;*
- *Gestione degli studi clinici;*
- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*
- *Gestione dei rapporti Intercompany;*
- *Predisposizione del bilancio e gestione della fiscalità;*
- *Gestione delle attività assembleari e delle operazioni sul capitale sociale.*

I Destinatari sono tenuti ad adeguare il proprio comportamento a quanto esposto nel presente documento.

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari, come definiti nella Parte Generale del presente Modello.

In generale, **è fatto obbligo** di assicurare che lo svolgimento delle predette attività avvenga nell'assoluto rispetto di:

- leggi e normative vigenti;
- principi di lealtà, correttezza e chiarezza;
- Codice Etico.

In generale, **è fatto divieto** di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di cui agli artt. 25-*ter* e 25-*quinquiesdecies* del D.lgs. 231/2001 innanzi richiamate.

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Predisposizione del bilancio e gestione della fiscalità.***

La predisposizione del bilancio potrebbe presentare profili di rischio in relazione alla configurazione dei **reati societari** nell'ipotesi in cui, ad esempio, la Società fornisca valutazioni delle poste di bilancio e delle riserve non corrispondenti alla reale situazione economica, finanziaria e patrimoniale, in modo da trarre in inganno i soci o il pubblico sulla solidità della Società stessa.

La predisposizione del bilancio potrebbe presentare profili di rischio in relazione alla configurazione dei **reati societari** nell'ipotesi in cui, ad esempio, nell'ambito della gestione della contabilità, la Società modifichi i dati contabili al fine di fornire una falsa rappresentazione della situazione patrimoniale, economica e finanziaria attraverso l'inserimento di voci di bilancio inesistenti o di valori difformi a quelli reali.

La predisposizione del bilancio potrebbe presentare profili di rischio in relazione alla configurazione dei **reati societari** nell'ipotesi in cui, ad esempio, la Società proceda all'approvazione di un bilancio non veritiero anche a causa di una non corretta gestione, registrazione, aggregazione e valutazione dei dati contabili.

La gestione della fiscalità potrebbe presentare profili di rischio in relazione alla configurazione dei **reati societari** nell'ipotesi in cui, ad esempio, la Società utilizzi nella predisposizione della propria dichiarazione dei redditi fatture per operazioni anche in parte inesistenti emesse da soggetti terzi (associazione per delinquere finalizzata alla commissione di reati in materia di imposte).

La gestione della contabilità e predisposizione del bilancio potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** nell'ipotesi in cui, ad esempio, la Società registri in contabilità fatture per operazioni in tutto o in parte inesistenti, da utilizzare in dichiarazione fiscale al fine di evadere le imposte sui redditi o sul valore aggiunto.

La gestione della contabilità e predisposizione del bilancio potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante altri artifici** nell'ipotesi in cui, ad esempio, la Società indichi in bilancio poste simulate supportate da documenti falsi, al fine di poter indicare in dichiarazione elementi passivi fittizi o elementi attivi inferiori a quelli reali ed

evadere le imposte sui redditi o sul valore aggiunto.

La gestione della fiscalità potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** nell'ipotesi in cui, ad esempio, il soggetto attivo utilizzi nella stessa dichiarazione annuale differenti tipologie di elementi passivi fittizi, sulla base, quindi, dell'annotazione tanto di fatture per operazioni inesistenti, che dell'impiego di altri documenti, anch'essi rappresentativi di una falsa realtà contabile.

La gestione della fiscalità potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante altri artifici** nell'ipotesi in cui, ad esempio, la Società al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indichi nelle dichiarazioni elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella suddetta attività **è fatto obbligo** di:

- garantire la più rigorosa trasparenza contabile in qualsiasi momento ed a fronte di qualsiasi circostanza e osservare le regole di chiara, corretta e completa registrazione nell'attività di contabilizzazione dei fatti relativi alla gestione della Società;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge, dei principi contabili applicabili e delle regole interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire una informazione veritiera e corretta sulla situazione economica, patrimoniale, finanziaria e fiscale della Società;
- assicurare il rispetto delle regole di segregazione dei compiti tra il soggetto che ha effettuato l'operazione, chi provvede alla registrazione in contabilità e chi effettua il relativo controllo;
- osservare le regole di chiara, corretta e completa registrazione nell'attività di contabilizzazione dei fatti relativi alla gestione della Società;
- registrare ogni rilevazione contabile che rifletta una transazione societaria, conservandone adeguata documentazione di supporto che permetta di individuare il motivo dell'operazione che ha generato la rilevazione e la relativa autorizzazione;
- assicurare il rispetto degli adempimenti (sia in termini di dichiarativi che di pagamenti) e delle scadenze definite dalla normativa fiscale;
- effettuare tempestivamente e correttamente, in modo veridico e completo, le comunicazioni previste dalla legge, dai regolamenti e dalle norme aziendali nel tempo vigenti;
- garantire il corretto trattamento fiscale delle componenti di reddito, detrazioni e deduzioni secondo quanto previsto dalla normativa fiscale;
- assicurare il rispetto degli adempimenti richiesti dalla normativa in materia di imposte dirette ed indirette;
- assicurare la corretta e completa archiviazione di tutta la documentazione dei processi nel rispetto delle scadenze previste dalla normativa di riferimento;
- assicurare che il calcolo delle imposte, sia dirette che indirette, nonché le relative

dichiarazioni fiscali siano sottoposte a controlli da parte di soggetti competenti prima della loro presentazione;

- assicurare che gli adempimenti fiscali siano eseguiti o supportati da professionisti esterni qualificati;
- assicurare un adeguato processo di qualifica dei consulenti che supportano la Società nella gestione delle suddette attività e garantire che i rapporti con le suddette siano formalizzati tramite contratti scritti riportanti clausole che specifichino:
  - che la terza parte dichiari di rispettare i principi di cui al D.lgs. 231/2001, nonché di attenersi ai principi del Codice Etico;
  - che la terza parte dichiari di aver posto in essere tutti i necessari adempimenti e cautele finalizzati alla prevenzione dei reati sopra indicati, avendo dotato – ove possibile – la propria struttura aziendale di procedure interne e di sistemi del tutto adeguati a tale prevenzione;
  - che la non veridicità delle suddette dichiarazioni potrebbe costituire causa di risoluzione del contratto ai sensi dell'art. 1456 c.c..

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- procedere alla registrazione in contabilità e alla successiva indicazione nelle dichiarazioni fiscali di fatture o altri documenti ricevuti a fronte di prestazioni soggettivamente o oggettivamente inesistenti (in tutto o in parte);
- distruggere o occultare scritture contabili o altra documentazione rilevante al fine di ottenere un vantaggio fiscale;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilancio, relazioni o prospetti o altri documenti contabili, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- predisporre o concorrere a predisporre documenti in tutto o in parte non veritieri per ottenere vantaggi indebiti, ad esempio per giustificare registrazioni contabili finalizzate ad ottenere benefici fiscali non dovuti;
- alterare o distruggere documenti ed informazioni finanziarie e contabili disponibili in rete attraverso accessi non autorizzati o altre azioni idonee allo scopo;
- presentare una dichiarazione mendace indicando elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti;
- porre in essere azioni finalizzate a fornire informazioni fuorvianti con riferimento all'effettiva rappresentazione della Società, non fornendo una corretta rappresentazione della situazione economica, patrimoniale, finanziaria e fiscale della Società;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilancio, relazioni o prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere (pur essendone un soggetto obbligato) la presentazione alle Autorità competenti di una delle dichiarazioni relative alle imposte sui redditi o sul valore

aggiunto.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- ***Gestione delle attività assembleari e delle operazioni sul capitale sociale.***

La gestione delle attività assembleari e delle operazioni sul capitale sociale potrebbe presentare profili di rischio in relazione ai **reati societari** nell'ipotesi in cui, ad esempio gli Amministratori o i Sindaci della Società, attraverso operazioni sul capitale o una gestione impropria delle attività assembleari, pongano in essere azioni a svantaggio dei soci della Società.

La gestione delle attività assembleari e delle operazioni sul capitale sociale potrebbe presentare profili di rischio in relazione ai **reati societari** nell'ipotesi in cui, ad esempio gli Amministratori, i Sindaci o i Soci della Società compiano operazioni illecite che vanno ad intaccare il patrimonio della Società.

La gestione delle attività assembleari e delle operazioni sul capitale sociale potrebbe presentare profili di rischio in relazione ai **reati societari** nell'ipotesi in cui, ad esempio gli amministratori espongano, in occasione di comunicazioni alle autorità pubbliche di vigilanza cui sono tenuti in forza di legge, fatti materiali non rispondenti al vero al fine di ostacolarne l'attività.

La gestione delle attività assembleari e delle operazioni sul capitale sociale potrebbe presentare profili di rischio in relazione ai **reati societari** nell'ipotesi in cui, ad esempio taluno, con atti simulati o fraudolenti, determini la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

La gestione delle attività assembleari e delle operazioni sul capitale sociale potrebbe presentare profili di rischio in relazione al **reato di sottrazione fraudolenta al pagamento di imposte** nell'ipotesi in cui, ad esempio, il rappresentante legale effettui delle operazioni simulate o a valori non congrui, al fine di sottrarre e/o rendere inattaccabili i cespiti patrimoniali, impedendone l'aggressione da parte delle autorità fiscali.

La gestione delle attività assembleari e delle operazioni sul capitale sociale potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante altri artifici** nell'ipotesi in cui, ad esempio, al fine di evadere le imposte sia compiuta una fraudolenta cessione di quote sociali o siano compiute operazioni di svalutazione del valore delle partecipazioni societarie o di altri attivi aziendali.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione delle predette attività **è fatto obbligo** di:

- gestire tutti gli adempimenti societari (convocazioni, tenuta libri sociali, adempimenti amministrativi, ecc.) secondo le modalità e le tempistiche previste dalla legge;
- assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- nelle operazioni di finanza straordinaria (riferite tipicamente all' assunzione di mutui e finanziamenti, sottoscrizione e aumenti di capitale sociale, concessione di garanzie e fideiussioni, concessione di finanziamenti e sottoscrizione di obbligazioni, acquisizioni di rami d'azienda o partecipazioni azionarie, altre operazioni straordinarie quali fusioni, scissioni, conferimenti) assicurare che i soggetti competenti dispongano di un supporto informativo adeguato tale da poter esprimere una decisione consapevole;

- per ogni operazione di finanza straordinaria da deliberare predisporre la documentazione idonea a valutarne la fattibilità e la convenienza strategica e economica, comprendente, ove applicabile:
  - descrizione quali-quantitativa dell'operazione;
  - caratteristiche e soggetti coinvolti nell'operazione;
  - struttura tecnica, principali garanzie e accordi collaterali e copertura finanziaria dell'operazione;
  - modalità di determinazione delle condizioni economiche dell'operazione ed indicazione di eventuali consulenti esterni/intermediari/advisors coinvolti;
  - impatto sulla situazione economica, finanziaria e patrimoniale prospettica;
  - valutazioni circa la congruità e la rispondenza all'interesse della Società dell'operazione da deliberare da parte di soggetti dotati di idonei poteri;
- assicurare l'adeguatezza di tutta la documentazione di supporto per valutare la fattibilità tecnico- operativa e la convenienza economica e finanziaria dell'operazione, anche di carattere non routinario, nonché i rischi fiscali connessi.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve che non possono per legge essere distribuite;
- effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
- procedere in ogni modo a formazione o aumento fittizio del capitale sociale;
- effettuare operazioni, anche con società del Gruppo, al fine di eludere le normative fiscali;
- porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alle seguenti attività:

- ***Gestione delle attività commerciali***

La gestione delle attività commerciali potrebbe presentare profili di rischio in relazione ai **reati tributari** nell'ipotesi in cui, ad esempio, la Società emetta fatture per operazioni in tutto o in parte inesistenti, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.

- ***Gestione degli adempimenti amministrativi ed attività ispettive***

La gestione degli adempimenti amministrativi ed attività ispettive potrebbe presentare profili di rischio in relazione alla configurazione del **reato di ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza**, nell'ipotesi in cui, ad esempio, gli amministratori espongono, in occasione di comunicazioni alle stesse Autorità cui sono tenuti in forza di legge, fatti materiali non rispondenti al vero al fine di ostacolarne l'attività.

- ***Selezione e gestione del personale e del sistema incentivante***

La selezione e gestione del personale e del sistema di incentivazione potrebbe presentare profili di rischio in relazione alla configurazione del **reato di dichiarazione fraudolenta mediante altri artifici**, nell'ipotesi in cui, ad esempio, sia accordato ad un dipendente della Società uno stipendio inferiore rispetto a quello indicato nella certificazione contabilizzata e utilizzata per la deduzione del relativo costo.

- ***Gestione delle note spese***

La gestione delle note spese potrebbe presentare profili di rischio in relazione alla configurazione del **reato di dichiarazione fraudolenta mediante uso di documenti per operazioni inesistenti**, nell'ipotesi in cui, ad esempio, al fine di evadere le imposte, il dipendente proceda all'emissione di note a fronte di spese non sostenute (in tutto o in parte) e, conseguentemente, il rappresentante legale della Società indichi nella dichiarazione fiscale elementi passivi fittizi.

- ***Gestione dei rapporti con Operatori Sanitari ed Organizzazioni Sanitarie***

La gestione dei rapporti con operatori sanitari potrebbe presentare profili di rischio in relazione ai **reati tributari** nell'ipotesi in cui, ad esempio, un soggetto apicale o sottoposto, al fine di ottenere un illecito vantaggio fiscale per la Società, nell'ambito di un rapporto di consulenza con un Operatore Sanitario proceda alla registrazione in contabilità di fatture per servizi in tutto o in parte non svolti dal consulente.

- ***Gestione delle attività di comunicazione e sponsorizzazione***

La gestione delle attività di comunicazione e sponsorizzazione potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** nell'ipotesi in cui, ad esempio, la Società registri in contabilità fatture per operazioni in tutto o in parte inesistenti.

- ***Gestione degli omaggi***

La gestione degli omaggi potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** nell'ipotesi in cui, ad esempio, un soggetto della Società inserisca in contabilità fatture o altri documenti per operazioni inesistenti e conseguentemente indichi nella dichiarazione fiscale elementi passivi fittizi.

- ***Gestione degli studi clinici***

La gestione degli studi clinici potrebbe presentare profili di rischio in relazione ai **reati tributari** nell'ipotesi in cui, ad esempio, la Società, al fine di ottenere un illecito vantaggio fiscale, proceda alla contabilizzazione di elementi passivi relativi ad attività non effettuate (in tutto o in parte) da parte di centri sperimentatori.

- ***Gestione degli acquisti di beni e servizi (incluse le consulenze)***

La gestione degli acquisti di beni e servizi presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante uso di fatture per operazioni inesistenti** nell'ipotesi in cui, ad esempio, un soggetto apicale o sottoposto, al fine di ottenere un vantaggio fiscale illecito per la Società, nell'ambito di un rapporto di fornitura proceda alla registrazione in contabilità di fatture per operazioni in tutto o in parte inesistenti.

- ***Gestione dei rapporti Intercompany***

La gestione dei rapporti *intercompany* potrebbe presentare profili di rischio in relazione al **reato di dichiarazione fraudolenta mediante uso di fatture per operazioni inesistenti** nell'ipotesi in cui, ad esempio, La Società, al fine di evadere le imposte, contabilizzi fatture passive emesse da

società del gruppo relative a servizi non resi (in tutto o in parte).

Per i principi di comportamento specifici in relazione alle sopra citate aree sensibili si rinvia a quanto previsto nella Parte Speciale A "*Reati contro la Pubblica Amministrazione e il suo patrimonio, reato di corruzione tra privati e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*" del presente Modello di Organizzazione, Gestione e Controllo.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Destinatari del presente Modello che, nello svolgimento della propria attività, si trovino a dover gestire attività rilevanti ai sensi degli artt. 25-*ter* e 25-*quinquiesdecies* del D.lgs. 231/2001, provvedono a comunicare tempestivamente all'Organismo di Vigilanza, in forma scritta, qualsiasi informazione concernente deroghe o violazioni dei principi di controllo e comportamento previsti al presente capitolo.

SANZIONI

In caso di violazione delle disposizioni contenute nella presente Parte Speciale, trovano applicazione le sanzioni disciplinari previste nel Modello di Organizzazione, Gestione e Controllo della Società, conformemente al CCNL applicato o al contratto di volta in volta sottoscritto.

Ogni violazione delle prescrizioni ivi contenute ovvero i comportamenti elusivi delle stesse da parte di soggetti terzi è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole inserite nei relativi contratti.

PARTE SPECIALE D

DELITTI DI CRIMINALITA' ORGANIZZATA E REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO

FUNZIONE DELLA PARTE SPECIALE D

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i "Destinatari" del Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato richiamate dagli artt. 24-*ter* e 25-*octies* del D.lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di definire:

- i principi di comportamento che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- i flussi informativi all'Organismo di Vigilanza.

FATTISPECIE DI REATO RILEVANTI

Di seguito vengono riportate le fattispecie di reato ritenute rilevanti per Careapt ai sensi degli artt. 24-*ter* e 25-*octies* del Decreto.

D.1 Delitti di criminalità organizzata (art. 24-ter D.lgs. 231/2001)

Associazione a delinquere (art. 416 c.p.)

Il reato punisce chi promuove, costituisce o organizza associazioni di tre o più persone con il fine di commettere più delitti.

Associazione di tipo mafioso anche straniere (art. 416-*bis*)

Vi incorre chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone.

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

Le disposizioni dell'art. 416-bis c.p. si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

Tutti i delitti se commessi avvalendosi delle condizioni previste dall'art. 416-bis c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91)

D.2 Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies D.lgs. 231/2001)

Ricettazione (art. 648 c.p.)

Il reato di ricettazione punisce chi acquista, riceve, occulta o si intromette nell'acquistare, ricevere o occultare denaro o cose provenienti da un qualsiasi delitto. Tale condotta è finalizzata alla realizzazione di un profitto a favore dell'autore stesso o di un terzo. Perché sussista ricettazione è necessario che l'autore del reato non abbia concorso alla realizzazione

del delitto dal quale provengono il denaro o le cose oggetto di ricettazione.

Riciclaggio (art. 648-*bis* c.p.)

La fattispecie di riciclaggio si configura ogni qualvolta taluno, sostituisce o trasferisce denaro, beni o altre utilità provenienti da un delitto non colposo ovvero compie in relazione ad essi altre operazioni. La condotta perché sia rilevante deve essere tale da ostacolare l'identificazione della provenienza delittuosa del denaro, dei beni o delle altre utilità. Così come per la ricettazione, anche il riciclaggio sussiste fuori dai casi di concorso dal delitto dal quale provengono il denaro, i beni o le altre utilità.

Nella condotta di "sostituzione" rientra ogni attività diretta a incidere sul compendio criminoso separando ogni possibile collegamento con il reato. Le concrete modalità operative possono consistere in operazioni bancarie, finanziarie, commerciali, attraverso le quali si scambiano le utilità economiche di provenienza illecita con altre lecite; ovvero con il cambio di cartamoneta in valute diverse, con speculazioni sui cambi, con l'investimento del danaro in titoli di Stato, azioni ecc.

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

Il reato di impiego di denaro punisce chiunque, fuori dai casi di concorso nel reato e fuori dai casi di ricettazione e riciclaggio sopra richiamati, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

La condotta punibile è descritta con il verbo impiegare, che non ha una precisa valenza tecnica e finisce con l'avere una portata particolarmente ampia, potendosi attagliare a qualunque forma di utilizzazione di denaro, beni o altre utilità provenienti da delitto indipendentemente da qualsiasi obiettivo o risultato utile per l'agente.

Autoriciclaggio (art. 648-*ter*.1 c.p.)

Il reato punisce chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

PRINCIPALI AREE DI RISCHIO

Le principali aree di rischio della Società, con riferimento ai delitti criminalità organizzata e ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché' autoriciclaggio, sono riconducibili a:

- *Gestione delle attività commerciali;*
- *Selezione e gestione del personale e del sistema di incentivazione;*
- *Gestione delle attività di comunicazione e sponsorizzazione;*
- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*
- *Gestione dei rapporti Intercompany;*
- *Gestione dei flussi finanziari;*
- *Predisposizione del bilancio e gestione della fiscalità;*
- *Gestione delle attività assembleari e delle operazioni sul capitale sociale.*

I Destinatari sono tenuti ad adeguare il proprio comportamento a quanto esposto nel presente documento.

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari, come definiti nella Parte Generale del presente Modello.

In generale, **è fatto obbligo** di assicurare che lo svolgimento delle predette attività avvenga nell'assoluto rispetto di:

- leggi e normative vigenti;
- principi di lealtà, correttezza e chiarezza;
- Codice Etico.

In generale, **è fatto divieto** di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di cui agli artt. 24-*ter* e 25-*octies* del D.lgs. 231/2001 innanzi richiamate.

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alle seguenti attività:

- **Gestione delle attività commerciali**

La gestione delle attività commerciali potrebbe presentare profili di rischio in relazione ai **delitti di criminalità organizzata** nell'ipotesi in cui, ad esempio, la Società instauri relazioni con clienti quali soggetti segnalati o vicini ad associazioni criminali allo scopo di ottenere dei benefici dalle attività illecite poste in essere dall'organizzazione stessa.

- **Selezione e gestione del personale e del sistema di incentivazione**

La gestione del personale e del sistema di incentivazione potrebbe presentare profili di rischio in relazione ai **delitti di criminalità organizzata** nell'ipotesi in cui, ad esempio, la Società, al fine di ricevere un vantaggio indebito, proceda alla selezione di un soggetto segnalato o vicino ad un'organizzazione criminale.

- **Gestione delle attività di comunicazione e sponsorizzazione**

La gestione delle attività di comunicazione e sponsorizzazione potrebbe presentare profili di rischio in relazione al reato di **associazione per delinquere** nell'ipotesi in cui, ad esempio, un soggetto sottoposto o apicale della Società, con la complicità di altri soggetti interni o esterni, fornisca denaro o altra utilità indebita ad un operatore sanitario per influenzarlo, illecitamente, a indurre il paziente ad acquistare i servizi offerti dalla Società.

- **Gestione degli acquisti di beni e servizi (incluse le consulenze)**

La gestione degli acquisti di beni e servizi potrebbe presentare profili di rischio potenziale in relazione ai **delitti di criminalità organizzata** nell'ipotesi in cui ad esempio, la Società stipuli contratti fittizi o a valori volutamente non congrui con fornitori vicini ad organizzazioni criminali, al fine di ottenere benefici economici e/o fiscali.

La gestione degli acquisti di beni e servizi potrebbe presentare profili di rischio potenziale in relazione al **reato di ricettazione** nell'ipotesi in cui ad esempio, un soggetto sottoposto o apicale,

al fine di ottenere un indebito vantaggio per la Società, proceda all'acquisto di beni di provenienza illecita.

La gestione degli acquisti di beni e servizi potrebbe presentare profili di rischio potenziale in relazione al **reato di autoriciclaggio** nell'ipotesi in cui ad esempio, nell'ambito della gestione dell'albo fornitori, si permetta l'inserimento di soggetti dediti all'emissione di fatture o altri documenti per operazioni inesistenti al fine di evadere le imposte sui redditi o sul valore aggiunto consentendo così alla Società di costituire provvista di provenienza illecita da impiegare, sostituire, trasferire in attività economiche, finanziarie, imprenditoriali o speculative, in modo da ostacolare concretamente l'identificazione della provenienza delittuosa.

- **Gestione dei rapporti *Intercompany***

La gestione dei rapporti *Intercompany* potrebbe presentare profili di rischio potenziale in relazione ai **reati di ricettazione, riciclaggio e autoriciclaggio** nell'ipotesi in cui, ad esempio la Società utilizzi le risorse finanziarie in operazioni con società del Gruppo, al fine di favorire l'immissione nel circuito legale di denaro di provenienza illecita.

- **Gestione dei flussi finanziari**

La gestione dei flussi finanziari potrebbe presentare profili di rischio potenziale in relazione ai **delitti di criminalità organizzata** nell'ipotesi in cui, ad esempio, la Società eroghi pagamenti non dovuti per prestazioni in tutto o in parte inesistenti a soggetti terzi legati ad associazioni criminose o mafiose al fine di agevolarne l'attività illecita.

La gestione dei flussi finanziari potrebbe presentare profili di rischio potenziale in relazione ai **reati di ricettazione, riciclaggio e autoriciclaggio** nell'ipotesi in cui, ad esempio, la Società utilizzi le risorse finanziarie in operazioni con soggetti terzi, al fine di favorire l'immissione nel circuito legale di denaro di provenienza illecita.

La gestione dei flussi finanziari potrebbe presentare profili di rischio potenziale in relazione al **reato di autoriciclaggio** nell'ipotesi in cui, ad esempio, la Società accantoni provviste finanziarie di provenienza illecita da impiegare, sostituire, trasferire, in attività economiche, finanziarie, imprenditoriali o speculative, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione delle predette attività, oltre a quanto indicato nella Parte Speciale A "*Reati contro la Pubblica Amministrazione e il suo patrimonio, reato di corruzione tra privati e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*" è, altresì, **fatto obbligo** di:

- assicurare che nessun pagamento o incasso sia regolato in contanti;
- per la gestione dei flussi in entrata e in uscita, garantire che siano utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea o enti creditizi/finanziari situati in uno Stato extracomunitario che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- assicurare che gli incassi e i pagamenti della Società nonché i flussi di denaro siano sempre tracciabili e provabili documentalmente.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alle

seguenti attività:

- **Predisposizione del bilancio e gestione della fiscalità**

La predisposizione del bilancio potrebbe presentare profili di rischio potenziale in relazione ai **reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio** nell'ipotesi in cui, ad esempio, la Società indichi poste di bilancio in modo da ostacolare concretamente l'identificazione della provenienza delittuosa di somme di denaro.

La gestione della fiscalità potrebbe presentare profili di rischio potenziale in relazione ai **reati di autoriciclaggio** nell'ipotesi in cui, ad esempio, la Società, indicando nelle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto elementi passivi fittizi, evada dette imposte e impieghi le risorse finanziarie così ottenute nella propria attività.

- **Gestione delle attività assembleari e delle operazioni sul capitale sociale**

La gestione delle attività assembleari e delle operazioni sul capitale sociale potrebbe presentare profili di rischio in relazione ai **reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio** nell'ipotesi in cui, ad esempio, gli Amministratori, il Sindaco o i Soci della Società compiano operazioni mediante l'impiego di denaro proveniente da attività illecite.

Per i principi di comportamento specifici riguardanti la predisposizione del bilancio e la gestione della fiscalità nonché la gestione delle attività assembleari ed operazioni sul capitale si rinvia a quanto previsto nella Parte Speciale C "*Reati Societari e Reati Tributari*" del presente Modello di Organizzazione, Gestione e Controllo.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Destinatari del presente Modello che, nello svolgimento della propria attività, si trovino a dover gestire attività rilevanti ai sensi degli artt. 24-*ter* e 25-*octies* del D.lgs. 231/2001, provvedono a comunicare tempestivamente all'Organismo di Vigilanza, in forma scritta, qualsiasi informazione concernente deroghe o violazioni dei principi di controllo e comportamento previsti al presente capitolo.

SANZIONI

In caso di violazione delle disposizioni contenute nella presente Parte Speciale, trovano applicazione le sanzioni disciplinari previste nel Modello di Organizzazione, Gestione e Controllo della Società, conformemente al CCNL applicato o al contratto di volta in volta sottoscritto.

Ogni violazione delle prescrizioni ivi contenute ovvero i comportamenti elusivi delle stesse da parte di soggetti terzi è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole inserite nei relativi contratti.

PARTE SPECIALE E

DELITTI DI OMICIDIO COLPOSO E LESIONI PERSONALI COLPOSE GRAVI E GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME A TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

FUNZIONE DELLA PARTE SPECIALE E

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i "Destinatari" del Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato richiamate dall'art. 25-*septies* del D.lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di definire:

- i principi di comportamento che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- i flussi informativi all'Organismo di Vigilanza.

FATTISPECIE DI REATO RILEVANTI

Di seguito vengono riportate le fattispecie di reato ritenute rilevanti per Careapt ai sensi dall'art. 25-*septies* del Decreto.

E.1 Delitti di omicidio colposo e lesioni personali colpose gravi e gravissime commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro (art. 25-septies D.lgs. 231/2001)

Omicidio colposo (art. 589 c.p.)

Vi incorre chiunque cagioni per colpa[10] la morte di una persona.

Lesioni personali colpose commesse con violazione delle norme a tutela della salute e sicurezza sul lavoro (art. 590, comma 3, c.p.)

Vi incorre chiunque cagioni ad altri per colpa una lesione personale grave o gravissima.

La lesione personale è grave (art. 583 c.p.):

- se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
- se il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione personale è gravissima (art. 583 c.p.) 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;
- la deformazione, ovvero lo sfregio permanente del viso.

[10] Ovvero per negligenza, imprudenza, imperizia o inosservanza di leggi, regolamenti, ordini o discipline.

PRINCIPALI AREE DI RISCHIO

Le principali aree di rischio della Società, con riferimento ai delitti di omicidio colposo e lesioni personali colpose gravi e gravissime commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro, sono riconducibili a:

- Gestione degli acquisti di beni e servizi (incluse le consulenze);
- *Gestione del sistema di prevenzione e protezione*.

I Destinatari sono tenuti ad adeguare il proprio comportamento a quanto esposto nel presente documento.

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari, come definiti nella Parte Generale del presente Modello.

In generale, **è fatto obbligo** di assicurare che lo svolgimento delle predette attività avvenga nell'assoluto rispetto di:

- leggi e normative vigenti;
- principi di lealtà, correttezza e chiarezza;
- Codice Etico.

In generale, **è fatto divieto** di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di cui all'art. 25-*septies* del D.lgs. 231/2001 innanzi richiamate.

- **Gestione del sistema di prevenzione e protezione**

La gestione del sistema di prevenzione e protezione potrebbe presentare profili di rischio in relazione ai **reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro** nell'ipotesi in cui, ad esempio, la Società, al fine di ottenere vantaggi di tipo economico, non si doti di tutti gli strumenti necessari per far fronte ai rischi identificati in tema di salute e sicurezza sul lavoro.

Sempre con riferimento all' attività sopra prevista, di seguito si indicano i principi specifici di comportamento.

La Società ha adottato un Documento di Valutazione dei Rischi (DVR), ai sensi dell'art. 28 Decreto legislativo 9 aprile 2008, n. 81 (di seguito anche "TU") ed ha predisposto un organigramma della sicurezza che consente di definire i compiti ed i poteri gravanti sui soggetti chiamati ad operare nel sistema della salute e della sicurezza nei luoghi di lavoro.

Il Datore di Lavoro è stato formalmente identificato nella figura del General Manager. È stato nominato il Medico Competente, nonché il Responsabile del Servizio di Prevenzione e Protezione e i Rappresentanti dei Lavoratori per la Sicurezza; inoltre, sono stati identificati gli addetti alla gestione delle emergenze per il primo soccorso e per la prevenzione degli incendi.

In via generale ai Destinatari, come sopra individuati, e a tutti i soggetti aventi compiti di responsabilità nella gestione degli adempimenti previsti dalle norme sulla tutela della salute e della sicurezza sul lavoro, **è fatto obbligo** di operare nel rispetto delle normative applicabili e garantire, ognuno nell'ambito di propria competenza:

- la definizione degli obiettivi per la sicurezza e la salute dei lavoratori e l'identificazione continua dei pericoli;
- un adeguato livello di informazione/formazione dei dipendenti e dei fornitori/appaltatori anche sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società;
- la prevenzione degli infortuni, delle malattie e la gestione delle emergenze;
- l'adeguatezza delle risorse umane - in termini di numero e qualifiche professionali - e materiali, necessarie al raggiungimento degli obiettivi prefissati dalla Società per la sicurezza e la salute dei lavoratori;
- l'applicazione di provvedimenti disciplinari nel caso di violazioni dei principi comportamentali definiti e comunicati dalla Società, in accordo con il Sistema Disciplinare enucleato nel Modello di Organizzazione, gestione e controllo adottato dalla Società ed al quale si rinvia (Parte Generale, Cap. 6).

Costituiscono, a titolo esemplificativo, illecito disciplinare e contravvenzione, le violazioni agli obblighi di cui all'art. 59 comma 1 lett. a) del D.lgs. 81/2008, secondo cui i lavoratori devono:

- preservare la salute e la sicurezza propria e delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle loro azioni ed omissioni, conformemente alla formazione, alle istruzioni e ai mezzi forniti loro dal Datore di Lavoro;
- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro ai fini della protezione collettiva ed individuale;
- segnalare immediatamente al Datore di Lavoro qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza;
- non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro anche tramite consulenti esterni accreditati.

Principi di controllo

I Destinatari coinvolti nella gestione della predetta attività devono garantire, ognuno per le parti di rispettiva competenza, l'esecuzione dei seguenti controlli:

Individuazione dei responsabili, identificazione dei poteri e gestione delle emergenze

- I soggetti nominati dalla Società ai sensi del D.lgs. 81/2008 (RSPP, Addetti al primo soccorso, ecc.) ed i Rappresentanti dei Lavoratori per la Sicurezza devono esercitare, ciascuno nell'ambito delle proprie competenze ed attribuzioni, i compiti di sicurezza specificamente affidati dalla normativa vigente e previsti nel sistema di sicurezza adottato dalla Società;
- i soggetti facenti parte dell'organigramma aziendale della sicurezza, nell'ambito delle proprie competenze, definiscono ruoli, responsabilità e facoltà di coloro che gestiscono, eseguono e verificano attività che hanno influenza sui rischi per la salute e la sicurezza;
- tutti i dipendenti devono avere cura della sicurezza propria e dei soggetti che hanno accesso alle strutture della Società, nonché osservare le misure, le istruzioni e le procedure aziendali in materia di salute e sicurezza.

Definizione degli obiettivi per la sicurezza e la salute dei lavoratori, identificazione e valutazione

continua dei rischi e attività di manutenzione

In particolare, in conformità agli adempimenti prescritti dal D.lgs. 81/2008 e successive modifiche e integrazioni, nonché in coerenza con i ruoli, i compiti e le responsabilità in materia di sicurezza:

- il Datore di Lavoro:
  - designa le figure dell'Organigramma sulla Sicurezza, in base ai requisiti di cui al D.lgs. 81/2008;
  - definisce gli obiettivi e i programmi per il miglioramento continuo delle condizioni di prevenzione e protezione in materia di sicurezza e salute, in collaborazione con il RSPP e il Medico competente;
  - effettua periodicamente, in collaborazione con il RSPP e il Medico Competente, una analisi formalizzata dei rischi esistenti; la valutazione dei rischi presenti in azienda deve essere ripetuta ogni qualvolta dovessero avvenire mutamenti organizzativi e operativi nonché modifiche tecniche.

Formazione ed informazione sulla sicurezza e salute ai dipendenti e lavoratori con contratto di somministrazione lavoro

Il Datore di Lavoro:

- garantisce che sia fornita adeguata formazione ai dipendenti in materia di sicurezza sia in occasione dell'assunzione che del trasferimento ad altre mansioni;
- provvede ad organizzare programmi di formazione/addestramento continui ai lavoratori, compresi quelli che prestano la propria attività con periodicità limitata;
- assicura che siano organizzati ed erogati programmi di formazione specifici ai lavoratori e che gli stessi siano in ogni caso adeguati agli eventuali rischi specifici della mansione cui il lavoratore è in concreto assegnato.

In considerazione della rilevanza delle attività formative in materia, i piani formativi aziendali sono allineati con i requisiti previsti dall'Accordo Stato – Regioni.

Sorveglianza sanitaria

È responsabilità del Datore di Lavoro monitorare, in collaborazione con il RSPP, lo svolgimento della sorveglianza sanitaria da parte del Medico Competente, dotandolo degli adeguati spazi per lo svolgimento dell'attività di propria competenza e per l'archiviazione della documentazione che da tale attività emerga.

È responsabilità del Medico Competente, purché non a scapito degli accertamenti obbligatori previsti a norma di legge, valutare l'adeguatezza ed eventualmente aggiornare il programma di sorveglianza in base alle eventuali sopravvenute esigenze.

Il protocollo sanitario è periodicamente aggiornato in base a nuove prescrizioni legislative, modifiche nelle attività e nei processi, identificazione di nuovi rischi per la salute dei lavoratori.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- porre in essere, collaborare o dare causa alla realizzazione di condotte commissive o omissive tali che, prese individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato considerate;
- porre in essere o concorrere in qualsiasi forma nella realizzazione di comportamenti che, sebbene siano tali da non integrare i reati indicati, possano potenzialmente tradursi in essi o agevolarne la commissione.

***

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alla seguente attività:

- **Gestione degli acquisti di beni e servizi (incluse le consulenze)**

La gestione degli acquisti di beni e servizi (incluse le consulenze) potrebbe presentare profili di rischio in relazione ai **reati in materia di salute e sicurezza sul lavoro** nell'ipotesi in cui, ad esempio, al fine di ottenere un risparmio economico, la Società selezioni fornitori che non rispettano le normative in materia.

Ai Destinatari coinvolti nella gestione dei fornitori, dei contratti d'appalto, d'opera o di somministrazione **è fatto obbligo** di:

- rispettare i principi di comportamento previsti nella Parte Speciale A "*Reati contro la Pubblica Amministrazione ed il suo Patrimonio e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*" di cui al presente Modello di Organizzazione, Gestione e Controllo;
- valutare, nel corso della selezione, la capacità delle imprese appaltatrici o dei lavoratori autonomi di garantire la tutela della salute e della sicurezza sia dei lavoratori impiegati dagli stessi che di quelli della Società;
- verificare l'idoneità tecnico – professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare in appalto o mediante contratto d'opera o di somministrazione, anche – ma non solo - secondo le modalità previste dall'art. 26 comma 1 del D.lgs. 81/2008;
- stipulare accordi scritti riportanti le modalità di gestione e coordinamento dei lavori in appalto;
- elaborare (ove previsto e con la cooperazione dell'appaltatore/subappaltatore), un "Documento Unico di Valutazione dei Rischi da Interferenze" (DUVRI) finalizzato a:
    - cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto del contratto;
    - coordinare gli interventi di prevenzione e protezione dai rischi cui sono esposti i lavoratori, informandosi reciprocamente, anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva;
- garantire che nei suddetti contratti siano indicati i costi relativi alla sicurezza del lavoro, con particolare riferimento a quelli propri connessi allo specifico appalto.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Destinatari del presente Modello che, nello svolgimento della propria attività, si trovino a dover gestire attività rilevanti ai sensi dell'art. 25-*septies* del D.lgs. 231/2001, provvedono a comunicare tempestivamente all'Organismo di Vigilanza, in forma scritta, qualsiasi informazione concernente deroghe o violazioni dei principi di controllo e comportamento previsti al presente capitolo.

Dovranno essere tempestivamente inviate all'Organismo di Vigilanza le informazioni in merito:

- all'accadimento di infortuni o denunce di malattie professionali;
- alle modifiche ed agli aggiornamenti del Documento di Valutazione dei Rischi;
- al piano di formazione ed al consuntivo della formazione erogata in materia di salute e sicurezza sui luoghi di lavoro;
- alle visite ispettive da parte dei funzionari della Pubblica Amministrazione e relativi rilievi emersi a seguito di verifiche e accertamenti;
- alle eventuali violazioni, da parte delle funzioni preposte (accertate internamente o ad opera di autorità competenti), relative ad adempimenti richiesti dalla normativa in materia di salute e sicurezza dell'ambiente di lavoro e relative azioni correttive intraprese.

SANZIONI

In caso di violazione delle disposizioni contenute nella presente Parte Speciale, trovano applicazione le sanzioni disciplinari previste nel Modello di Organizzazione, Gestione e Controllo della Società, conformemente al CCNL applicato o al contratto di volta in volta sottoscritto.

Ogni violazione delle prescrizioni ivi contenute ovvero i comportamenti elusivi delle stesse da parte di soggetti terzi è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole inserite nei relativi contratti.

PARTE SPECIALE F

DELITTI CONTRO LA PERSONALITA' INDIVIDUALE E REATO DI IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

FUNZIONE DELLA PARTE SPECIALE F

La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i "Destinatari" del Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato richiamate dagli artt. 25-*quinquies* e 25-*duodecies* del D.lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di definire:

- i principi di comportamento che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello;
- i flussi informativi all'Organismo di Vigilanza.

FATTISPECIE DI REATO RILEVANTI

Di seguito vengono riportate le fattispecie di reato ritenute rilevanti per Careapt ai sensi degli artt. 25-*quinquies e 25-duodecies* del Decreto.

F.1 Delitti contro la personalità individuale

Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.)

Salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque:

1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

Se i fatti sono commessi mediante violenza o minaccia, si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato.

Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all´aspettativa obbligatoria, alle ferie;
3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà:

1) il fatto che il numero di lavoratori reclutati sia superiore a tre;
2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;

3) l´aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

F.2 Delitto di impiego di cittadini di stati terzi il cui soggiorno è irregolare

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 co. 12-*bis* del Decreto legislativo 25 luglio 1998, n. 286)

Il reato si configura allorquando il datore di lavoro occupa alle proprie dipendenze lavoratori:

- privi del permesso di soggiorno;
- il cui permesso di soggiorno è scaduto e non è stato richiesto il rinnovo nei termini di Legge;
- il cui permesso di soggiorno è stato revocato o annullato.

Il predetto reato comporta la responsabilità amministrativa di cui al Decreto quando:

- i lavoratori reclutati sono in numero superiore a tre;
- trattasi di minori in età non lavorativa;
- i lavoratori intermediati sono esposti a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

PRINCIPALI AREE DI RISCHIO

Le principali aree di rischio della Società, con riferimento ai delitti contro la personalità individuale e reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, sono riconducibili a:

- *Selezione e gestione del personale e del sistema di incentivazione;*
- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*

I Destinatari sono tenuti ad adeguare il proprio comportamento a quanto esposto nel presente documento.

PRINCIPI DI COMPORTAMENTO E MODALITÀ ESEMPLIFICATIVE DI COMMISSIONE DEL REATO

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari, come definiti nella Parte Generale del presente Modello.

In generale, **è fatto obbligo** di assicurare che lo svolgimento delle predette attività avvenga nell'assoluto rispetto di:

- leggi e normative vigenti;
- principi di lealtà, correttezza e chiarezza;
- Codice Etico.

In generale, **è fatto divieto** di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di cui agli artt. 25-*quinquies e 25-duodecies* del D.lgs. 231/2001 innanzi richiamate.

Di seguito sono elencate le principali modalità esemplificative dei reati con riferimento alle seguenti attività:

- **Gestione del personale e del sistema di incentivazione**

La gestione del personale e del sistema di incentivazione potrebbe presentare profili di rischio potenziale in relazione al **delitto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare** nell'ipotesi in cui, ad esempio, Il datore di lavoro della Società occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno.

La gestione del personale e del sistema di incentivazione potrebbe presentare profili di rischio potenziale in relazione al **reato di intermediazione illecita e sfruttamento del lavoro** nell'ipotesi in cui, ad esempio, la Società corrisponda ai propri lavoratori una retribuzione sproporzionata per difetto rispetto alla quantità e qualità del lavoro prestato ovvero viola ripetutamente la normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione della predetta attività oltre a quanto previsto alla Parte Speciale A "*Reati contro la Pubblica Amministrazione ed il suo patrimonio, reato di corruzione tra privati e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*" del presente Modello **è** altresì **fatto obbligo** di:

- garantire il rispetto della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria ed alle ferie;
- garantire una retribuzione proporzionata alla quantità ed alla qualità del lavoro prestato;
- verificare che i candidati cittadini di paesi terzi:
- siano in possesso di regolare permesso di soggiorno che abiliti al lavoro (non scaduto o revocato o annullato);
- in caso di permesso di soggiorno scaduto, abbiano presentato richiesta di rinnovo entro il termine previsto dalla normativa (documentata dalla relativa ricevuta postale);
- monitorare la validità dei documenti dei dipendenti cittadini di stati terzi e sollecitare il rinnovo degli stessi prima della scadenza indicata sul permesso di soggiorno.

Nell'ambito dei citati comportamenti **è fatto divieto** di:

- assumere personale, anche con contratti temporanei, senza il rispetto delle normative vigenti in materia previdenziale, fiscale, assicurativa e sulla disciplina dell'immigrazione,

ecc.;

- assumere dipendenti extracomunitari che non siano in regola con i requisiti richiesti dalla legge per soggiornare e svolgere attività lavorativa all'interno del territorio nazionale.

***

- **Gestione degli acquisti di beni e servizi (incluse le consulenze);**

La gestione degli acquisti di beni e servizi potrebbe presentare profili di rischio in relazione al **delitto di impiego di cittadini di stati terzi il cui soggiorno è irregolare** nell'ipotesi in cui, ad esempio, la Società, nell'ambito di un appalto, si rivolga a fornitori che impiegano lavoratori cittadini di stati terzi privi del permesso di soggiorno.

La gestione degli acquisti di beni e servizi (incluse le consulenze) potrebbe presentare profili di rischio in relazione ai **reati contro la personalità individuale** nell'ipotesi in cui, ad esempio, la Società nell'ambito di un appalto si rivolga a fornitori che impiegano lavoratori non rispettando le condizioni di lavoro previste dalla normativa.

Ai Destinatari che, per ragione del proprio incarico o della propria funzione o di specifico mandato, siano coinvolti nella gestione della predetta attività, oltre a quanto previsto nella Parte Speciale A "*Reati contro la Pubblica Amministrazione ed il suo patrimonio, reato di corruzione tra privati e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*" del presente Modello, **è** altresì **fatto obbligo** di:

- garantire che sia verificata la sussistenza dei requisiti normativi di regolarità della controparte tramite la consegna della documentazione prevista dalla legge (e.g., Documento Unico di Regolarità Contributiva – DURC);
- verificare la regolarità retributiva e contributiva dei lavoratori mediante verifiche, anche a campione, dei contratti di lavoro o del Libro Unico del Lavoro;
- assicurare la verifica del possesso del permesso di soggiorno in corso di validità per eventuale personale extracomunitario alle dipendenze di appaltatori e subappaltatori.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Destinatari del presente Modello che, nello svolgimento della propria attività, si trovino a dover gestire attività rilevanti ai sensi degli artt. 25-*quinquies e 25-duodecies* del D.lgs. 231/2001, provvedono a comunicare tempestivamente all'Organismo di Vigilanza, in forma scritta, qualsiasi informazione concernente deroghe o violazioni dei principi di controllo e comportamento previsti al presente capitolo.

SANZIONI

In caso di violazione delle disposizioni contenute nella presente Parte Speciale, trovano applicazione le sanzioni disciplinari previste nel Modello di Organizzazione, Gestione e Controllo della Società, conformemente al CCNL applicato o al contratto di volta in volta sottoscritto.

Ogni violazione delle prescrizioni ivi contenute ovvero i comportamenti elusivi delle stesse da parte di soggetti terzi è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole inserite nei relativi contratti.